Micro Focus Security ArcSight Real-time Threat Detection

Software Version: 4.0

Real-time Threat Detection Default Content Release Notes

Legal Notices

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

What's New

Real-time Threat Detection is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. It consolidates and normalizes data from disparate devices across your enterprise network in a centralized view.

This release of Real-time Threat Detection default content introduces out-of-the-box content for the Security Threat Monitoring and Threat Intelligence Platform use cases to help you utilize Real-Time Threat Detection and protect your environment.

- Security Threat Monitoring
- Threat Intelligence Platform

Security Threat Monitoring

Displays the out-of-the-box rules from the Security Threat Monitoring package.

Note: All URLs can be found under All Rules/ArcSight Foundation/Security Threat Monitoring

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
A Member was Added and Removed from Privileged Group within 24 Hours	Persistence T1098-Account Manipulation	Detects when users added and removed from a privileged group within 24 hours.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4729, 4733, 4757
User Account Created and Deleted within 24 Hours	Persistence T1136-Create Account	Detects user account creation and then deletion within 24 hours (Default TTL: 24 Hours) which triggers a correlation event sent to a triage main channel. This rule uses an active list.	Operating System	/Authentication/Delete ANOM_DEL_ACCT
A Member was Added into a Privileged Group	N/A	Detects users added into privileged groups.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4728, 4732, 4756
Egress DNS Communications Passed by Firewall	Exfiltration T1048.003-Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Detects egress DNS communications passed by a firewall. This rule is disabled by default, because volume might be very high if asset modeling for DNS servers is not done.	Firewall Events	/Access/Start /Access /Firewall
User Account Created	N/A	Detects user account creation.	Operating System	/Authentication/Add ANOM_ADD_ACCT ADD_USER NOT NULL

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Successful Brute Force Login	Credential Access T1110-Brute Force	Detects successful authentication events after a suspected brute force attempt. The rule triggers when the user account, attacker system, and target system information of successful authentication event matches an entry in the Brute Force Attempts active list.	Operating System	/Authentication/Verify /Success /Brute Force/Login
Multiple Failed Login to Different Accounts from Single Source	Credential Access T1110.003-Password Spraying	Detects multiple failed log-in attempts to different accounts from the same source.	Operating System	/Authentication/Verify
Egress Communications with Cleartext Protocol	Exfiltration T1048-Exfiltration Over Alternative Protocol	Detects cleartext protocols crossing a perimeter.	Firewall Events	/Access/Start /Access /Firewall
Detected Cross Site Scripting	Initial Access T1189-Drive-by Compromise	Detects cross-site scripting attacks to the application server via the request URLs and also from other IDS and application devices.	Web Server	/Application /IDS/Host/Antivirus /IDS
Consecutive Unsuccessful Logins to Same Account from different IPs	Credential Access T1110.001-Password Guessing	Detects sets of 3 consecutive unsuccessful logins to the same account from 3 different IP addresses.	Operating System	/Authentication/Verify
High Severity IDS Event	Lateral Movement T1210-Exploitation of Remote Services	Detects all the high-severity exploit attacks simulated in various ways gathering information from IDS.	IDS or IDP	/IDS/Network

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Consecutive Unsuccessful Logins to Same Account from different Countries	Credential Access T1110.001-Password Guessing	Detects sets of 3 consecutive unsuccessful logins to the same account from 3 different countries.	Operating System	/Authentication/Verify
Attack To Vulnerable Asset	N/A	Detects exploitation attempts on vulnerable assets.	Microsoft Windows	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Attack Vulnerable Asset
Multiple Unique IDS Events to Same Destination	Lateral Movement T1210-Exploitation of Remote Services	Detects multiple unique IDS events gathering information from IDS. This rule triggers only where there are 4 unique IDS events in a span of 30 minutes to the same destination.	IDS or IDP	/IDS/Network
Pass The Hash	Lateral Movement, Defense Evasion T1550.002-Pass the Hash	Detects Pass The Hash attack attempts on Windows machines. Upon each detection, the rules adds the target address to a suppression list in order to avoid multiple alerts on same address in a short period of time.	Microsoft Windows	NtLmSsp NTLM 3 Microsoft-Windows-Security-Auditing:4624 and 4625
Multiple Services Down on Same Host	Impact T1489-Service Stop	Detects multiple services down on same host in a 30 minutes lapse. Upon each detection, the rules adds the target address to a suppression list in order to avoid multiple alerts on same address in a short period of time. This rule is disabled by default due to possible performance impact.	Microsoft Windows	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Service Stopped /All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Service Failed
Authentication Attempted to Disabled Account	N/A	Detects authentication attempts to a disabled account.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4625 Security:531

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Privileged Account Locked Out	Credential Access T1110-Brute Force	Detects account lockouts.	Microsoft Windows Operating System	Microsoft-Windows-Security-Auditing:4740 Security:644 and 66:0
High Volume of Denies to Same Destination	N/A	Detects a high volume of denies to the same destination.	Firewall Events	/Access/Start /Access /Firewall
Malware Detected	N/A	Detects malware activities on devices. Upon each detection, the rule adds the target address to a suppression list in order to avoid multiple alerts on same address in a short period of time.	IDS or IPS	/IDS/Host/Antivirus /Host/Infection/Virus /Host/Application/Malware /Delete /Found /Check
Detected Code Injection	Initial Access T1190-Exploit Public-Facing Application	Detects code injections attacks to the application server via the request URLs, other IDS, and application devices.	Web Server	/Application /IDS/Host/Antivirus /IDS
Exploit Attempt Detected by IDS	Lateral Movement	Detects exploit attacks that gather information from IDS.	IDS or IDP	/IDS/Network
Detected SQL Injection	Initial Access T1210-Exploitation of Remote Services	Detects SQL Injection attacks to the application server via the request URL, other IDS, and application devices.	Web Server	/Application /IDS/Host/Antivirus /IDS

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Privilege Escalation Attempt Detected	Privilege Escalation T1068-Exploitation for Privilege Escalation	Detects privileged exploit attacks that gather information from IDS.	IDS or IDP	/Exploit/Privilege Escalation /IDS/Network
Brute Force IDS Detected Attempts	Credential Access T1110.001-Password Guessing	Detects brute force attack attempts detected by IDS. On the first event, the user account, attacker system, and target system information is added to the Brute Force Attempts active list.	IDS or IPS	/Brute Force/Login /IDS
Audit Cleared Log	Defense Evasion T1070-Indicator Removal on Host	Detects audit log clearing. Upon each detection, the rules adds the target address to a suppression list in order to avoid multiple alerts on same address in a short period of time.	Microsoft Windows	/Modify/Content /Host/Resource/File /Operating System /Success arcSight NTDS 15401 Microsoft-Windows-Eventlog:1102
Multiple Access Attempts To Malicious Domains From Same Source Address	Command And Control T1568.002-Domain Generation Algorithms	Detects multiple access attempts to malicious domains from same source address.	Microsoft Windows	Query:A, AAAA, and TxT
Consecutive Unsuccessful Logins to Administrative Account	Credential Access T1110.001-Password Guessing	Detects sets of 5 consecutive unsuccessful logins to privileged accounts within 1 minute.	Operating System	/Authentication/Verify

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Egress Restricted Services Communications Passed by Firewall	Initial Access, Persistence T1133-External Remote Services	Detects egress communications to restricted services passed by firewall.	Firewall Events	/Access/Start /Access /Firewall
Egress Communications to Suspicious Country	N/A	Detects egress communications to a suspicious country.	Firewall Events	/Access/Start /Access /Firewall
Brute Force OS and Application Attempts	Credential Access T1110.001-Password Guessing	Detects brute force attacks on OS and applications. The rule triggers when the failed authentication event from the same attacker system, using the same user account, to the same target system, exceeds the threshold. On first threshold, information about user account, attacker system, and target system is added to the Brute Force Attempts active list.	Operating System	/Authentication/Verify /Success /Brute Force/Login
DoS Activity Detected by IDS	Impact T1498.001-Direct Network Flood	Detects Network Denial of Service attacks gathering information from IDS.	IDS or IDP	/DoS /IDS/Network
New Process Created by InstallUtil	Defense Evasion T1218.004-InstallUtil	Detects when new processes created by Installutil.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
Multiple Attempts to Discover User Accounts	Discovery T1087.001-Local Account	Detects attempts to discover multiple user accounts present in local and security groups.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4799, 4798, and 4688 net

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Powershell Invoke-command Executed on Remote Host	Lateral Movement T1021.006-Windows Remote Management	Detects PowerShell Invoke-commands executed on a remote host.	PowerShell	PowerShell:800
Login after Work Hour	Initial Access, Privilege Escalation, Persistence, Defense Evasion T1078-Valid Accounts	Detects logins after work hours.	Operating System	/Authentication/Verify /Success /All Filters/ArcSight Foundation/MITRE ATT
Suspicious Access Control List Modifications	N/A	Adds suspicious discretionary access control list modification events to the suspicious ransomware activities tracking active list.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1
Data Loss through Network Shared Drive	Collection T1039-Data from Network Shared Drive	Detects any data loss occurring through a network shared drive.	McAfee	McAfee DLP:40101 OUTGOING_FS
Key Created At Silent Process Exit Registry Folder	Persistence, Privilege Escalation T1546.012-Image File Execution Options Injection	Detects key creation at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\.	Microsoft Windows Sysmon	Microsoft-Windows-Sysmon:1 C:\Windows\regedit.exe C:\Windows\System32\reg.exe SilentProcessExit
Data Loss through Email Redirect	Collection T1114-Email Collection	Detects suspected data loss from email redirects.	Exchange Server	REDIRECT

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
MSBuild.exe Executed on Non Development Environment	Defense Evasion T1127.001-MSBuild	Detects MSBuild.exe execution on non-development machines.	Microsoft Windows	C:\Windows\Microsoft.NET\Framework MSBuild.exe Microsoft-Windows-Security-Auditing:4688
Security Accounts Manager accessed through unauthorized tools	Credential Access T1003.002-Security Account Manager	Creates correlation events when the security accounts manager is accessed with unauthorized tools.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Mimikatz pwdumpx.exe PSEXESVC gsecdump secretsdump.py
Linux Auditd Kernel Module Loaded in Critical Server	Persistence, Privilege Escalation T1547.006-Kernel Modules and Extensions	Detects the loading Linux kernel module. This rule has special instructions to install the connector and configure log: https://sec.microfocus.com/foswiki/bin/view/ArcSightActivate/PLinuxOSConnectorInstallation	Unix	module-load
Malicious PowerShell Commandlets	Execution T1059.001-PowerShell	Detects malicious PowerShell commandlets run on your environment.	Microsoft Windows	PowerShell:800 powersploit PSAttack Empire
Data Loss through Email	Collection T1114-Email Collection	Detects data loss from outgoing emails.	McAfee	/Host/Application/Service/Email /Information Leak McAfee DLP:40200 OUTGOING_EMAIL
Code Execution Through.lnk File	Execution T1204.001-Malicious Link	Detects malicious code execution via .lnk file.	IDS or IPS	/Exploit /Redirection
Files Deleted On A Host	N/A	Detects files deleted from a command line interface on a host.	Microsoft Windows, Unix	Microsoft DELETE cmd.exe powershell.exe sdelete.exe sdelete64.exe /usr/bin/rm

