OpenText
ArcSight Intelligence SaaS

MITRE ATT&CK Coverage Guide

Document Release Date: Sep 2023

opentext™

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

ArcSight Intelligence MITRE ATT&CK v.9 Framework Coverage

This document outlines the MITRE ATT&CK techniques and their associated tactics that are, in theory, detectable using ArcSight Intelligence if the corresponding behaviors are present in the event data provided to it. The document is organized by tactics then techniques. Each technique covered is listed in a separate section that presents a list of sub-techniques (if applicable), the types of data sources required, and an overview of the behavioral indicators used to detect the technique. Whereas this document lists sub-techniques, analysis of coverage was performed only at the technique level. If a technique with sub-techniques is listed as covered, one or more of its sub-techniques is covered, but not necessarily all of them.

TA0001: Initial Access

Initial Access techniques which are covered.

- T1189: Drive-by Compromise
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1200: Hardware Additions
- T1566: Phishing
- T1091: Replication Through Removable Media
- T1195: Supply Chain Compromise
- T1199: Trusted Relationship
- T1078: Valid Accounts

T1189: Drive-by Compromise

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2

Web Proxy	Rare HTTP method	2
Web Proxy	Rare User Agent	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1190: Exploit Public-Facing Application

Types of Data Sources Required

- Web Proxy
- VPN

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Rare HTTP method	2
Web Proxy	Rare User Agent	2
VPN	Unusual number of successful VPN logins	4
VPN	Unusual number of VPN login attempts	4
VPN	Rare successful VPN login type	1
VPN	Rare failed VPN login type	1

T1133: External Remote Services

Types of Data Sources Required

- VPN

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
VPN	Anomalous working hours/days	2
VPN	Impossible travel	1
VPN	Unusual number of failed VPN logins	4
VPN	Unusual number of successful VPN logins	4
VPN	Unusual number of VPN login attempts	4
VPN	Rare successful VPN login type	1
VPN	Rare failed VPN login type	1
VPN	Login attempts to an unusual number of countries	4
VPN	Rare country	1
VPN	Unusual number of users accessing from a country	1
VPN	Unusual number of IP addresses	4

T1200: Hardware Additions

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Web Proxy	Anomalous working hours/days	2
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4
Web Proxy	Rare OS	2
Web Proxy	Rare device	2

T1566: Phishing

- T1566.001: Spearphishing Attachment
- T1566.002: Spearphishing Link
- T1566.003: Spearphishing via Service

Types of Data Sources Required

- Authentication

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Authentication	Anomalous working hours/days	2
Authentication	Impossible travel	1
Authentication	Unusual number of successful login attempts [per destination]	8
Authentication	Rare login attempt by a user [per destination]	2

T1091: Replication Through Removable Media

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2

Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1195: Supply Chain Compromise

- T1195.001 Compromise Software Dependencies and Development Tools
- T1195.002 Compromise Software Supply Chain
- T1195.003 Compromise Hardware Supply Chain

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2

T1199: Trusted Relationship

Types of Data Sources Required

- Repository
- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Repository, Access	Anomalous working hours/days	2
Repository	Sudden Mooch	1
Repository	Unusual Project Take	1
Repository	Inactive Project Take	1
Access	Rare resource	2
Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2

T1078: Valid Accounts

- T1078.001 Default Accounts
- T1078.002 Domain Accounts
- T1078.003 Local Accounts
- T1078.004 Cloud Accounts

Types of Data Sources Required

- Endpoint
- Authentication
- Access
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Authentication, Access, Web Proxy	Anomalous working hours/days	2
Endpoint, Authentication, Access, Web Proxy	Impossible travel	1
Endpoint	Rare service machine	1
Endpoint	Rare service	2
Authentication	Unusual number of successful login attempts [per destination]	8
Access	Unusually high number of resources being accessed by a user	4
Access	Inactive resources access	1
Access	Rare resource	2
Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2
Access	Unusual number of distinct resources accessed for a neighbourhood	6
Web Proxy	Rare browser	2
Web Proxy	Rare device	2

TA0002: Execution

Execution techniques which are covered.

