# SIEM MITRE FiGHT Matrix Monitoring

## Release 26.1

## Contents

# 1 What is OpenText SIEM MITRE FiGHT Matrix?

OpenText SIEM MITRE FiGHT Matrix Monitoring release 26.1 supports the MITRE FiGHT™ framework, that provides a comprehensive knowledge base of adversary Tactics and Techniques specifically tailored for telecom industry. Modeled after the widely recognized MITRE ATT&CK® framework, FiGHT™ helps organizations understand and defend against threats unique to 5G environments. It categorizes techniques as theoretical, proof of concept (PoC), or observed, offering a detailed view of potential attack vectors.

# 2 Why is this important?

As 5G technology continues to expand globally, it introduces new attack surfaces that adversaries will inevitably exploit. By integrating FiGHT support, OpenText empowers our customers to:

- Conduct more effective threat assessments for 5G systems.
- Enable adversarial emulation to test their defenses.
- Identify critical security coverage gaps.
- Inform and optimize cyber investment planning for 5G security.

# 3 What's New?

SIEM MITRE FiGHT Matrix Monitoring release 26.1 includes:

- 51 correlation rules mapped to 29 Techniques across 14 Tactics.
- 3 dashboards for actionable insights
- 1 active channel for real-time monitoring
- 1 report for comprehensive analysis
- 1 use case to accelerate deployment

*Note: The MITRE FiGHT matrix is based on the MITRE ATT&CK framework but operates independently. While the Tactic and Technique IDs may look similar, they are distinct and not interchangeable. If you enable rules from both the MITRE ATT&CK and MITRE FiGHT packages, you may see similar alerts triggered in each because the two packages function separately.*

# 4 Requirements

## 4.1 ESM Requirements

OpenText SIEM MITRE FiGHT  Monitoring 26.1 requires **OpenText Enterprise Security Manager 7.6 or later**, and **default content version 4.8** or above.

## 4.2 Log Source Requirements

| Log Source | Requirement |
|---|---|
| Amazon Web Services | SmartConnector for Amazon Web Services CloudTrail |
| Linux Audit | OpenText Linux Audit File SIEM SmartConnector |

| | |
|---|---|
| Microsoft IIS File | SmartConnector for Microsoft IIS File |
| Microsoft Office 365 | OpenText Microsoft 365 Defender SIEM SmartConnector |
| Microsoft Windows | OpenText Microsoft Windows Connector SIEM SmartConnector |

OpenText SIEM MITRE FiGHT Monitoring 26.1 requires SmartConnectors to catch and provide information about events. Information about the log sources associated with each rule are listed in the Appendix A. You can find the relevant SmartConnector in the SmartConnector Grand List (A-Z).

# 5 How to Get the Package?

The SIEM MITRE FiGHT Monitoring 26.1 content package is now available for download from the OpenText Marketplace. Simply visit the OpenText Marketplace, search for “SIEM MITRE FiGHT Monitoring Package 26.1” and download it to your local drive.

## 5.1 Verifying the Downloaded Software

OpenText Marketplace has a .zip file for the MITRE_ FiGHT_Monitoring_v26.1 release:

- MITRE_ FiGHT_Monitoring_v1.0.arb,
- MITRE_ FiGHT_Monitoring_v1.0.arb.sig,
- Release notes.

Evolving security requirements necessitate renewing certificates used in the signature verification process. OpenText provides a digital public key to enable you to verify that the signed software you received is indeed from OpenText and has not been manipulated in any way by a third party. To ensure successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

Visit the following site for information and instructions:

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

# 6 Installation Steps

Make sure **ESM 7.6 or later** is installed with **Default Content 4.8 or above**.

1. Download the MITRE_ FiGHT_Monitoring_v26.1.zip file.
2. Extract the zipped files.
3. Go to the ESM Console.

4. Click **Packages**.
5. Click **Import**.
6. Select the MITRE_ FiGHT_Monitoring.arb.
7. Follow the prompts to install or update this package.