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Exploit of Client Application	Execution T1203-Exploitation for Client Execution	Detects exploitation on client applications (like web browsers, Microsoft Office, Adobe Reader, and Flash).	Snort	/Exploit
Dynamic Data Exchange Related Attack	Execution T1559.002-Dynamic Data Exchange	Detects attacks leveraging Dynamic Data Exchange (DDE) technology.	ISS	[1:44694], [1:44695], [1:45214], [1:45215], [1:47844], [1:47845], [1:47846], [1:47847], [1:47848], [1:47849] XML_Excel_DDE_Command_Exec RTF_DDEAUTO_Command_Exec XML_Office_DDEAUTO_Command_Exec
Data Loss through Screen Capture	Collection T1113-Screen Capture	Detects data loss occurring via screen capture.	McAfee	McAfee DLP:40602 OUTGOING_MEMORY_VIA_SCREEN_CAPTURE
New Scheduled Task Created	Persistence, Execution, Privilege Escalation T1053.005-Scheduled Task	Detects new scheduled tasks created using windows events. Windows Event 602 also covers changes to the scheduled task.	Microsoft Windows	Security:602 Microsoft-Windows-Security-Auditing:4698
New Child Process Launched by CMSTP	Defense Evasion T1218.003-CMSTP	Detects new child processes launched by CMSTP.exe.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
Data Compression Process Started on Critical Host	Collection T1560.001-Archive via Utility	Creates a correlation event when a process from the Applications active list starts on a critical host.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1
PsExec Tool Execution	Execution T1569.002-Service Execution	Detects the execution of sysinternals PsExec tool.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4689 and 4688 PSEXESVC.EXE Service Control Manager:7045

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
External Device With autorun.inf Detected	N/A	Detects external drives with autorun.inf.	Microsoft Windows	autorun.inf /Host/Resource /Success /Operating System
Information Transfer to Removable Storage Device	Exfiltration T1052.001-Exfiltration over USB	Creates correlation events when information is transferred to a removable external device.	McAfee Microsoft Windows	McAfee DLP:40102 OUTGOING_FS_REMOVABLE Removable Storage Device Rule All USB drives Microsoft-Windows-Security-Auditing:4656
Malicious Control Panel File Detected	Defense Evasion T1218.002-Control Panel	Detects malicious control panel files.	TippingPoint	/Host/Application/Malware /Found /Compromise [1:33939], [1:33942], [1:33941], [1:33940], [1:33943] POP3:EXT:DOT-CPL SMTP:EXT:DOT-CPL 3784 2898 11839 2897 2320 3785 9542 2899 1793 19263 2896 12287 9543
Execution through Module Load	Execution T1129-Shared Modules	Detects exploit execution through dll.	IDS or IPS	/Exploit DLL-LOAD
Execution of Processes with Trailing Spaces	Defense Evasion T1036.006-Space after Filename	Detects the execution of linux processes with trailing spaces.	Unix	/Execute/Start /Operating System /Application /Failure .*\s$

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
HTRAN Signature Detected	Command And Control T1090.001-Internal Proxy	Detects HTRAN.	NetScreen	TROJAN:HTRAN-UA MISC:HTRAN-PROXY-CONNECT-FAILED
Data Loss through Clipboard Data	Collection T1115-Clipboard Data	Detects data loss through the clipboard data.	McAfee	McAfee DLP:40602 OUTGOING_MEMORY_VIA_CLIPBOARD
Suspicious Use of MSXSL.EXE	Defense Evasion T1220-XSL Script Processing	Detects suspicious use of msxsl.exe.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 msxsl.exe
Suspicious Use of WMIC	Execution T1047-Windows Management Instrumentation	Detects suspicious use of wmic.exe.	Microsoft Windows	C:\Windows\System32\wbem\WMIC.exe Microsoft-Windows-Security-Auditing:4688
Regsvcs OR Regasm Making Network Connection	Defense Evasion T1218.009-Regsvcs/Regasm	Detects network connections initiated by Regsvcs/Regasm.	Microsoft Windows	RegSvcs.exe RegAsm.exe C:\Windows\Microsoft.NET\Framework
CMSTP Involved on Network Connection	Defense Evasion T1218.003-CMSTP	Detects network connections initiated by CMSTP.exe	Microsoft Windows	cmstp.exe C:\Windows\System32 C:\Windows\SysWOW64
MetaSploit Detected	Execution T1059-Command and Scripting Interpreter	Detects Metasploit framework installation on systems using assessment tools.	Scanner	/Assessment Tools /scanner/device/uri /scanner/device/vulnerability CVE-2011-1056 CVE-2005-2482

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
VNC Exploit Execution	Lateral Movement, Execution T1072-Software Deployment Tools	Detects potential exploits on vnc related software.	IDS or IPS	/Exploit vnc
Track Modified Service	N/A	Detects modified services.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 sc.exe reg.exe delete add NOT NULL
Credential Dumping through Keefarce	Credential Access T1003-OS Credential Dumping	Detects credential dumping via Keefarce.	Microsoft Windows Sysmon	Microsoft-Windows-Sysmon: 1, 7, and 8 KeeFarce.exe
Script Executed On Critical Host	Execution T1059-Command and Scripting Interpreter	Detects script execution on a critical host.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 wscript.exe cscript.exe
HTA File Download	Defense Evasion T1218.005-Mshta	Detects a host trying to download an .HTA file.	Proxy	/Proxy
Large Information Transfer to Removable Storage Device	Exfiltration T1052.001-Exfiltration over USB	Creates correlation events when a large file transfers to a removable storage device.	McAfee Microsoft Windows	McAfee DLP:40102 OUTGOING_FS_REMOVABLE Removable Storage Device Rule All USB drives Microsoft-Windows-Security-Auditing:4656

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Suspicious Activity after New Service	Privilege Escalation, Persistence T1543-Create or Modify System Process	Detects suspicious activities after adding new service.	IDS or IPS	/Suspicious /Compromise /Hostile
MSXSL.exe Detected on Non Development Environment	Defense Evasion T1220-XSL Script Processing	Detects MSXSL.exe on a non-development environment.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 msxsl.exe
Detected DLL Hijacking Activity by PowerSploit	Privilege Escalation, Defense Evasion, Persistence T1574.001-DLL Search Order Hijacking	Detects DLL Hijacking activity by powersploit.	Microsoft Windows	PowerShell:800
Suspicious Activity after Modify Service	Privilege Escalation, Persistence T1543-Create or Modify System Process	Detects suspicious activities after adding a new service.	IDS or IPS	/Suspicious /Compromise /Hostile
Suspicious Powershell Command Line Argument Detected	Execution T1059.001-PowerShell	Detects suspicious powershell command line arguments.	Microsoft Windows	powershell.exe C:\Windows\System32\WindowsPowerShell\ C:\Windows\SysWOW64\WindowsPowerShell\ Microsoft-Windows-Security-Auditing:4688

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Logging Service On Host Has Stopped	Defense Evasion T1562.002-Disable Windows Event Logging	Detects when logging has stopped on a host.	Operating System	/Execute/Stop /Host/Application/Service /Operating System /Success
Host Firewall Has Stopped	Defense Evasion T1562.001-Disable or Modify Tools	Detects when host firewall service has stopped on host.	Operating System	/Execute/Stop /Host/Application/Service /Operating System /Success
Removable Device Blocked On Host	Initial Access T1200-Hardware Additions	Detects when a removable device is blocked on a host.	Microsoft Windows	/Host /Found /Success /Application
Detected Format String Attack	Initial Access T1190-Exploit Public-Facing Application	Detects format strings attacks.	Web Server	/IDS/Network /Application /IDS/Host/Antivirus /Exploit/Vulnerability /Traffic Anomaly/Application Layer /Compromise
Shell Command Execution	Execution T1059-Command and Scripting Interpreter	Detects potential shell commands and shellcode attacks.	Qualys	/Code/Shell Command /scanner/device/vulnerability /Code/Application Command
PowerShell Executed From Browser	Initial Access T1189-Drive-by Compromise	Detects powershell execution from a browser.	Microsoft Windows	Microsoft-Windows-Sysmon:1 powershell.exe iexplore.exe chrome.exe opera.exe firefox.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Image File Execution Options Injection	Persistence, Privilege Escalation T1546.012-Image File Execution Options Injection	Detects Image File Execution Options Injection through reg.exe command.	Microsoft Windows	reg.exe C:\Windows\System32 C:\Windows\SysWOW64 Microsoft-Windows-Security-Auditing:4688 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Detected Squiblydoo Attack	Defense Evasion T1218.010-Regsvr32	Detects Squiblydoo attacks.	Snort	[1:40829] and [1:40830]
InstallUtil Involved on Network Connection	Defense Evasion T1218.004-InstallUtil	Detects network connections initiated by InstallUtil.	Microsoft Windows	InstallUtil.exe C:\Windows\Microsoft.NET\Framework
Detected Enabled DCOM	Execution T1559.001-Component Object Model	Detects if DCOM is enabled on the system using vulnerability scanner events.	Qualys	/scanner/device/vulnerability /scanner/device/uri CVE-2013-4924, CVE-2003-0352, CVE-2004-0124, CVE-2002-2077, CVE-2017-0298, CVE-2003-0605, CVE-2003-0813, CVE-2017-0100 Qualys|90042
CertUtil used to decode file on host	Defense Evasion T1140-Deobfuscate/Decode Files or Information	Detects certutil used to decode a file.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 certutil.exe
External Device On Machine Infected With Malware	Lateral Movement, Initial Access T1091-Replication Through Removable Media	Detects malware infections on machines where an external drive was plugged with autorun.inf.	N/A	/All Rules/Real-time Rules/Security Threat Monitoring/Malware Monitoring/Malware Detected

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
JavaScript Code Executed through rundll32	Defense Evasion T1218.011-Rundll32	Detects JavaScript Code Executed via rundll32.	Microsoft Windows	rundll32.exe C:\Windows\System32 C:\Windows\SysWOW64 Microsoft-Windows-Security-Auditing:4688
Suspicious Boot Configuration Data Modifications	N/A	Adds suspicious Boot Configuration Data modification events to the Suspicious Ransomware Activities tracker active list.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1
Possible Ransomware Detected	Impact T1486-Data Encrypted for Impact	Detects when one of the following conditions are met: a large file modification in the users directory. Or, two different events from following three types: shadow copy deletion attempt, suspicious access list modifications, suspicious boot configuration data modifications.	Microsoft Windows	/All Rules/Real-time Rules/Security Threat Monitoring/Host Monitoring/Large amount of file modifications in users directories
Default Account Enabled	Defense Evasion, Persistence, Initial Access, Privilege Escalation T1078.001-Default Accounts	Detects enabling of default accounts.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4722 /Authorization/Add /Host/ /Success
File Deleted On Malware Infected host	Defense Evasion T1070.004-File Deletion	Detects file deletion on malware-infected hosts.	N/A	/All Rules/Real-time Rules/Security Threat Monitoring/Malware Monitoring/Malware Detected
Suspicious Activity after Scheduled Task	Privilege Escalation, Execution, Persistence T1053-Scheduled Task/Job	Detects suspicious activities after a scheduled task is created or updated.	IDS or IPS	/Suspicious /Compromise /Hostile

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Abnormal Use of hh.exe	Defense Evasion T1218.001-Compiled HTML File	Detects abnormal use of hh.exe command.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
Suspicious Activity after Local Job Changes	Privilege Escalation, Execution, Persistence T1053-Scheduled Task/Job	Detects suspicious activities after local scheduled job is changed.	IDS or IPS	/Suspicious /Compromise /Hostile
Shadow Copy Deletion Attempt	N/A	Adds events with process command line parameters containing commands to delete shadow copies to the Suspicious Ransomware Activities Tracker active list.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1
Track Job Scheduling Change	N/A	Detects changes of the /etc/crontab file.	N/A	N/A
API Hooking Detected	Collection, Credential Access T1056.004-Credential API Hooking	Detects API hooking using a volatility apihooks plugin.	ApiHook	hook:api
Powershell Script Executed by SyncAppvPublishingServer	Defense Evasion T1218-Signed Binary Proxy Execution	Detects powershell scripts executed by SyncAppvPublishingServer.	Microsoft Windows	SyncAppvPublishingServer.vbs SyncAppvPublishingServer.exe C:\Windows\System32\ C:\Windows\SysWOW64\ Microsoft-Windows-Security-Auditing:4688
Detected DLL Injection by Mavinject.exe	Defense Evasion T1218-Signed Binary Proxy Execution	Detects dll injections via Mavinject.exe.	Microsoft Windows	mavinject.exe C:\Windows\System32\ C:\Windows\SysWOW64\ Microsoft-Windows-Security-Auditing:4688