- T1059: Command and Scripting Interpreter
- T1609: Container Administration Command
- T1610: Deploy Container
- T1203: Exploitation for Client Execution
- T1559: Inter-Process Communication
- T1106: Native API
- T1053: Scheduled Task/Job
- T1129: Shared Modules
- T1072: Software Deployment Tools
- T1569: System Services
- T1204: User Execution
- T1047: Windows Management Instrumentation

T1059: Command and Scripting Interpreter

- T1059.001: PowerShell
- T1059.002: AppleScript
- T1059.003: Windows Command Shell
- T1059.004: Unix Shell
- T1059.005: Visual Basic
- T1059.006: Python
- T1059.007: JavaScript
- T1059.008: Network Device CLI

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1609: Container Administration Command

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4

T1610: Deploy Container

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4

T1203: Exploitation for Client Execution

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Unusual total inbound bytes received	2
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual amount of data accessed	4
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Rare browser	2

T1559: Inter-Process Communication

- T1559.001: Component Object Model
- T1559.002: Dynamic Data Exchange

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1106: Native API

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1053: Scheduled Task/Job

- T1053.001: At (Linux)
- T1053.002: At (Windows)
- T1053.003: Cron

- T1053.004: Launchd [MacOS]
- T1053.005: Scheduled Task
- T1053.006: Systemd Timers
- T1053.007: Container Orchestration Job

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4

T1129: Shared Modules

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1

Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1072: Software Deployment Tools

Types of Data Sources Required

- Repository
- Endpoint
- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Repository	Large, Sudden Unusual Take Action [per project]	4
Repository	Sudden Mooch	1
Repository	Unusual Project Take	1
Repository	Inactive Project Take	1
Repository	Sudden Unusually Large Take	4
Repository	Unusual Number of Accessed Projects	4
Endpoint	Rare process	2
Access	Unusual amount of collections with failed accesses	4
Access	Rare collection to fail to access for a user	1
Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2

T1569: System Services

- T1569.001: Launchctl
- T1569.002: Service Execution

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1204: User Execution

- T1204.001: Malicious Link
- T1204.002: Malicious File
- T1204.003: Malicious Image

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1047: Windows Management Instrumentation

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Unusual total inbound bytes received	2
Endpoint	Rare process	2
Endpoint	Rare service	2

TA0003: Persistence

Persistence techniques which are covered.

- T1098: Account Manipulation
- T1197: BITS Jobs
- T1547: Boot or Logon Autostart Execution
- T1037: Boot or Logon Initialization Scripts
- T1176: Browser Extensions
- T1554: Compromise Client Software Binary
- T1136: Create Account
- T1543: Create or Modify System Process
- T1546 Event Triggered Execution
- T1133: External Remote Services
- T1574: Hijack Execution Flow
- T1525: Implant Internal Image
- T1556: Modify Authentication Process
- T1137: Office Application Startup
- T1542: Pre-OS Boot
- T1053: Scheduled Task/Job
- T1505: Server Software Component
- T1205: Traffic Signaling
- T1078: Valid Accounts

T1098: Account Manipulation

- T1098.001: Additional Cloud Credentials
- T1098.002: Exchange Email Delegate Permissions
- T1098.003: Add Office 365 Global Administrator Role
- T1098.004: SSH Authorized Keys

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Activity from Rare User	1
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4

T1197: BITS Jobs

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Web Proxy	Anomalous working hours/days	2
Endpoint, Web Proxy	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1547: Boot or Logon Autostart Execution

- T1547.001: Registry Run Keys / Startup Folder
- T1547.002: Authentication Package
- T1547.003: Time Providers
- T1547.004: Winlogon Helper DLL
- T1547.005: Security Support Provider
- T1547.006: Kernel Modules and Extensions
- T1547.007: Re-opened Applications
- T1547.008: LSASS Driver
- T1547.009: Shortcut Modification
- T1547.010: Port Monitors
- T1547.011: Plist Modification
- T1547.012: Print Processors
- T1547.013: XDG Autostart Entries
- T1547.014: Active Setup
- T1547.015: Login Items

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2

Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1037: Boot or Logon Initialization Scripts

- T1037.001: Logon Script (Windows)
- T1037.002: Logon Script (Mac)
- T1037.003: Network Logon Script
- T1037.004: RC Scripts
- T1037.005: Startup Items

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1176: Browser Extensions

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1554: Compromise Client Software Binary

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1136: Create Account

- T1136.001: Local Account
- T1136.002: Domain Account
- T1136.003: Cloud Account