# Appendix A: Full Rule List

| Rule Name | Tactic (Technique ID) | Description | Rule Path | Data Source |
|---|---|---|---|---|
| Detected SQL Injection | Initial Access, Impact, Collection<br>(FGT1190) | This rule detects SQL Injection attacks targeting application servers through malicious SQL commands in request URLs. Monitors web server activity and IDS alerts for SQL injection patterns. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0009 Collection/FGT1190-Exploit Public-Facing Application/Detected SQL Injection | Web Server Activity Events<br>/Application /IDS/Host/Antivirus<br>/IDS |
| Suspicious Remote System Discovery Commands Entered On Windows | Discovery (FGT1018) | This rule identifies reconnaissance activity through execution of network discovery commands on Windows systems. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0007 Discovery/FGT1018-Remote System Discovery/Suspicious Remote System Discovery Commands Entered On Windows | Microsoft-Windows-Security-Auditing:4688<br>Microsoft-Windows-Sysmon:1<br>PowerShell:800 |
| Suspicious Data Transfer Process Started From Command Line | Command and Control, Exfiltration<br>(FGT1048) | This rule detects suspicious execution of file transfer utilities (ftp, winscp, and bitsadmin) launched from command line rather than through Explorer. Validates that command-line arguments contain actual parameters. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0010 Exfiltration/FGT1048-Exfiltration Over Alternative Protocol/Suspicious Data Transfer Process Started From Command Line | Microsoft-Windows-Security-Auditing:4688<br>Microsoft-Windows-Sysmon:1 |
| Login after Work Hour | Persistence, Initial Access, Privilege Escalation, Defense Evasion (FGT1078) | This rule identifies potentially unauthorized access by detecting successful authentication events occurring outside normal business hours. Monitors for successful login attempts that may indicate compromised credentials or insider threats. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/Login after Work Hour | /Success /Authentication/Verify |

| | | | | |
|---|---|---|---|---|
| Potential Distributed DoS | Impact (FGT1498) | This rule detects Distributed Denial of Service attacks by identifying when a single target receives DoS-categorized events from multiple unique attackers (minimum 4) within a 2-minute window. Aggregates attacks by attacker IP addresses to identify coordinated DDoS campaigns. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0040 Impact/FGT1498-Network Denial of Service/Potential Distributed DoS | /DoS |
| Suspicious Network Tunneling Tool Executed | Command And Control (FGT1572) | This rule detects potential malicious use of network tunneling tools such as nc.exe, ncat.exe, or plink.exe when executed from unexpected or non-standard locations on a host. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0011 Command And Control/FGT1572-Protocol Tunneling/Suspicious Network Tunneling Tool Executed | Microsoft-Windows-Security-Auditing:4688 |
| AWS Brute Force Activity from EC2 Instance | Credential Access (FGT1110.001) | This rule detects brute force attacks originating from AWS EC2 instances by monitoring Amazon SecurityHub findings categorized as 'BruteForce' and 'EC2'. Identifies when compromised cloud instances are used to conduct password guessing attacks. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0006 Credential Access/FGT1110-Brute Force/FGT1110.001-Password Guessing/AWS Brute Force Activity from EC2 Instance | Amazon SecurityHub EC2 |
| AWS Port Scan | Reconnaissance, Discovery (FGT1046) | This rule identifies port scanning and network reconnaissance activities on AWS EC2 instances through Amazon SecurityHub findings categorized as 'Sweep', 'Probe', or 'Scan'. Detects adversaries enumerating services and identifying vulnerabilities in cloud infrastructure. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0043 Reconnaissance/FGT1046-Network Service Discovery/AWS Port Scan | Amazon SecurityHub |
| Removable Device Blocked On Host | Impact (FGT1200) | This rule detects when removable media devices are blocked by security controls on endpoints. Monitors application-level block events for removable storage indicating attempted hardware additions. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0040 Impact/FGT1200-Hardware Additions/Removable Device Blocked On Host | /Host<br>/Found<br>/Success<br>/Application |