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Detected Directory Traversal	Initial Access T1190-Exploit Public-Facing Application	Detects directory traversal attacks.	Web Server	/IDS/Network /Application /IDS/Host/Antivirus
Suspicious Use of Msiexec.exe	Defense Evasion T1218.007-Msiexec	Detects suspicious use of Msiexec.exe.	Microsoft Windows	msiexec.exe C:\Windows\SysWOW64\ C:\Windows\System32\ Microsoft-Windows-Security-Auditing:4688
Windows Remote Management Enabled by PowerShell	Lateral Movement T1021.006-Windows Remote Management	Detects Windows Remote Management enabling via powershell.	Microsoft Windows	PowerShell:800
Track Scheduled Task	N/A	Tracks schedule tasks and writes them down on Suspicious Activities Tacking Active List.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4702, 4698, 4700
Multiple RDP Connections from the Same Host in Short Period of Time	Lateral Movement T1021.001-Remote Desktop Protocol	Detects multiple RDP connections from the same host in short period of time.	Microsoft Windows	mstsc.exe
Suspicious Data Transfer Process Started From Command Line	Exfiltration T1048-Exfiltration Over Alternative Protocol	Creates correlation events when a process from the Applications active list is started from the command line.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Information Transfer to Removable Device	Exfiltration T1052-Exfiltration Over Physical Medium	Creates correlation events when information is transferred to a removable external device.	McAfee Microsoft Windows	McAfee DLP:40102 OUTGOING_FS_REMOVABLE Removable Storage Device Rule All USB drives Microsoft-Windows-Security-Auditing:4656
Log into Multiple Systems in Short Period	Initial Access, Privilege Escalation, Persistence, Defense Evasion T1078-Valid Accounts	Detects logins to multiple systems in a short time period.	Operating System	/Authentication/Verify /Success
Registry Injection	Privilege Escalation, Defense Evasion T1055-Process Injection	Detects any modification on Appinit_DLL, AppCertDlls and IFEO (Image File Execution Options) which are registry keys that malware usually modifies for injection and persistence.	Microsoft Windows	Microsoft-Windows-Sysmon:13 HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\
Mshta Command Execution	Defense Evasion T1218.005-Mshta	Detects Mshta command executions.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 mshta.exe
Track New Service	N/A	Tracks new services.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4697 Service Control Manager:7045 NOT NULL
Key Created At Image File Execution Options Registry Folder	Persistence, Privilege Escalation T1546.012-Image File Execution Options Injection	Detects keys created on HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Option.	Microsoft Windows Sysmon	Sysmon Microsoft-Windows-Sysmon:12 and 13 HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Suspicious Use of PubPrn.vbs	Defense Evasion T1216.001-PubPrn	Detects suspicious use of PubPrn.vbs.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 cscript.exe
Multiple RDP Connections from the Same User in Short Period of Time	Lateral Movement T1021.001-Remote Desktop Protocol	Detects multiple RDP connections from the same user in short period of time.	Microsoft Windows	mstsc.exe
Large amount of file modifications in users directories	Impact T1486-Data Encrypted for Impact	Detects large amounts of file creation/modification in user directories.	Microsoft Windows	explorer.exe Microsoft-Windows-Security-Auditing:4656 Microsoft-Windows-Sysmon:11
Terminated User Account Added to the Privileged Group	Persistence T1098-Account Manipulation	Detects when a terminated user account is added to the privilege group.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4728, 4732, 4756
NXDOMAIN Attack	Impact T1498.001-Direct Network Flood	Detects multiple DNS queries to non-existing domains from the same source address.	Amazon Microsoft Windows	AWS Route53 CloudWatch Logs DNS Trace Log
Suspicious Large DNS Domain Requested	Command And Control T1071.004-DNS	Detects long DNS queries. Long queries are sometimes used for data exfiltration or C2 communication.	Amazon Microsoft Windows	AWS Route53 CloudWatch Logs DNS Trace Log

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
System Process Discovery	Discovery T1057-Process Discovery	Detects adversaries looking for information about running processes on a system. **Linux Note:** In order to capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service.	Microsoft Windows, auditd	SYSCALL|execve|success Microsoft-Windows-Security-Auditing:4688 tasklist.exe
System Network Configuration Discovery	Discovery T1016-System Network Configuration Discovery	Detects adversaries looking for details about the network configuration and settings of systems they access. **Linux Note:** In order to capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service.	Microsoft Windows, auditd	SYSCALL|execve|success Microsoft-Windows-Security-Auditing:4688 netsh.exe ipconfig.exe nltest.exe arp.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Remote System Discovery	Discovery T1018-Remote System Discovery	Detects adversaries looking for details about other systems by IP address, hostname, or other logical identifiers on a network. **Linux Note:** To capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve # For monitoring particular file location, we have to add the below rule to the file -w /etc/hosts -p rwa -k hosts_file_access Here,-w stands for the file path monitoring hosts location, -p stands for permissions and -k is the field which provides a name to the log logged in the Unix. Please retain the name as hosts_file_access, because we have used the same string name in one of the variables in the rule condition to catch these events. Restart the auditd service once the configuration is completed. **Windows Note:** To capture the Windows logs when an adversary tries to open and read certain files or directories please follow instructions provided in the link below. https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder Here, the path to be audited is C:\Windows\System32\Drivers\etc\hosts	Microsoft Windows, auditd	SYSCALL|open|success hosts_file_access Microsoft-Windows-Security-Auditing:4663

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Malicious process Masquerading as Windows Process	Defense Evasion T1036.005-Match Legitimate Name or Location	Detects malicious files running as a windows-known list of processes from a place other than c:\windows\system32.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 C:\Windows\System32 C:\Windows\SysWOW64\
Terminated User Account Successful Logon Detected	Persistence T1098-Account Manipulation	Creates correlation events when the successful login of a terminated user account is detected.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4624
Suspicious Network Scanning	Discovery T1046-Network Service Scanning	Detects attempts to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation.	Scanner	/Scan/ /Recon /IDS
Named Pipe Filename Local Privilege Escalation	Privilege Escalation T1068-Exploitation for Privilege Escalation	Detects named piped impersonations.	Microsoft Windows Sysmon	Sysmon Microsoft-Windows-Sysmon:1 and 13
Suspicious Network Sniffing	Credential Access, Discovery T1040-Network Sniffing	Detects suspicious network sniffing activities happening on the network.	Microsoft	ANOM_PROMISCUOUS SYSCALL|setsockopt|success Microsoft-Windows-Security-Auditing:4688 dumpcap.exe
A user account was terminated	N/A	Detects accounts deleted from the active directory.	Microsoft Windows	Microsoft Microsoft Windows /Success Security:630 Microsoft-Windows-Security-Auditing:4726

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Credential Dumping via ProcDump and Task Manager	Credential Access T1003.001-LSASS Memory	Detects when the ProcDump dumps the memory space of Lsass.exe and credential dumping through window task manager.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 procdump Microsoft-Windows-Sysmon:11 taskmgr.exe
Suspicious Application Discovery Activity On A Host	Discovery T1518-Software Discovery	Detects multiple queries to the registries that contain information about applications installed on a host.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4663 Query key value
TeamViewer Logging Disabled	Defense Evasion T1562.001-Disable or Modify Tools	Detects when TeamViewer is disabled. Adversaries might disable TeamViewer Logging to avoid detections.	Microsoft Windows	Microsoft-Windows-Sysmon:13 teamviewer_service.exe
Multiple Queries to Registry for Discovery	Discovery T1012-Query Registry	Detects when an adversary interacts with the Windows Registry to gather information about the system, configuration, and installed software. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	/Host/Resource/Registry /Access /Success Microsoft-Windows-Security-Auditing:4688 reg.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Password Policy Discovery	Discovery T1201-Password Policy Discovery	Detects attempts to access detailed information about the password policy used within an enterprise network. This would help the adversary create a list of common passwords and launch dictionary and brute force attacks. **Linux Note:** To capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve # For monitoring particular file location, we have to add the below rule to the file -w /etc/login.defs -p rx -k password_policy_discovered -w /etc/pam.d/system-auth -p rx -k password_policy_discovered Here,-w stands for the file path monitoring password policy files location, -p stands for permissions and -k is the field which provides a name to the log logged in the Unix. Please retain the name as password_policy_discovered, because, we have used the same string name in one of the variable in the rule condition to catch these events. Restart the auditd service once the configuration is completed. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation	Microsoft Windows, auditd	Microsoft-Windows-Security-Auditing:4688 SYSCALL|execve|success SYSCALL|open|success SYSCALL|readlink|success password_policy_discovered

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
		Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing		
Data Encoding Using Certutil	Command And Control T1132.001-Standard Encoding	Detects when a file has been encoded using Certutil.	Microsoft Windows	Microsoft-Windows-Sysmon:1 C:\Windows\System32\certutil.exe
PowerShell Antivirus Software Discovery	Discovery T1518.001-Security Software Discovery	Detects when Powershell is used to list the anti-virus software on machine.	Microsoft Windows	PowerShell:800

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Modification of Password Domain Policy	Discovery T1201-Password Policy Discovery	Detects attempts to access and modify detailed information about the password policy used within an enterprise network. This would help the adversary create a list of common passwords and launch dictionary and brute force attacks **Linux Note:** To capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve # For monitoring particular file location, we have to add the below rule to the file -w /etc/login.defs -p wa -k password_policy_modified -w /etc/pam.d/system-auth -p wa -k password_policy_modified Here,-w stands for the file path monitoring password policy files location, -p stands for permissions and -k is the field which provides a name to the log logged in the Unix. Please retain the name as password_policy_modified, because, we have used the same string name in one of the variable in the rule condition to catch these events. Restart the auditd service once the configuration is completed.	Microsoft Windows auditd	CONFIG_CHANGE SYSCALL|open|success SYSCALL|rename|success password_policy_modified Microsoft-Windows-Security-Auditing:4739 Authentication Policy Change Password

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Suspicious Process Run Location	Defense Evasion T1036.003-Rename System Utilities	Detects windows processes executed by a suspicious location. In Windows, some files should never execute out of certain directory locations. Any of these locations may exist for a variety of reasons, and executables may be present in the directory, but they should not execute.	Microsoft Windows	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688 \SystemVolumeInformation C:\Windows\Tasks \RECYCLER C:\Windows\debug C:\Windows\fonts C:\Windows\help C:\Windows\wbem C:\Windows\debut
Browser's Saved Credentials Access Detected	Credential Access T1555.003-Credentials from Web Browsers	Detects attempts to access the saved credentials from the browser (Limited to Chrome, Mozilla, Opera and IE).	Microsoft Windows	Microsoft-Windows-Security-Auditing:4663 ReadData
Registry Modified by Reg.exe	Defense Evasion T1112-Modify Registry	Detects registry modification by reg.exe command line.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 reg.exe C:\Windows\System32 C:\Windows\SysWOW64
Remote PowerShell Session Activity On Host	Execution T1059.001-PowerShell	Detects remote powershell sessions established on a host.	Microsoft Windows	Microsoft-Windows-Sysmon:1 C:\Windows\System32\svchost.exe
Possible Macro Embedded on Office Document	Defense Evasion T1027.002-Software Packing	Detects embedded macros in an Office document.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 wscript.exe powershell.exe
Windows Firewall Rule Discovery	Discovery T1518.001-Security Software Discovery	Detects queries made on registry that keeps Windows Firewall Rules.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4663 Query key value

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Suspicious File Discovery Activity On Host	Discovery T1083-File and Directory Discovery	Detects when multiple file extensions are accessed on the same machine in short period of time.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4663 ReadAttributes
File Transfer Using TeamViewer	Command And Control T1105-Ingress Tool Transfer	Detects remote file transfers using a TeamViewer application.	Microsoft Windows	Microsoft-Windows-Sysmon:11 teamviewer.exe
An Attempted Access to Lsass.exe	Credential Access T1003.001-LSASS Memory	Detects attempts to access Lsass.exe.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4656 and 4663 cscript.exe
Potential Privilege Escalation via Unquoted Service	Defense Evasion, Privilege Escalation, Persistence T1574.009-Path Interception by Unquoted Path	Detects when an Unquoted Service vulnerability is compromised.	Microsoft Windows	Microsoft-Windows-Sysmon:1 C:\program.exe Microsoft-Windows-Sysmon:11
Keystrokes Logging Attempt by PowerShell	Collection, Credential Access T1056.001-Keylogging	Detects when PowerShell modules and cmdlets trying to log keystrokes.	Microsoft Windows	PowerShell:800 GetAsyncKeyState GetKeyState GetAsyncKeyState GetKeyState KeyboardProc KeyboardProc SetWindowsHookEx WH_KEYBOARD_LL WH_KEYBOARD_LL SetWindowsHookEx Microsoft-Windows-PowerShell:4104

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Inhibit System Recovery	Impact T1490-Inhibit System Recovery	Detects the disabling or deletion of the built-in operating system services designed to help in recovery.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 vssadmin.exe wbadmin.exe bcdedit.exe
Suspicious RDP Redirection Using TSCON	Lateral Movement T1021.001-Remote Desktop Protocol	Detects RDP Session redirects via TSCON.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1
RDP Over a Reverse SSH Tunnel	Command And Control T1090-Proxy	Detects RDP connections over a reverse SSH tunnel.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4624 and 5156 10
Remote File Copy Using Certutil.exe	Command And Control T1105-Ingress Tool Transfer	Detects certutil.exe usage to download files from the internet.	Microsoft Windows	Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing:4688 C:\Windows\System32\certutil.exe
Suspicious Network Connections From Rundll32 Process	Defense Evasion T1218.011-Rundll32	Detects when rundll32.exe processes initiate a network connection to an IP address outside protected company range.	Microsoft Windows	Microsoft-Windows-Sysmon:3 rundll32.exe
Multiple Access To Windows Default Shared Folders From Same Source Address	Lateral Movement T1021.002-SMB/Windows Admin Shares	Detects when the same source address tries to access default windows admin share folders on multiple devices.	Microsoft Windows	Microsoft-Windows-Security-Auditing:5140

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Windows Registry Run Keys and Startup Folder	Persistence, Privilege Escalation T1547.001-Registry Run Keys / Startup Folder	Detects added entries to the run keys in the registry or startup folder.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 reg.exe PowerShell:800
Unusual Windows Process Relationship	Defense Evasion, Privilege Escalation T1055.012-Process Hollowing	Detects unusual parent-child windows system process relationships.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 C:\Windows\System32\
Account Tampering - Suspicious Failed Logon	Initial Access, Privilege Escalation, Persistence, Defense Evasion T1078-Valid Accounts	Detects uncommon error codes on failed logins that occur due to suspicious activity or tampering with accounts.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4625 User logon to account disabled by administrator User logon from unauthorized workstation User logon outside authorized hours User logon with expired account Microsoft-Windows-Security-Auditing:4776
Privilege Escalation through PrintSpoofer	Privilege Escalation T1068-Exploitation for Privilege Escalation	Detects impersonation privilege abuse on Windows 10 and server 2019.	Microsoft Windows	Microsoft-Windows-Sysmon:17 and 18 printspoofer.exe \spoolss

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Juicy-Rotten-Rogue Potato Exploitation	Privilege Escalation T1068-Exploitation for Privilege Escalation	Detects privilege escalation using Juicy, Rotten, and Rogue potato exploitation.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4624 3 Microsoft-Windows-Sysmon:1 w3wp.exe Microsoft-Windows-Sysmon:1 potato.exe Microsoft-Windows-Sysmon:17 roguepotato.exe \roguepotato\pipe\ Microsoft-Windows-Sysmon:1 roguepotato.exe
Possible Screen Capture by PowerShell	Collection T1113-Screen Capture	Detects screen capture by PowerShell.	Microsoft Windows	PowerShell:800 Drawing.Bitmap CopyFromScreen System.Drawing ::VirtualScreen Drawing.Bitmap CopyFromScreen System.Drawing ::VirtualScreen Microsoft-Windows-PowerShell:4104
Information Collection through Keystroke Applications	Collection, Credential Access T1056.001-Keylogging	Detects Input Capture techniques via Keystroke Applications.	IDS or IPS	/IDS/Network /IDS/Host /IDS /IDS/Host/Antivirus keylogger
Windows Firewall Rule Changed by netsh command	Defense Evasion T1562.001-Disable or Modify Tools	Detects when a windows firewall rule is changed by netsh command.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 netsh.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Fileless UAC Bypass Using sdclt.exe	Privilege Escalation, Defense Evasion T1548.002-Bypass User Account Control	Detects user access bypass via sdclt.exe.	Microsoft Windows	Microsoft-Windows-Sysmon:1 and 10 sdclt.exe
Suspicious Process Launched From Microsoft Office Applications	Initial Access T1566.001-Spearphishing Attachment	Detects uncommon processes launched from Microsoft office applications.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
Tor Traffic Activity Detected On The Network	Command And Control T1090.003-Multi-hop Proxy	Detects outbound traffic on ports 9001 or 9030. These ports are used by Tor for network communication.	Firewall Events	/Access/Start /Access /Firewall /Access/Start /Access /Firewall
New Child Process Launched by WMIiPRVSE.EXE	Execution T1047-Windows Management Instrumentation	Detects processes spawned from wmiprvse.exe.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
New Scheduled Task Via Schtasks	Persistence, Execution, Privilege Escalation T1053.005-Scheduled Task	Detects newly scheduled tasks created via the schtasks.exe command.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 schtasks.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
New Service Installation Detected	Privilege Escalation, Persistence T1543.003-Windows Service	Detects new service installations reported by windows security event 4697.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4697
UAC ByPass Registry Key Changed	Privilege Escalation, Defense Evasion T1548.002-Bypass User Account Control	Detects entries changes relevant to UAC Bypass.	Microsoft Windows	Microsoft-Windows-Sysmon:12 and 13
Malware Detected on localhost	N/A	Detects malware activities on the devices. Upon each detection, the rule adds the hostname to a suppression list in order to avoid multiple alerts from the same host in a short period of time.	IDS or IPS	/IDS/Host/Antivirus /Host/Infection/Virus /Host/Application/Malware /Delete /Found /Check
Obfuscated PowerShell Detected	Defense Evasion T1027-Obfuscated Files or Information	Detects obfuscated PowerShell execution.	Microsoft Windows	powershell.exe C:\Windows\System32\WindowsPowerShell\ C:\Windows\SysWOW64\WindowsPowerShell\ Microsoft-Windows-Security-Auditing:4688
New Service Installation Reported by SCM	Privilege Escalation, Persistence T1543.003-Windows Service	Detects new service installations reported by security control manager.	Microsoft Windows	Service Control Manager:7045

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Masquerading Through Unicode Right-To-Left Override (RTLO)	Defense Evasion T1036.002-Right-to-Left Override	Detects masquerading attempts via unicode right-to-left override (RTLO).	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
Possible Masquerading Detected	Defense Evasion T1036-Masquerading	Detects possible masquerading of processes.	Microsoft Windows	Microsoft-Windows-Sysmon:1 and 7 C:\Windows\System32 google arcsight OneDrive
New Command-Line Session	Execution T1059.003-Windows Command Shel	Detects new command-line sessions.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 cmd.exe
Dynamic Data Exchange Malware Detected	Execution T1559.002-Dynamic Data Exchange	Detects dynamic-data-exchange malware activities on the devices.	N/A	/All Rules/Real-time Rules/Security Threat Monitoring/Malware Monitoring/Malware Detected /All Rules/Real-time Rules/Security Threat Monitoring/Malware Monitoring/Malware Detected on localhost DDEDownloader W97M/Macroles W97M.DDEXLOADER W97M/Ddeauto Downloader.DDE OLE.DDE MSWord/DDE ddeauto DDEautoexec

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Possible Process Hollowing by PowerShell	Defense Evasion, Privilege Escalation T1055.012-Process Hollowing	Detects process hollowing by PowerShell.	Microsoft Windows	PowerShell:800 NtUnmapViewOfSection ZWUnmapViewOFSection NtUnmapViewOfSection ZWUnmapViewOFSection WriteProcessMemory ReadProcessMemory PROCESS_BASIC_INFORMATION NtQueryInformationProcess Microsoft-Windows-PowerShell:4104
Suspicious Remote Desktop Protocol	Lateral Movement T1021.001-Remote Desktop Protocol	Detects suspicious RDP commands.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 mstsc.exe
Possible Remote File Copy From Command Line	Command And Control T1105-Ingress Tool Transfer	Detects files copied over the network from CLI.	Microsoft Windows Sysmon	PowerShell PowerShell:800 Microsoft-Windows-Sysmon:1 xcopy.exe wget.exe robocopy.exe pscp.exe certutil.exe cmd.exe bitsadmin.exe powershell.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Chained Rule - System Information Discovery	Discovery T1082-System Information Discovery	Detects attempts to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. **Linux Note:** In order to capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows auditd	SYSCALL|execve|success Microsoft-Windows-Security-Auditing:4688 reg.exe Microsoft-Windows-Security-Auditing:4688 systeminfo.exe hostname.exe
Unlimited Sudo Cache Timeout Set	Defense Evasion, Privilege Escalation T1548.003-Sudo and Sudo Caching	This rule is fired when an adversary sets unlimited sudo cache timout. **Note:** In order to capture this use case please enable Snoopy Logging in the machine (or) simply provide the path /var/log/secure by installing the syslog file connector on the machine to be monitored.	Unix	N/A

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Sudo Command Execution Detected	Defense Evasion, Privilege Escalation T1548.003-Sudo and Sudo Caching	Detects sudo command executions. **Linux Note:** To capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart the auditd service once the configuration is completed.	Unix	SYSCALL|execve|success EXECVE sudo
Process Spawned by PsExec	Execution T1569.002-Service Execution	Detects processes spawned by PsExec.exe.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
Registry Modified Using PowerShell	Defense Evasion T1112-Modify Registry	This rule is fired when an adversary look for information about running processes on a system. **Linux Note:** In order to capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service.	Microsoft Windows	PowerShell:800