| | | | | |
|---|---|---|---|---|
| AWS Root Account Usage | Persistence, Initial Access, Privilege Escalation, Defense Evasion (FGT1078.001) | This rule detects usage of AWS root accounts which should be restricted and monitored. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/FGT1078.001-Default Accounts/AWS Root Account Usage | Amazon SecurityHub |
| Port Forwarding Detected | Command And Control (FGT1090.001) | This rule identifies configuration of port forwarding (port proxying/tunneling) on Windows systems using netsh.exe commands. Detects 'netsh interface portproxy add' commands used to redirect network traffic and establish internal proxies.<br>*Note: To capture the Windows logs, please enable command line auditing in the below policy location paths.*<br>Administrative Templates\System\Audit Process Creation<br>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking<br>*https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing* | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0011 Command and Control/FGT1090-Proxy/FGT1090.001-Internal Proxy/Port Forwarding Detected | Microsoft-Windows-Security-Auditing:4688 |

| | | | | |
|---|---|---|---|---|
| Suspicious RDP Redirection Using TSCON | Discovery, Lateral Movement (FGT1021) | This rule detects RDP session hijacking using the TSCON utility to redirect active or disconnected RDP sessions without credentials. Monitors for 'tscon' commands with '/dest:rdp-tcp' parameter indicating session redirection attempts. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0008 Lateral Movement/FGT1021-Remote Services/Suspicious RDP Redirection Using TSCON | Microsoft-Windows-Security-Auditing:4688<br>Microsoft-Windows-Sysmon:1 |
| AWS Pentest Activity | Privilege Escalation, Persistence, Defense Evasion, Initial Access (FGT1078.004) | This rule identifies when AWS cloud accounts are used with penetration testing tools making unauthorized API requests. Monitors Amazon SecurityHub findings categorized as 'PenTest' indicating potential credential compromise. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/FGT1078.004-Cloud Accounts/AWS Pentest Activity | Amazon SecurityHub |
| Proxy Modification Attempt | Command And Control (FGT1090) | This rule detects attempts to modify system proxy settings using netsh commands ('netsh interface portproxy' or 'netsh winhttp set proxy'). Adversaries modify proxy configurations to route traffic through attacker-controlled infrastructure or bypass network restrictions. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0011 Command and Control/FGT1090-Proxy/Proxy Modification Attempt | Microsoft-Windows-Security-Auditing:4688<br>Microsoft-Windows-Sysmon:1 |
| Default Account Enabled | Persistence, Initial Access, Privilege Escalation, Defense Evasion (FGT1078.001) | This rule alerts when default system accounts are enabled, which poses security risks as these accounts often have known credentials. Monitors Windows Event ID 4722 (user account enabled) and checks against a list of default accounts. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/FGT1078.001-Default Accounts/Default Account Enabled | Microsoft-Windows-Security-Auditing:4722<br>/Authorization/Add<br>/Host/<br>/Success |
| Multiple Unique IDS Events to Same Destination | Impact, Lateral Movement, Discovery (FGT1210) | This rule detects potential attack campaigns by identifying when a single target receives 4 or more unique IDS event types within 30 minutes. Indicates diverse attack techniques being used against the same victim. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0008 Lateral Movement/FGT1210-Exploitation of Remote Services/Multiple Unique IDS Events to Same Destination | /IDS/Network |