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Crackmapexec Pass the Hash	Lateral Movement, Defense Evasion T1550.002-Pass the Hash	Detects Pass the Hash (PtH) via crackmapexec	Microsoft Windows Sysmon	Microsoft-Windows-Sysmon:1 crackmapexec.exe
Invoke-DCOM Attempted via PowerShell	Lateral Movement T1021.003-Distributed Component Object Model	Detects Invoke-DCOM commands run via PowerShell on remote hosts via COM objects over DCOM.	Microsoft Windows	Microsoft-Windows-PowerShell:4104
Windows Admin Share Accessed	Lateral Movement T1021.002-SMB/Windows Admin Shares	Detects when a windows admin share has been accessed.	Microsoft Windows	Microsoft-Windows-Security-Auditing:5140
File Downloaded On Host	Command And Control T1105-Ingress Tool Transfer	Detects files downloaded using a web browser on the host.	Microsoft Windows	Microsoft-Windows-Sysmon:15
Possible Application Shimming Process Execution Indicator	Persistence, Privilege Escalation T1546.011-Application Shimming	Detects the execution of sdbinst.exe.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 sdbinst.exe
AD Object Permission Enumerated	Discovery T1069-Permission Groups Discovery	Detects attempts to enumerate the permissions of an AD object.	Microsoft	Microsoft-Windows-PowerShell:4104, 4688, 5158 Microsoft-Windows-Sysmon:1 dsacls.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
File or Folder Deleted Using cmd.exe	Defense Evasion T1070.004-File Deletion	Detects Windows deletion of files and folders using cmd.exe / c.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 cmd.exe
Windows Hooking API Used by PowerShell	Collection, Credential Access T1056.004-Credential API Hooking	Detects windows hooking API used by powershell.	Microsoft Windows	PowerShell:800 SetWindowsHookEx CallNextHookEx SetWinEventHook UnhookWindowsHookEx SetWindowsHookEx CallNextHookEx SetWinEventHook UnhookWindowsHookEx KeyboardProc LowLevelMouseProc GetProcAddress Hook Microsoft-Windows-PowerShell:4104
Proxy Server Address Modified	Command And Control T1090-Proxy	Detects when HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer values are modified.	Microsoft Windows	Microsoft-Windows-Sysmon:13
Possible Process Injection by PowerShell	Privilege Escalation, Defense Evasion T1055-Process Injection	Detects process injection by powershell.	Microsoft Windows	PowerShell:800 getprocaddress virtualalloc createthread getmodulehandle Microsoft-Windows-PowerShell:4104

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Possible Credential Dumping	Credential Access T1003.001-LSASS Memory	Detects when a process tries to access lsass.exe.	Microsoft Windows	Microsoft-Windows-Sysmon:10 C:\WINDOWS\system32\lsass.exe C:\Program Files (x86)\Google\Update\GoogleUpdate.exe C:\Program Files (x86)\McAfee\Common Framework\masvc.exe Sysmon.exe \Windows Defender\ PowerShell.exe wscript.exe cscript.exe C:\WINDOWS\system32
Disable System Firewall Using Registry Keys	Defense Evasion T1562.004-Disable or Modify System Firewall	Detects the disabling of the windows system firewall. Enable auditing of Sysmon or Windows Process Create events in order to capture the logs.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 reg.exe
DCOM Instance Creation Attempted	Lateral Movement T1021.003-Distributed Component Object Model	Detects DCOM instance creation attempts via PowerShell.	Microsoft Windows	Microsoft-Windows-PowerShell:4104
New Powershell Session	Execution T1059.001-PowerShell	Detects new powershell sessions.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 powershell.exe
Active Directory Database Dumping via Ntdsutil	Credential Access T1003.003-NTDS	Detects when NTDSUtil tool is used to dump a Microsoft Active Directory database to a disk.	Microsoft Windows	Microsoft-Windows-Sysmon:1

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Suspicious Remote System Discovery Commands Entered On Linux	Discovery T1018-Remote System Discovery	Detects when remote system discovery commands are entered on Linux machine.	Unix	SYSCALL|execve|success /usr/sbin/arp /usr/bin/nslookup /usr/bin/ping /usr/bin/traceroute /usr/sbin/arping /usr/bin/host
Possible Application Shimming Registry Indicator	Persistence, Privilege Escalation T1546.011-Application Shimming	Detects the changing of an entry relevant to application shimming.	Microsoft Windows	Microsoft-Windows-Sysmon:12 and 13
DCOM Objects Enumeration via PowerShell	Lateral Movement T1021.003-Distributed Component Object Model	Detects attempts to perform enumeration of DCOM objects via PowerShell.	Microsoft Windows PowerShell	PowerShell:800 HKCR:\CLSID Microsoft-Windows-PowerShell:4104
AD Reconnaissance through AdFind	Discovery T1087-Account Discovery	Detects when the Adfind tool is used for reconnaissance in an Active Directory environment.	Microsoft Windows	Microsoft-Windows-Sysmon:1 AdFind.exe
Possible Application Window Discovery	Discovery T1010-Application Window Discovery	Detects application window discovery activity on a host.	Microsoft Windows PowerShell	Microsoft-Windows-PowerShell:4104 PowerShell:800
Suspicious net use usage detected	Lateral Movement T1021.002-SMB/Windows Admin Shares	Detects when an windows admin is used in the command net use.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 net.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Scheduled Task Deleted	Defense Evasion T1070.004-File Deletion	Detects the deletion of scheduled tasks.	Microsoft Windows	schtasks.exe Microsoft-Windows-Security-Auditing:4688
Possible Application Shimming New Shim DataBase Indicator	Persistence, Privilege Escalation T1546.011-Application Shimming	Detects new shim database files created in the default shim database directory.	Microsoft Windows	Microsoft-Windows-Sysmon:11
Suspicious File Created	Command And Control T1105-Ingress Tool Transfer	Detects suspicious files created on the host.	Microsoft Windows	Microsoft-Windows-Sysmon:11
Brute Force Password Protected Office Files	Credential Access T1110-Brute Force	Detects multiple failed attempts to a password protected microsoft office files like doc, excel, and pptx.	OAlerts	OAlerts Microsoft Office 16 Alerts:300
sdclt Suspicious Process Detected	N/A	Detects sdclt suspicious processes.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 NOT NULL sdclt.exe
Suspicious Process Launched By User	Execution T1204-User Execution	Detects when a user executes a suspicious file.	Microsoft Windows	/All Rules/Real-time Rules/Security Threat Monitoring/Host Monitoring/Suspicious Process Launched From Microsoft Office Applications Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 c:\windows c:\program files powershell.exe cmd.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Possible File and Folder Discovery On Linux	Discovery T1083-File and Directory Discovery	Detects multiple commands related to file and folder discovery run on the same Linux machine in a short time.	Unix	Unix SYSCALL|execve|success
Powershell Related Alert	Execution T1059.001-PowerShell	Detects powershell related alerts.	N/A	T1059.001
Suspicious Uncommonly Used Port Events by Script	Command And Control T1571-Non-Standard Port	Detects commonly used port events launched by a script.	Microsoft Windows	Microsoft-Windows-Sysmon:3 powershell.exe wscript.exe cscript.exe
Possible Data Exfiltration	Exfiltration T1041-Exfiltration Over C2 Channel	Detects suspicious amounts of data transferred to any host outside the protect network.	Zeek	N/A
File or Folder Deletion on Linux	Defense Evasion T1070.004-File Deletion	Detects deletion of files and folders on the Linux system. To capture this use case, the following steps are needed to be done: 1. Install Snoopy Logging (open source) on the Linux machine that is being monitored 2. Install Syslog file connector 3. Provide the path as /var/log/secure in the Syslog connector	Unix	Unix
Remote Access Tool Detected	Command And Control T1219-Remote Access Software	Detects remote access tools.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 vncserver.exe aa_v3.exe logmein.exe tv_x64.exe tv_x32.exe teamviewer.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
System Information Discovery	Discovery T1082-System Information Discovery	Detects attempts to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. **Linux Note:** In order to capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows auditd	SYSCALL|execve|success Microsoft-Windows-Security-Auditing:4688 reg.exe Microsoft-Windows-Security-Auditing:4688 systeminfo.exe hostname.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Browser's Saved Credentials Dumping Attempt by PowerShell	Credential Access T1555.003-Credentials from Web Browsers	Detects PowerShell modules or cmdlets trying to dump a browser's saved credentials based on PowerShell events.	Microsoft Windows	PowerShell:800 New-Object IO.FileStream \AppData\Local\Google\Chrome\User Data\Default\Login Data \AppData\Roaming\Mozilla\Firefox\Profiles signons logins.json key4.db key3.db Microsoft-Windows-PowerShell:4104 New-Object IO.FileStream
File or Folder deleted by PowerShell	Defense Evasion T1070.004-File Deletion	Detects file or folder deletion by PowerShell.	Microsoft Windows	PowerShell:800
Suspicious Data Encryption Process Started From Command Line	Collection T1560-Archive Collected Data	Creates a correlation event when a process from the Applications active list is started from the command line using encryption parameters.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1
File Copied On Shared Folder	Command And Control T1105-Ingress Tool Transfer	Detects files copied on a shared folder. In order to get these events, enable folder auditing on Windows.	Microsoft Windows	Microsoft Windows Microsoft-Windows-Security-Auditing:5145 WriteData (or AddFile)

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Virtual Machine Environment Discovery Using Registry	Defense Evasion, Discovery T1497.002-User Activity Based Checks	Detects interactions with the Windows Registry to gather information about the system, configuration, and installed software. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 reg.exe PowerShell:800
Disable Windows System Firewall	Defense Evasion T1562.004-Disable or Modify System Firewall	Detects the disabling of the windows system firewall. **Windows Note:** In order to capture the windows logs, please follow the below steps In order to audit any policy changes in windows, please enable auditing in the following fields in the group policy editor: Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Policy Change Under the Policy Change fields, there are multiple subcategories. Enable Auditing for the following fields: Audit Filtering Platform Policy Change Audit MPSSVC Rule-Level Policy Change Audit other Policy Change Events Restart the service mpssvc.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4950 and 4688 MPSSVC Rule-Level Policy Change No netsh.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Possible Software Packing Attempted	Defense Evasion T1027.002-Software Packing	Detects Software Packing attempts through UPX and Mpress packers.	Microsoft	Microsoft-Windows-PowerShell:4104 Microsoft-Windows-Sysmon:1 mpress.exe upx.exe
Possible System Owner Discovery	Discovery T1033-System Owner/User Discovery	Detects system owner discovery activity on the machine.	Microsoft Windows, PowerShell	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 quser.exe whoami.exe qwinsta.exe wmic.exe net.exe net1.exe Microsoft-Windows-PowerShell:4104
Indirect Command Execution	Defense Evasion T1202-Indirect Command Execution	Detects forfiles.exe or pcalua.exe used to run a process.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 forfiles.exe pcalua.exe
Data Likely Staged for Exfiltration	Collection T1074-Data Staged	Detects when any data is likely staged in a centralized location.	Microsoft	Microsoft-Windows-PowerShell:4104 PowerShell:600 and 800 Microsoft-Windows-Sysmon:1
Possible Network Share Discovery	Discovery T1135-Network Share Discovery	Detects network share discovery activity on a host.	Microsoft Window, PowerShell	Microsoft-Windows-Security-Auditing:4688 net.exe PowerShell:800
Windows File Deleted Using Sdelete	Defense Evasion T1070.004-File Deletion	Detects Sdelete command executions.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 sdelete

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
UAC ByPass through sdclt.exe	Privilege Escalation, Defense Evasion T1548.002-Bypass User Account Control	Detects UAC Bypass through sdclt.exe. Make sure rule sdclt.exe Suspicious Command Executed is enabled before using this rule.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
Suspicious Data Compression Process Started From Command Line	Collection T1560-Archive Collected Data	Creates a correlation event when a process from the applications active list starts from the command line.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Sudoers File Modified	Defense Evasion, Privilege Escalation T1548.003-Sudo and Sudo Caching	Detects attempts to modify the sudoers file in the Linux system. **Linux Note:** To capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve # For monitoring particular file location, we have to add the below rule to the file -w /etc/sudoers -p w -k sudoers_file_ modified Here,-w stands for the file path monitoring hosts location, -p stands for permissions and -k is the field which provides a name to the log logged in the Unix. Please retain the name as sudoers_file_modified, because, we have used the same string name in one of the variable in the rule condition to catch these events. Restart the auditd service once the configuration is completed.	auditd	Unix sudoers_file_modified
Access Token Manipulation by Powersploit	Defense Evasion, Privilege Escalation T1134.002-Create Process with Token	Detects Access Token Manipulation via Powersploit.	Microsoft Windows	Microsoft-Windows-PowerShell:4104

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
WMI Command Executed	Execution T1047-Windows Management Instrumentation	Detects abuse of Windows Management Instrumentation (WMI) to achieve execution. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 wmic.exe PowerShell:800
Disabled tty_tickets for Sudo Caching	Defense Evasion, Privilege Escalation T1548.003-Sudo and Sudo Caching	Detects the disabling of tty_tickets for sudo caching. **Note:** In order to capture this use case please enable Snoopy Logging in the machine (or) simply provide the path /var/log/secure by installing the syslog file connector on the machine to be monitored.	Unix	N/A
Possible File And Folder Discovery On Windows Machine	Discovery T1083-File and Directory Discovery	Detects activity related to file and folder discovery on the host.	Microsoft Windows	PowerShell:800 Microsoft-Windows-PowerShell:4104 Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1
Outbound SSH Connection Detected	Command And Control T1573.002-Asymmetric Cryptography	Detects outbound SSH connections.	Microsoft Windows, Zeek	Microsoft-Windows-Sysmon:3

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Suspicious Commonly Used Port Events by Script	Command And Control T1071-Application Layer Protocol	Detects commonly used port events launched by a script.	Microsoft Windows	Microsoft-Windows-Sysmon:3 powershell.exe wscript.exe cscript.exe
Remote Access Tool Downloaded Using PowerShell	Command And Control T1219-Remote Access Software	Detects remote access tools downloaded using PowerShell.	Microsoft Windows	PowerShell:800 DownloadFile
Commands Executed to Create a New Service	Privilege Escalation, Persistence T1543-Create or Modify System Process	Detects abuse to the system by creating new services using a Command Line tool or PowerShell. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 sc.exe PowerShell:800
LoggedOn Users Enumeration Detected	Discovery T1087-Account Discovery	Detects logged-on user enumeration performed via cmd and PowerShell.	Microsoft Windows	Microsoft-Windows-Sysmon:1 quser.exe query.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Data Collection through Mimikittenz	Collection T1005-Data from Local System	Detects Data Collection attempts via Mimikittenz.	Microsoft	Microsoft-Windows-PowerShell:4104 Microsoft-Windows-Windows Defender:1116 Microsoft-Windows-Windows Defender:1117 mimikittenz
Service Modified through Registry Using PowerShell	Privilege Escalation, Persistence T1543.003-Windows Service	Detects system services modifications through registry using powershell commands.	Microsoft Windows	PowerShell:800
Disable System Firewall Using PowerShell	Defense Evasion T1562.004-Disable or Modify System Firewall	Detects when a windows system firewall is disabled. Enable auditing of Windows PowerShell events in order to capture the logs.	Microsoft Windows	PowerShell:800
Suspicious Remote System Discovery Commands Entered On Windows	Discovery T1018-Remote System Discovery	Detects remote system discovery commands entered on a Windows machine.	Microsoft Windows, PowerShell	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 tracert.exe nltest.exe nslookup.exe dsquery.exe arp.exe ping.exe net.exe net1.exe PowerShell:800

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Browser Bookmark Discovery	Discovery T1217-Browser Bookmark Discovery	Detects attempts to enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may also highlight additional targets after an adversary has access to valid credentials, especially Credentials in Files associated with logins cached by a browser. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 PowerShell:800

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Changes to Windows Firewall Exception List	Defense Evasion T1562.004-Disable or Modify System Firewall	Detects modification to the windows system firewall exception list. **Windows Note:** In order to capture the windows logs, please follow the below steps. In order to audit any policy changes in windows, please enable auditing in the following fields in the group policy editor: Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Policy Change Under the Policy Change fields, there are multiple subcategories. Enable Auditing for the following fields: Audit Filtering Platform Policy Change Audit MPSSVC Rule-Level Policy Change Audit other Policy Change Events Restart the service mpssvc.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4948, 4947, 4946 MPSSVC Rule-Level Policy Change
Suspicious Executable File with Double Extension	Defense Evasion T1036-Masquerading	Detects when a windows executable file has a double extension.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
DNS-Tunnel Creation Attempted via DNScat	Command And Control T1071.004-DNS	Detects when DNScat is downloaded and DNS Tunnel Creation is attempted.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 dnscat
Process Discovery Using PowerShell	Discovery T1057-Process Discovery	Detects when an adversary looks for information about running processes on a system using PowerShell Command.	Microsoft Windows PowerShell	PowerShell:800

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Proxy Modification Attempt	Command And Control T1090-Proxy	Detects attempts to change the proxy settings using netsh.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1 netsh.exe
Possible Application Shimming PE Original Filename and Hash Indicator	Persistence, Privilege Escalation T1546.011-Application Shimming	Detects sdbinst.exe original PE File names or hash.	Microsoft Windows	Microsoft-Windows-Sysmon:1 md5=b365f6d8d8b2f42cb499179ea0693b9e sdbinst.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
System Network Connections Discovery	Discovery T1049-System Network Connections Discovery	Detects adversaries looking for details about the network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. **Linux Note:** In order to capture the Linux logs, please include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing **Powershell Note:** To capture the PowerShell logs, please make necessary modifications as per the below connector guide link. https://community.microfocus.com/dcvta86296/attachments/dcvta86296/connector-documentation/1290/2/MSPowershellWin	PowerShell	SYSCALL|execve|success Microsoft-Windows-Security-Auditing:4688 netstat.exe Microsoft-Windows-Security-Auditing:4688 net.exe net1.exe route.exe PowerShell:800

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
		EvtLog_N.pdf		
Domain Trust Discovery	Discovery T1482-Domain Trust Discovery	Detects attempts to gather information on domain trust relationships that may be used to identify opportunities in Windows multi-domain/forest environments. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 dsquery.exe nltest.exe PowerShell:800
Credentials in Registry Discovery	Credential Access T1552.002-Credentials in Registry	Detects queries the Registry looking for credentials and passwords that have been stored for use by other programs or services. **Windows Note:** To capture the Windows logs, please enable command-line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 reg.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Reconnaissance Activity Detected	Reconnaissance T1595.001-Scanning IP Blocks	Detects reconnaissance activity.	Scanner	/Recon /Scan /Success
Cloud Monitoring Disabled	Defense Evasion T1562.008-Disable Cloud Logs	Detects when cloud monitoring has been disabled or deleted from the environment. **False Positives:** Administrator account doing maintenance in the cloud environment.	SecurityHub	StopLogging DeleteTrail MICROSOFT.INSIGHTS/DIAGNOSTICSETTINGS/DELETE Logging
Possible Horizontal Scan Detected	Reconnaissance T1595.001-Scanning IP Blocks	Detects scans of mutiple target addresses over a victim's firewall. By default, the aggregation is set to 50 hits in 1 minute. **Note:** A horizontal scan is described as scan against a group of IPs for a single port.	Firewall	/Firewall /Communicate/Query /Success
Possible Vertical Scan Detected	Reconnaissance T1595.001-Scanning IP Blocks	Detects attempts attempts to scan multiple destination ports. By default, the aggregation is set to 20 hits in 1 minute. **Note:** A vertical scan is described as a single IP being scanned for multiple ports.	Firewall	/Firewall /Communicate/Query /Success
Scanning IP Blocks	Reconnaissance T1595.001-Scanning IP Blocks	Detects attempts to run scans to gather information that can be used during the MITRE chain. The scope of this rule is only for a possible insider trying to scan IP blocks to target another system.	Scanner	/Scan/IP Protocol /Recon
New Self-Signed Certificate Created using PowerShell	Resource Development T1587.003-Digital Certificates	Detects attempts to create a new Self-Signed Certificate using PowerShell by an insider.	Microsoft Windows PowerShell	PowerShell:800

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Vulnerability Scanning	Reconnaissance T1595.002-Vulnerability Scanning	Detects attempts to run scans to gather the information that can be used during the next stages in the MITRE Chain. The scope of this rule is only for a possible insider trying to do a vulnerability scan to target a victim machine.	Scanner	/Scan/Vulnerability /Recon
Azure Runbook Created	Defense Evasion T1562.001-Disable or Modify Tools	Detects azure runbook creation in the cloud environment. **Investigation Tip:** Adversaries could create runbooks to execute automate tasks in the azure cloud environment. **False Positives:** Cloud administrator executing administrative tasks in the cloud environment.	Azure	MICROSOFT.AUTOMATION/AUTOMATIONACCOUNTS/RUNBOOKS/WRITE
Cloud Account Created	N/A	Detects users account creation in the ctive list Cloud Accounts Created. Then the information will be used as support for chaining conditions so that the amount of possible false positives can be reduced. Every user account tracked in the active list will be only by 24 hours as default and after this time the record will be automatically removed.	Azure	Add user
Azure Runbook Deleted	Defense Evasion T1562.001-Disable or Modify Tools	Detects azure runbook deletion in the cloud environment. **Investigation Tip:** Adversaries could delete existing azure runbooks to disrupt certain functionalities within the cloud environment. **False Positives:** Administrator account doing maintenance in the cloud environment.	Azure	MICROSOFT.AUTOMATION/AUTOMATIONACCOUNTS/RUNBOOKS/DELETE

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Cloud Instance Created By Recent User Created	Defense Evasion T1578.002-Create Cloud Instance	Detects cloud instances created by a user account recently created in the cloud environment. The user that created an instance must be in the active list Cloud Accounts Created to produce an alert. **False positives:** A new administrator account created creating cloud instances	Azure	MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE
Cloud Key Vault Updated	Credential Access T1552.001-Credentials In Files	This use case alerts when cloud key storage modified or created on the cloud environment. **Investigation Tip:** Find out if user updating or creating the key vaults is authorized to do such activity. **False Positives:** Administrator account doing maintenance in the cloud environment.	Azure	MICROSOFT.KEYVAULT/VAULTS/WRITE
Azure Service Principal Created	Persistence T1098.001-Additional Cloud Credentials	Detects azure service principal creation. **Investigation Tip:** Adversaries could abuse of service principals and use it as backdoors to consistently access the environment and carry out malicious activities. Monitor service principals and ensure this is created by an authorized account. **False Positives:** Administrator account doing maintenance in the cloud environment.	Azure	Add service principal
Cloud Key Vault Deleted	Credential Access T1552.001-Credentials In Files	Detects cloud key storagedeletion on the cloud environment. **Investigation Tip:** Find out if user deleting the key vault is authorized to do such activity. **False Positives:** Administrator account doing maintenance in the cloud environment.	Azure	MICROSOFT.KEYVAULT/VAULTS/DELETE

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Azure Resource Group Deleted	Defense Evasion T1562.001-Disable or Modify Tools	Alerts when azure resource groups are deleted. **Investigation Tip:** Adversaries could delete resource groups to disrupt the environment or to destroy data, therefore investigate if deletion was done by an authorized account. **False Positives:** Administrator account doing maintenance in the cloud environment.	Azure	MICROSOFT.RESOURCES/SUBSCRIPTIONS/RESOURCEGROUPS/DELETE
Cloud Network Monitoring Disabled	Defense Evasion T1562.001-Disable or Modify Tools	Alerts when network diagnostic settings have been disabled or deleted on the cloud environment. **Investigation Tip:** Find out if user account is authorized to carry out any of these activities. **False Positives:** Administrator account doing maintenance in the cloud environment.	Azure	MICROSOFT.NETWORK/NETWORKWATCHERS/DELETE
Cloud Firewall Deleted	Defense Evasion T1562.007-Disable or Modify Cloud Firewall	This use case alerts when any of the firewall features provided by the cloud vendor it is disabled or deleted. **False Positive:** Regular activity performed by cloud administrators.	Azure	MICROSOFT.NETWORK/AZUREFIREWALLS/DELETE
Cloud Instance Snapshot By Recent User Created	Defense Evasion T1578.001-Create Snapshot	This use case alerts when cloud snapshots are created by a user account recently created in the cloud environment. The user that created the snapshot must be in the active list Cloud Accounts Created to produce an alert. **False positives:** A new administrator account creating cloud snapshots.	Azure	MICROSOFT.COMPUTE/SNAPSHOTS/WRITE