| | | | | |
|---|---|---|---|---|
| Detected Format String Attack | Initial Access, Impact, Collection (FGT1190) | This rule identifies format string attacks in web requests or detected by other security devices. Monitors request URLs containing multiple format specifiers (%c, %d, %i) indicating exploitation attempts. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0009 Collection/FGT1190-Exploit Public-Facing Application/Detected Format String Attack | Web Server Activity Events |
| Malicious process Masquerading as Windows Process | Defense Evasion (FGT1036.005) | This rule detects malicious executables masquerading as legitimate Windows system processes by running from non-standard locations. Validates that processes with Windows executable names are NOT running from System32 or SysWOW64 directories. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0005 Defense Evasion/FGT1036-Masquerading/FGT1036.005-Match Legitimate Name or Location/Malicious process Masquerading as Windows Process | Microsoft-Windows-Security-Auditing:4688 |
| Egress Communications with Cleartext Protocol | Command and Control, Exfiltration (FGT1048) | This rule identifies outbound network traffic using cleartext protocols (HTTP, FTP, Telnet) crossing network perimeters, which expose data to interception. Monitors firewalls accept events with cleartext protocols. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0010 Exfiltration/FGT1048-Exfiltration Over Alternative Protocol/Egress Communications with Cleartext Protocol | /Access/Start<br>/Access<br>/Firewall |
| Detected Directory Traversal | Initial Access, Impact, Collection (FGT1190) | This rule detects directory traversal attacks in web applications where attackers attempt to access files outside the web root using path manipulation. Monitors web server logs and IDS alerts for directory traversal patterns. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0009 Collection/FGT1190-Exploit Public-Facing Application/Detected Directory Traversal | Web Server Activity Events |
| Multiple RDP Connections from the Same User in Short Period of Time | Discovery, Lateral Movement (FGT1021) | This rule identifies potential lateral movement by detecting when a single user establishes RDP connections to multiple systems (3+) within a short timeframe (30 minutes). Indicates reconnaissance or propagation of activity across the network. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0008 Lateral Movement/FGT1021-Remote Services/Multiple RDP Connections from the Same User in Short Period of Time | Attacker Host or Address Present<br>Target Host or Address Present |

| | | | | |
|---|---|---|---|---|
| Suspicious Remote System Discovery Commands Entered On Linux | Discovery (FGT1018) | This rule detects network reconnaissance on Linux systems through execution of discovery commands like ifconfig, netstat, route, arp, and nmap. Monitors process execution and command-line arguments for tools used to map network topology. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0007 Discovery/FGT1018-Remote System Discovery/Suspicious Remote System Discovery Commands Entered On Linux | Unix SYSCALL |
| VNC Exploit Execution | Execution, Lateral Movement (FGT1072) | This rule detects exploitation attempts against VNC remote access services. Identifies attacks targeting VNC vulnerabilities to gain unauthorized remote access. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0008 Lateral Movement/FGT1072-Software Deployment Tools/VNC Exploit Execution | /Exploit |
| Suspicious Generative AI Activity | Resource Development (FGT1588) | This rule identifies suspicious interactions with generative AI platforms that may indicate data exfiltration, policy violations, or reconnaissance activities. Monitors web traffic to AI services for anomalous patterns. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0042 Resource Development/FGT1588-Obtain Capabilities/Suspicious Generative AI Activity | /Communicate |
| Exploit of Client Application | Execution (FGT1203) | This rule detects exploitation of client-side applications (like web browsers, Microsoft Office, Adobe Reader and Flash). Monitors for known exploit patterns, malicious file execution, or vulnerability exploitation in client software. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0002 Execution/FGT1203-Exploitation for Client Execution/Exploit of Client Application | Snort /Exploit |
| Suspicious Commonly Used Port Events by Script | Command And Control (FGT1071) | This rule identifies scripting languages (PowerShell, Python, Bash, etc.) making network connections on commonly used ports. Monitors process execution combined with network activity that may indicate malicious scripts. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0011 Command And Control/FGT1071-Application Layer Protocol/Suspicious Commonly Used Port Events by Script | Microsoft-Windows-Sysmon:3 |