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Cloud Storage Deleted	Impact T1485-Data Destruction	Alerts when cloud storage was deleted. **Investigation Tip:** Adversaries could delete resource groups to disrupt the environment or to destroy data, therefore investigate if deletion was done by an authorized account. **False Positives:** Administrator account doing maintenance in the cloud environment.	Azure	MICROSOFT.STORAGE/STORAGEACCOUNTS/DELETE
Multiple Cloud Firewall Updates	Defense Evasion T1562.007-Disable or Modify Cloud Firewall	Alerts when multiple cloud firewall updates are made by same user account in a short period of time. **False Positives:** Regular Administrator cloud account user performing changes on the environment.	Azure	MICROSOFT.NETWORK/AZUREFIREWALLS/WRITE
Cloud Instance Deleted By Recent User Created	Defense Evasion T1578.003-Delete Cloud Instance	Alerts when cloud instances are deleted by a user account recently created in the cloud environment. The user that deleted the instance must be in the active list Cloud Accounts Created to produce an alert. **False positives:** A new administrator account deleting cloud instances	Azure	MICROSOFT.COMPUTE/VIRTUALMACHINES/DELETE
Email with Malicious Url	Initial Access T1566.002-Spearphishing Link	Rule detects emails with malicious Url on Office 365.	365 Defender	InitialAccess T1566.002
AWS Unusual Policy Changes on S3 buckets	Defense Evasion T1562.001-Disable or Modify Tools	Rule detects abnormal permission policy changes on S3 Buckets.	SecurityHub	Policy:S3

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
AWS Instance Querying DGA Domains	Command And Control T1568.002-Domain Generation Algorithms	Rule detects when an AWS EC2 instance is querying DGA domains.	SecurityHub	DGA
AWS EC2 Unusual Port Traffic	Command And Control T1571-Non-Standard Port	Rule detects when an EC2 instance has established a communication on an unusual port.	SecurityHub	EC2 NetworkPortUnusual
AWS Phishing Activity from EC2 Instance	Initial Access T1566-Phishing	Detects suspicious activity related to phishing or Spam on EC2 instance.	SecurityHub	EC2 Phishing Spam
Files Created	N/A	Tracks files created by browser and mail applications.	Microsoft Windows	Microsoft-Windows-Sysmon:11 chrome.exe firefox.exe brave.exe opera.exe iexplorer.exe outlook.exe
AWS Pentest Activity	Privilege Escalation, Persistence, Defense Evasion, Initial Access T1078.004-Cloud Accounts	Detects when an AWS cloud account has been used on penetration testing tool to make unauthorized API request on the cloud.	SecurityHub	PenTest

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
AWS Root Account Usage	Defense Evasion, Persistence, Initial Access, Privilege Escalation T1078.001-Default Accounts	Detects AWS suspicious activity on root accounts.	SecurityHub	Root
Possible Domain Account Created	Persistence T1136.002-Domain Account	Detects domain account creation from the command line interface on a computer.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 net.exe
AWS Account Privilege Escalation Activity	Privilege Escalation, Persistence, Defense Evasion, Initial Access T1078.004-Cloud Accounts	Detects when anomalous API requests associated with privilege escalation activity has been observed from any AWS cloud account.	SecurityHub	PrivilegeEscalation
AWS Brute Force Activity from EC2 Instance	Credential Access T1110.001-Password Guessing	Detects AWS suspicious brute force activity on EC2 instance.	SecurityHub	EC2 BruteForce
Unusual Microsoft Office Network Connections	Defense Evasion T1221-Template Injection	Detects unusual traffic generated by Microsoft Office applications.	Microsoft Windows Sysmon	Microsoft-Windows-Sysmon:3 excel.exe winword.exe powerpnt.exe eqnedt32.exe fltldr.exe mspub.exe msaccess.exe outlook.exe infopath.exe onenote.exe visio.exe winproj.exe

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Possible WMI Persistence	Persistence, Privilege Escalation T1546.003-Windows Management Instrumentation Event Subscription	Detects a possible WMI persistence activity on the machine.	Microsoft Windows	Microsoft-Windows-Sysmon:19, 20, and 21
AWS Exfiltration Activity	Exfiltration T1537-Transfer Data to Cloud Account	Detects suspicious activity related to exfiltration on the AWS cloud environment.	SecurityHub	Exfiltration TrafficVolumeUnusual
AWS Port Scan	Discovery T1046-Network Service Scanning	Detects AWS port scan activity on EC2 instance.	SecurityHub	Sweep Probe Scan
AWS Impossible Travel	Privilege Escalation, Persistence, Defense Evasion, Initial Access T1078.004-Cloud Accounts	Detects multiple successful console logins for the same IAM user around the same time in various geographical locations.	SecurityHub	UnauthorizedAccess:IAMUser-ConsoleLoginSuccess
AWS DoS Activity from EC2 Instance	Impact T1498.001-Direct Network Flood	Detects AWS DoS activity from EC2 instance.	SecurityHub	EC2 DenialOfService

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
AWS Password Policy Changed	Privilege Escalation, Persistence, Defense Evasion, Initial Access T1078.004-Cloud Accounts	Detects when a password policy was weakened on AWS cloud account.	SecurityHub	Stealth IAMUser-PasswordPolicyChange
Possible Domain Account Discovery	Discovery T1087.002-Domain Account	Detects when domain account discovery activity has been detected on a machine.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 net.exe
Suspicious SharePoint Activity	Collection T1213.002-Sharepoint	Detects when a large amount of files have been accessed by the same username in a short period of time.	SharePoint Online	FileAccessed SharePointFileOperation
AWS EC2 Bitcoin Activity	Impact T1496-Resource Hijacking	Detects when an AWS EC2 instance has been found querying IP addresses or domains associated with Cryptocurrency activity.	SecurityHub	EC2 Bitcoin
Malware Detected On File Downloaded on Machine	Execution T1204.002-Malicious File	Detects malware activity on files downloaded on the device by an user. If there is a malware infection and the file exists on the active list, an alert fires and further analysis on the machine is required.	IDS or IPS	/IDS/Host/Antivirus /Host/Infection/Virus /Host/Application/Malware /Delete /Found /Check

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Possible Archive of Collected Data Using PowerShell	Collection T1560-Archive Collected Data	Detects attempts compress data that is collected using PowerShell. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-PowerShell:4104 Execute a Remote Command
Possible DCSync OS Credential Dumping	Credential Access T1003.006-DCSync	Detects DCSync OS credential dumping based on windows event 4662. For more information about this event, refer to https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4662.	Microsoft Windows	Microsoft-Windows-Security-Auditing:4662 {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Possible Change of Default File Association	Privilege Escalation, Persistence T1546.001-Change Default File Association	Detects attempts to establish persistence by executing malicious content triggered by a file type association. When a file is opened, the default program used to open the file (also called the file association or handler) is checked. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
SharePoint Activity by Privileged User	Collection T1213.002-Sharepoint	Detects when a file is accessed by a privileged username. You can customize the privileged user account using upper case to the list /All Active Lists/ArcSight Foundation/Common/Privilege User Account.	SharePoint Online	File SharePointFileOperation

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
Odbcconf to Proxy Execution of Malicious Payloads	Defense Evasion T1218.008-Odbcconf	Detects attempts to abuse odbcconf.exe to proxy execution of malicious payloads. Odbcconf.exe is a Windows utility that allows you to configure Open Database Connectivity (ODBC) drivers and data source names. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688
COR_ PROFILER to Hijack Program Execution Flow	Persistence, Privilege Escalation, Defense Evasion T1574.012-COR_ PROFILER	Detects the leveraging of the COR_ PROFILER environment variable to hijack the execution flow of programs that load the .NET CLR. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-PowerShell:4104 Execute a Remote Command

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
AWS S3 Policy Misconfiguration	Collection T1530-Data from Cloud Storage Object	Detects suspicious activity related to AWS S3 policy misconfiguration.	Amazon	Policy:S3 PublicAccessDisabled BucketAnonymousAccessGranted BucketPublicAccessGranted
Signed Binary Proxy Execution	Defense Evasion T1218-Signed Binary Proxy Execution	Detects attempts to bypass process and signature-based defenses by proxying the execution of malicious content with signed binaries. **Windows Note:** To capture the Windows logs, please enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-PowerShell:4104 Execute a Remote Command

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource Description	Log Source	Data Source
AWS S3 Unauthorized Access	Collection T1530-Data from Cloud Storage Object	Detects suspicious activity related to AWS S3 unauthorized access.	Amazon	UnauthorizedAccess:S3 MaliciousIPCaller.Custom TorIPCaller
Credentials in Group Policy Preferences	Credential Access T1552.006-Group Policy Preferences	Detects attempts to find unsecured credentials in Group Policy Preferences (GPP). **Windows Note:** To capture the Windows logs, please enable command-line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing	Microsoft Windows	Microsoft-Windows-Security-Auditing:4688 Microsoft-Windows-Sysmon:1
Mark-of-the-Web Bypass Using PowerShell	Defense Evasion T1553.005-Mark-of-the-Web Bypass	Detects abuse of specific file formats to subvert Mark-of-the-Web (MOTW) controls.	Microsoft Windows	PowerShell:800 Microsoft-Windows-PowerShell:4104 Unblock-File

Threat Intelligence Platform

Displays the out-of-the-box rules from the Threat Intelligence Platform package.

Note: All URLs can be found under All Rules/ArcSight Foundation/Threat Intelligence Platform/.

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
File Hash is related to Sophisticated APT malware or 0-day Activity	Initial Access T1566.002-Spearphishing Link	Detects outbound traffic to suspicious phishing sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Address is related to Sophisticated APT Malware or 0-day Activity	Initial Access T1566.002-Spearphishing Link	Detects outbound traffic to suspicious phishing sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events /All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain
Outbound Communication to a Phishing Address	Initial Access	Detects emails sent to suspicious receivers.	Events with Email address, like Outlook	N/A
Outbound Communication to a Phishing Domain	Initial Access	Detects outbound suspicious DNS queries.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Received Email From Phishing Address	Initial Access	Adds indicator types to a list.	ArcSight Internal Events	activelist:101
Received Email From Malware Address	Exfiltration	Removes indicator types from a list.	ArcSight Internal Events	activelist:102

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Data Transfer over Main Channel to C2 Server	N/A	Detects outbound traffic to suspicious sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Add Additional File Hash To APT Tracking List	N/A	Detects inbound traffic from suspicious sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Inbound Events
Add Suspicious Domain To APT Tracking List	N/A	Detects protected internal company addresses located on a reputation list.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Activate/Core/Common/Network Filters/Boundary Filters/Internal Target
Email Address is related to Sophisticated APT malware or 0-day Activity	N/A	Detects inbound traffic from suspicious sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Inbound Events
Add Suspicious Email To APT Tracking List	N/A	Detects protected internal company domains located on a suspicious list.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Activate/Core/Common/Network Filters/Boundary Filters/Internal Source

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Inbound Suspicious Traffic	N/A	Detects protected internal company addresses on a reputation list.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Activate/Core/Common/Network Filters/Boundary Filters/Internal Source
No Update from GTAP Connector	N/A	Detects outbound traffic to suspicious command and control domains.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events /All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain
Email Sent To Suspicious Address	N/A	Detects outbound traffic to suspicious sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Malware Activity to a Suspicious Domain	Command And Control	Detects outbound traffic to suspicious command and control servers.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Command and Control Outbound Communication on Uncommonly Used Port	N/A	Detects outbound web traffic to suspicious domains.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events /All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain
High Confidence Alerts to Suspicious Source	N/A	Detects suspicious file hash on hosts.	Events with File Hash, like Sysmon	N/A

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
DNS Query to a Suspicious Address	Initial Access	Detects protected internal company domains on suspicious domain lists.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Activate/Core/Common/Network Filters/Boundary Filters/Internal Target
Received Phishing Email With An Attachment	N/A T1486-Data Encrypted for Impact	Detects outbound traffic to suspicious ransomware sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Add Indicator Types	N/A	Detects emails received from suspicious addresses when the indicator types are not listed in the Active List Indicator Types.	Events with Email address, like Outlook	N/A
Remove Indicator Types	N/A	Detects outbound traffic with suspicious URLs.	Proxy Events	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Domain is related to APT Malware Activity	N/A T1486-Data Encrypted for Impact	Detects outbound traffic to suspicious ransomware sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events /All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain
File Hash is related to APT Malware Activity	N/A	Detects outbound web traffic to suspicious addresses.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Outbound Traffic to a Suspicious Domain	Command And Control	Detects outbound suspicious DNS queries.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events /All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain
Command and Control Outbound Communication on Commonly Used Port	N/A T1566.002-Spearphishing Link	Detects email received from a phishing address.	Events with Email address, like Outlook	N/A
Inbound Traffic from a Suspicious Domain	N/A T1566.002-Spearphishing Link	Detects email received from a malware address.	Events with Email address, like Outlook	N/A
High Confidence Alerts with Suspicious File Hash	N/A T1041-Exfiltration Over C2 Channel	Creates correlation events when there is communication to a command and control server over a main channel.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Address /All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Domain
Internal Destination Address Found in Suspicious Address List	N/A	Detects outbound traffic to suspicious malware sites.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events /All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Error in GTAP Connector Service Message	Command And Control T1571-Non-Standard Port	Detects outbound C2 communications over non-standard ports to bypass proxies and firewalls that have been improperly configured.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Domain /All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Address
Command and Control Inbound Communication on Uncommonly Used Port	N/A T1566.001-Spearphishing Attachment	Detects emails received containing attachments from suspicious sources.	Events with Email address, like Outlook	N/A
Inbound Traffic from a Suspicious Address	N/A T1071-Application Layer Protocol	Detects outbound C2 communications over a commonly used port to bypass proxies and firewalls that have been improperly configured.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Address /All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Domain
Internal Source Domain Found in Suspicious Domain List	N/A T1571-Non-Standard Port	Detects inbound C2 communications over non-standard ports to bypass proxies and firewalls that have been improperly configured.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/C2 Inbound Communication from a Suspicious Address /All Filters/ArcSight Foundation/Threat Intelligence Platform/C2 Inbound Communication from a Suspicious Domain

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Email Address is related to APT Malware Activity	N/A T1071-Application Layer Protocol	Detects inbound C2 communications over Commonly used ports to bypass proxies and firewalls that have been improperly configured.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/C2 Inbound Communication from a Suspicious Address /All Filters/ArcSight Foundation/Threat Intelligence Platform/C2 Inbound Communication from a Suspicious Domain
Add Additional URL To APT Tracking List	N/A	Detects outbound traffic to suspicious malware addresses.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Internal Source Address Found in Suspicious Address List	N/A T1048-Exfiltration Over Alternative Protocol	Creates a correlation event when there is communication to command and control servers over alternative protocols.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Address /All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Domain
Command and Control Communication to a Suspicious Domain	N/A T1566.002-Spearphishing Link	Detects emails received from command and control addresses.	Events with Email address, like Outlook	N/A
Outbound Traffic to a Suspicious Address	Command And Control T1092-Communication Through Removable Media	Detects potential Information transfers to removable media over command and control servers.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Rules/Real-time Rules/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Domain

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Command and Control Remote File Copy	N/A T1566.002-Spearphishing Link	Detects emails received from ransomware addresses.	Events with Email address, like Outlook	N/A
Add Additional Email To APT Tracking List	Command And Control T1105-Ingress Tool Transfer	Detects files that might be copied from an external adversary-controlled system through the Command and Control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Command and Control Inbound Communication on Commonly Used Port	N/A	Adds inbound traffic from suspicious addresses to an active list called Suspicious Protocol Tracking. Then it is used by the rule Botnet Activity/Command and Control Multiband Communication.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Inbound Events
Command and Control Communication to a Suspicious Address	N/A T1071.001-Web Protocols	Detects communications between different protocols. This rule is dependent on the rule Botnet Activity/Inbound Suspicious Traffic.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Malware Activity to a Suspicious Address	N/A	Detects file hash in the (additional) suspicious hash active list with threat level high (Sophisticated APT malware or 0-day Activity).	Events with File Hash, like Sysmon	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Hash/File Hash in Suspicious Hash List Sophisticated APT malware or 0-day Related

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Domain is related to Sophisticated APT malware or 0-day Activity	N/A	Detects source or destination addresses on the (additional) suspicious address active list with threat level high (Sophisticated APT malware or 0-day Activity).	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Address/Destination in Suspicious Address List Sophisticated APT malware or 0-day Related /All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Address/Source in Suspicious Address List Sophisticated APT malware or 0-day Related
Add Additional Domain To APT Tracking List	N/A	Adds additional file hash to the APT Tracking list.	Events with File Hash, like Sysmon	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events
Data Transfer over Alternative Protocol to C2 Server	Exfiltration	Adds suspicious domains to the APT Tracking List.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events
Dangerous Browsing to a Suspicious Domain	N/A	Detects email addresses on the (additional) suspicious email active list with threat level high (Sophisticated APT malware or 0-day Activity).	Events with Email address, like Outlook	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Email/Source in Suspicious Email List Sophisticated APT malware or 0-day Related /All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Email/Destination in Suspicious Email List Sophisticated APT Malware or 0-day Related
Suspicious File Hash Activity in Host	N/A	Adds suspicious email addresses to the APT Tracking List.	Events with Email address, like Outlook	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Received Email From A Command And Control Address	Initial Access	Detects domains is in the (additional) suspicious domain active list with threat level medium (APT malware).	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain /All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Domain/Source in Suspicious Domain List APT Malware Related
Potential Information Transfer Through Removable Media Over C2 Communication	Command And Control	Detects file hash on the (additional) suspicious hash active list with threat level medium (APT malware).	Events with File Hash, like Sysmon	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Hash/File Hash in Suspicious Hash List APT Malware Related
Command and Control Multiband Communication	Command And Control	Detects email addresses on the (additional) suspicious email active list with threat level medium (APT malware).	Events with Email address, like Outlook	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Email/Source in Suspicious Email List APT Malware Related /All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Email/Destination in Suspicious Email List APT Malware Related
Received Email From Ransomware Address	Initial Access	Adds additional URLs to the APT Tracking list.	Proxy Events	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events
Add Additional Address To APT Tracking List	N/A	Adds additional email addresses to the APT Tracking List.	Events with Email address, like Outlook	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Add Suspicious Addresses To APT Tracking List	N/A	Detects domains on the(additional) suspicious address active list with threat level high (Sophisticated APT malware or 0-day Activity).	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain /All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Domain/Source in Suspicious Domain List Sophisticated APT malware or 0-day Related
Internal Destination Domain Found in Suspicious Domain List	N/A	Adds the additional domains to the APT Tracking List.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events
Address is related to APT Malware Activity	N/A	Adds the additional addresses to the APT Tracking List.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events
URL is related to APT Malware Activity	N/A	Adds suspicious addresses to the APT Tracking List.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
URL is related to Sophisticated APT malware or 0-day Activity	N/A	Detects source or destination addresses on the (additional) suspicious address active list with threat level medium (APT malware).	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Address/Destination in Suspicious Address List APT Malware Related /All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Address/Source in Suspicious Address List APT Related
Track GTAP Connector Service Message	N/A	Detects URLs on the (additional) suspicious URL active list with threat level medium (APT malware).	Proxy Events	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious URL/URL in Suspicious URL List APT Malware Related
Ransomware Activity to a Suspicious Address	Impact	Detects URLs on the (additional) suspicious URL active list with threat level high (Sophisticated APT malware or 0-day Activity).	Proxy Events	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious URL/URL in Suspicious URL List Sophisticated APT malware or 0-day
Add Suspicious URL To APT Tracking List	N/A	Adds suspicious URLs to the APT Tracking list.	Proxy Events	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events
Possible 0-day Related Activity	N/A	Detects when APT-related indicators are added to the APT Tracking active list and the threat level is high (Sophisticate APT Malware or 0-day) and 0-day, 0day or zero day is the indicatorType.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT Tracking Events
Email Received From Suspicious Address	N/A	Adds suspicious file hash to the APT Tracking list.	Events with File Hash, like Sysmon	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events

Real-time Correlation Rule name	MITRE Tactic and Technique	Resource description	Log Source	Data Source
Add Suspicious File Hash To APT Tracking List	N/A	Detects outbound suspicious traffic with high or very high confidence.	Events with IP or hostname, like firewall, IDS, operating System, or Proxy	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/Outbound Events
Dangerous Browsing to a Suspicious URL	N/A	Detects alerts of suspicious file hash with high or very high confidence.	Events with File Hash, like Sysmon	Correlation /All Rules/Real-time Rules/Threat Intelligence Platform/Suspicious File Hash/Suspicious File Hash Activity in Host
Ransomware Activity to a Suspicious Domain	Impact	Detects entry expirations from the Track GTAP Connector list; which means there is no update from connector for a certain time period (defined by active list TTL).	ArcSight Internal Events	activelist:104 Track GTAP Connector
Dangerous Browsing to a Suspicious Address	N/A	Detects GTAP Connector errors receiving or processing a malicious list.	ArcSight Internal Events	Service message Galaxy Threat Acceleration Program
DNS Query to a Suspicious Domain	N/A	Tracks GTAP Connector service message events and adds them to an active list.	ArcSight Internal Events	N/A
Track GTAP Connector Update Count	N/A	Tracks GTAP connector update counts and adds them to an active list.	ArcSight Internal Events	agent:050

Package Requirements

This package has Real-time Threat Detection and Log Source requirements.

Realt-time Threat Detection Requirements

Requires Real-time Threat Detection 8.0.

Log Source Requirements

This package requires the following log sources:

Log Source	Requirement
AWS Security Hub	ArcSight Security Hub SmartConnector
GTAP	CyberRes Galaxy Threat Acceleration Program 2.0
Linux Audit	ArcSight Linux Audit File SmartConnector
Microsoft Office 365	ArcSight Microsoft 365 Defender SmartConnector
Microsoft Windows	ArcSight Windows Connector SmartConnector

Deployment

The .zip file contains three files:

- package .arb file
- signature .arb file
- Readme

Installation

1. Go to the ArcSight Console.
2. Click **Packages**.
3. Click **Import**.
4. Select the package .arb from the .zip file.
5. Follow the prompts to import and install this package.

Uninstallation Process

Right-click the package from the ArcSight Console, then select **Uninstall Package**.

Verifying the Downloaded Installation Software

Micro Focus provides a digital public key to enable you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

https://support.microfocus.com/kb/doc.php?id=7025140

PublicationStatus

Released: NOT RELEASED

Updated: Wednesday, March 22, 2023

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Real-time Threat Detection Default Content Release Notes (Real-time Threat Detection 4.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!