| | | | | |
|---|---|---|---|---|
| Detected Code Injection | Initial Access, Impact, Collection (FGT1190) | This rule identifies code injection attacks in web applications including SQL injection, JavaScript injection, and command injection attempts. Monitors web server logs and security device alerts for injection patterns. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0009 Collection/FGT1190-Exploit Public-Facing Application/Detected Code Injection | Web Server Activity Events<br>/Application<br>/IDS/Host/Antivirus<br>/IDS |
| New Self-Signed Certificate Created using PowerShell | Resource Development (FGT1587) | This rule detects the creation of self-signed certificates via PowerShell commands (New-SelfSignedCertificate) used to enable encrypted communications or intercept traffic. Monitors PowerShell Event 800 for certificate creation activity. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0042 Resource Development/FGT1587-Develop Capabilities/New Self-Signed Certificate Created using PowerShell | PowerShell:800 |
| Egress DNS Communications Passed by Firewall | Command and Control, Exfiltration (FGT1048.003) | This rule identifies DNS traffic exiting the network perimeter which could indicate DNS tunneling for data exfiltration or C2 communication. Monitors firewall permit events for outbound DNS (port 53) traffic<br>*Note:This rule is disabled by default, because it can generate excessive log volume if asset modeling for DNS servers is not configured.* | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0010 Exfiltration/FGT1048-Exfiltration Over Alternative Protocol/FGT1048.003-Exfiltration Over Unencrypted Non-C2 Protocol/Egress DNS Communications Passed by Firewall | /Access/Start<br>/Access<br>/Firewall |
| Track MITRE FiGHT Rules triggered | | This rule aggregates all MITRE FiGHT framework rule triggers for comprehensive monitoring and reporting. Collects events with MITRE ID labels to maintain central visibility across the environment. | /All Rules/ArcSight Foundation/MITRE FiGHT/Track MITRE FiGHT Rules triggered | Correlation events |
| Process Executed with Whitespace Special Characters | Defense Evasion (FGT1036.005) | This rule detects processes executed with abnormal whitespace characters in file paths used to bypass security controls.  The following special characters are monitored: U+2000 (En Quad), U+2001 (Em Quad), U+2002 (En Space), and U+200A (Hair Space). | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0005 Defense Evasion/FGT1036-Masquerading/FGT1036.005-Match Legitimate Name or Location/Process Executed with Whitespace Special Characters | Microsoft-Windows-Security-Auditing:4688 |

| | | | | |
|---|---|---|---|---|
| High Severity IDS Event | Impact, Lateral Movement, Discovery (FGT1210) | This rule triggers intrusion detection system events marked as high or very high severity, indicating significant security threats. Provides early warning of serious attacks requiring immediate investigation. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0008 Lateral Movement/FGT1210-Exploitation of Remote Services/High Severity IDS Event | /IDS/Network |
| AWS Account Privilege Escalation Activity | Privilege Escalation, Persistence, Defense Evasion, Initial Access (FGT1078.004) | This rule detects when anomalous API requests associated with privilege escalation activity have been observed from any AWS cloud account. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/FGT1078.004-Cloud Accounts/AWS Account Privilege Escalation Activity | Amazon SecurityHub |
| Suspicious Remote Desktop Protocol | Discovery, Lateral Movement (FGT1021) | This rule identifies suspicious RDP activity including connections from unusual sources, failed authentication attempts, or abnormal RDP session behavior. Monitors for RDP-related security events indicating potential unauthorized access. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0008 Lateral Movement/FGT1021-Remote Services/Suspicious Remote Desktop Protocol | Microsoft-Windows-Security-Auditing:4688<br>Microsoft-Windows-Sysmon:1 |
| Tor Traffic Activity Detected On The Network | Command And Control (FGT1090.003) | This rule detects Tor anonymization of network traffic which may indicate attempts to hide activities or establish covert channels. Identifies Tor protocol patterns, known Tor exit nodes, or Tor-related DNS queries. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0011 Command And Control/FGT1090-Proxy/FGT1090.003-Multi-hop Proxy/Tor Traffic Activity Detected On The Network | /Access/Start<br>/Access<br>/Firewall |
| AWS Impossible Travel | Privilege Escalation, Persistence, Defense Evasion, Initial Access (FGT1078.004) | This rule detects physically impossible travel scenarios where AWS account authentication occurs from geographically distant locations within an impossible timeframe. Indicates compromised credentials being used from multiple locations. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/FGT1078.004-Cloud Accounts/AWS Impossible Travel | Amazon SecurityHub |
| Remote System Discovery | Discovery (FGT1018) | This rule identifies network reconnaissance activities through remote system discovery techniques..<br>*Note 1: To capture the Linux logs, please include the below* | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0007 Discovery/FGT1018-Remote System Discovery/Remote System Discovery | SYSCALL<br>Unix<br>Microsoft-Windows-Security-Auditing:4663 |

| | | | | |
|---|---|---|---|---|
| | | *rules in the audit.rules file in your Linux Machine.*<br>Path: /etc/audit/audit.rules<br>Include the below rules based on the linux architecture:<br>-a exit,always -F arch=b64 -F euid=0 -S execve<br>-a exit,always -F arch=b32 -F euid=0 -S execve<br># For monitoring particular file location, we have to add the below rule to the file<br>-w /etc/hosts -p rwa -k hosts_file_access<br>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.<br>Restart the auditd service once the configuration is completed.<br>*Note 2: 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.*<br>[https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder](https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder)<br>Here, the path to be audited is C:\Windows\System32\Drivers\etc\hosts | | |

| | | | | |
|---|---|---|---|---|
| Successful Brute Force Login | Credential Access (FGT1110) | This rule detects successful authentication following multiple failed login attempts, indicating successful brute force or password guessing attacks. Correlates failed authentications with subsequent success to identify compromised accounts. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0006 Credential Access/FGT1110-Brute Force/Successful Brute Force Login | /Authentication/Verify/Success/Brute Force/Login |
| Hide Artifacts to Evade Detection | Defense Evasion (FGT1564) | This rule identifies attempts to hide files, processes, or artifacts to evade security monitoring. Detects use of hidden file attributes, registry modifications, or rootkit-like behavior. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0005 Defense Evasion/FGT1564-Hide Artifacts/Hide Artifacts to Evade Detection | /IDS/Application/Assessment Tools |
| Account Tampering - Suspicious Failed Logon | Persistence, Initial Access, Privilege Escalation, Defense Evasion (FGT1078) | This rule detects patterns of suspicious failed login attempts that may indicate account enumeration, password spraying, or brute force attacks. Monitors for high volumes of failures, unusual sources, or specific failure patterns. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/Account Tampering - Suspicious Failed Logon | Microsoft-Windows-Security-Auditing:4625<br>Microsoft-Windows-Security-Auditing:4776 |
| Script Executed On Critical Host | Execution (FGT1059) | This rule alerts when scripts (PowerShell, VBScript, JavaScript, Bash, Python) are executed on designated critical systems or servers. Critical assets require heightened monitoring as script execution may indicate compromise. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0002 Execution/FGT1059-Command and Scripting Interpreter/Script Executed On Critical Host | Microsoft-Windows-Security-Auditing:4688<br>Microsoft-Windows-Sysmon:1 |
| Possible Masquerading Detected | Defense Evasion (FGT1036) | This rule identifies potential masquerading where processes or files appear to impersonate legitimate software but exhibit suspicious characteristics. Detects naming anomalies, unusual locations, or behavioral indicators. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0005 Defense Evasion/FGT1036-Masquerading/Possible Masquerading Detected | Microsoft-Windows-Sysmon:7<br>Microsoft-Windows-Sysmon:1 |
| Possible Data Exfiltration | Exfiltration (FGT1041) | This rule detects potential data exfiltration by monitoring large outbound data transfers, unusual protocol usage, or connections to suspicious external destinations. Identifies anomalous data movement patterns. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0010 Exfiltration/FGT1041-Exfiltration Over C2 Channel/Possible Data Exfiltration | Bro<br>Zeek |

| | | | | |
|---|---|---|---|---|
| Changes to Windows Firewall Exception List | Defense Evasion (FGT1562.004) | This rule monitors modifications to Windows Firewall exception rules which adversaries configure to allow malicious traffic.<br>*Note: In order to capture the windows logs, please follow the below steps*<br>In order to audit any policy changes in windows, please enable auditing in the following fields in the group policy editor:<br>Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Policy Change<br>Under the Policy Change fields, there are multiple subcategories. Enable Auditing for the following fields:<br>Audit Filtering Platform Policy Change<br>Audit MPSSVC Rule-Level Policy Change<br>Audit other Policy Change Events<br>Restart the service mpssvc. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0005 Defense Evasion/FGT1562-Impair Defenses/FGT1562.004-Disable or Modify System Firewall/Changes to Windows Firewall Exception List | Microsoft-Windows-Security-Auditing:4948<br>Microsoft-Windows-Security-Auditing:4947<br>Microsoft-Windows-Security-Auditing:4946 |
| Suspicious Network Scanning | Reconnaissance, Discovery (FGT1046) | This rule identifies network scanning activities including port scans, host discovery sweeps, and service enumeration. Detects patterns of probing multiple hosts/ports indicative of reconnaissance. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0043 Reconnaissance/FGT1046-Network Service Discovery/Suspicious Network Scanning | /Recon<br>/IDS |
| AWS Password Policy Changed | Privilege Escalation, Persistence, Defense Evasion, Initial Access (FGT1078.004) | This rule alerts when AWS password policies are modified, potentially weakening security controls | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/FGT1078.004-Cloud Accounts/AWS Password Policy Changed | Amazon SecurityHub |

| | | | | |
|---|---|---|---|---|
| Disable Windows System Firewall | Defense Evasion (FGT1562.004) | This rule detects commands or configurations that disable Windows Firewall, removing a critical defense layer.<br>Note: In order to capture the windows logs, please follow the below steps<br>In order to audit any policy changes in windows, please enable auditing in the following fields in the group policy editor:<br>Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Policy Change<br>Under the Policy Change fields, there are multiple subcategories. Enable Auditing for the following fields:<br>Audit Filtering Platform Policy Change<br>Audit MPSSVC Rule-Level Policy Change<br>Audit other Policy Change Events<br>Restart the service mpssvc. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0005 Defense Evasion/FGT1562-Impair Defenses/FGT1562.004-Disable or Modify System Firewall/Disable Windows System Firewall | Microsoft-Windows-Security-Auditing:4950<br>Microsoft-Windows-Security-Auditing:4688 |
| Exploit Attempt Detected by IDS | Impact, Lateral Movement, Discovery (FGT1210) | This rule triggers on IDS signatures specifically categorized as exploit attempts, indicating active exploitation of vulnerabilities. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0008 Lateral Movement/FGT1210-Exploitation of Remote Services/Exploit Attempt Detected by IDS | /IDS/Network |

| | | | | |
|---|---|---|---|---|
| Brute Force IDS Detected Attempts | Credential Access (FGT1110.001) | This rule identifies brute force and password guessing attempts detected by intrusion detection systems. Correlates IDS alerts categorized as brute force to track credential stuffing and password attacks. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0006 Credential Access/FGT1110-Brute Force/FGT1110.001-Password Guessing/Brute Force IDS Detected Attempts | /Brute Force/Login/IDS |
| Log into Multiple Systems in Short Period | Persistence, Initial Access, Privilege Escalation, Defense Evasion (FGT1078) | This rule detects potentially suspicious behavior where a single account authenticates to multiple systems within a compressed timeframe. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0003 Persistence/FGT1078-Valid Accounts/Log into Multiple Systems in Short Period | /Success/Authentication/Verify |
| Multiple RDP Connections from the Same Host in Short Period of Time | Discovery, Lateral Movement (FGT1021) | This rule identifies potential lateral movement when a single host initiates RDP connections to multiple destinations (3+) within 30 minutes. Indicates reconnaissance, spreading, or propagation activity via remote desktop. | /All Rules/ArcSight Foundation/MITRE FiGHT/TA0008 Lateral Movement/FGT1021-Remote Services/Multiple RDP Connections from the Same Host in Short Period of Time | Attacker Host or Address Present<br>Target Host or Address Present |

## About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on-premises or in the cloud. For more information about OpenText (NASDAQ/TSX: OTEX), visit opentext.com.

**Connect with us:**

Twitter | LinkedIn