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Rare service machine	1
Endpoint	Rare service	2

T1543: Create or Modify System Process

- T1543.001: Launch Agent
- T1543.002: Systemd Service
- T1543.003: Windows Service
- T1543.004: Launch Daemon

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1

Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4

T1546: Event Triggered Execution

- T1546.001: Change Default File Association
- T1546.002: Screensaver
- T1546.003: Windows Management Instrumentation Event Subscription
- T1546.004: Unix Shell Configuration Modification
- T1546.005: Trap
- T1546.006: LC_LOActive Directory_DYLIB Addition
- T1546.007: Netsh Helper DLL
- T1546.008: Accessibility Features
- T1546.009: AppCert DLLs
- T1546.010: AppInit DLLs
- T1546.011: Application Shimming
- T1546.012: Image File Execution Options Injection
- T1546.013: PowerShell Profile
- T1546.014: Emond
- T1546.015: Component Object Model Hijacking

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4

Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1133: External Remote Services

Types of Data Sources Required

- Endpoint
- VPN

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, VPN	Anomalous working hours/days	2
Endpoint, VPN	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Rare service	2
VPN	Unusual number of failed VPN logins	4
VPN	Unusual number of successful VPN logins	4
VPN	Unusual number of VPN login attempts	4
VPN	Rare successful VPN login type	1
VPN	Rare failed VPN login type	1
VPN	Login attempts to an unusual number of countries	4

VPN	Rare country	1
VPN	Unusual number of users accessing from a country	1
VPN	Unusual number of IP addresses	4

T1574: Hijack Execution Flow

- T1574.001: DLL Search Order Hijacking
- T1574.002: DLL Side-Loading
- T1574.004: Dylib Hijacking
- T1574.005: Executable Installer File Permissions Weakness
- T1574.006: Dynamic Linker Hijacking
- T1574.007: Path Interception by PATH Environment Variable
- T1574.008: Path Interception by Search Order Hijacking
- T1574.009: Path Interception by Unquoted Path
- T1574.010: Services File Permissions Weakness
- T1574.011: Services Registry Permissions Weakness
- T1574.012: COR_PROFILER

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1525: Implant Internal Image

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1556: Modify Authentication Process

- T1556.001: Domain Controller Authentication
- T1556.002: Password Filter DLL
- T1556.003: Pluggable Authentication Modules
- T1556.004: Network Device Authentication

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4

Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1137: Office Application Startup

- T1137.001: Office Template Macros
- T1137.002: Office Test
- T1137.003: Outlook Forms
- T1137.004: Outlook Home Page
- T1137.005: Outlook Rules
- T1137.006: Add-ins

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1542: Pre-OS Boot

- T1542.001: System Firmware
- T1542.002: Component Firmware
- T1542.003: Bootkit

- T1542.004: ROMMONkit
- T1542.005: TFTP Boot

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1053: Scheduled Task/Job

- T1053.001: At (Linux)
- T1053.002: At (Windows)
- T1053.003: Cron
- T1053.004: Launchd
- T1053.005: Scheduled Task
- T1053.006: Systemd Timers
- T1053.007: Container Orchestration Job

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4

T1505: Server Software Component

- T1505.001: SQL Stored Procedures
- T1505.002: Transport Agent
- T1505.003: Web Shell
- T1505.004: IIS Components

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1205: Traffic Signaling

- T1205.001: Port Knocking

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Web Proxy	Anomalous working hours/days	2
Endpoint, Web Proxy	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2

T1078: Valid Accounts

- T1078.001: Default Accounts
- T1078.002: Domain Accounts
- T1078.003: Local Accounts
- T1078.004: Cloud Accounts

Types of Data Sources Required

- Endpoint
- Authentication
- Access
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Authentication, Access, Web Proxy	Anomalous working hours/days	2
Endpoint, Authentication, Access, Web Proxy	Impossible travel	1
Endpoint	Rare service machine	1
Endpoint	Rare service	2
Authentication	Unusual number of successful login attempts [per destination]	8
Access	Unusually high number of resources being accessed by a user	4
Access	Inactive resources access	1
Access	Rare resource	2
Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2
Access	Unusual number of distinct resources accessed for a neighbourhood	6
Web Proxy	Rare browser	2
Web Proxy	Rare device	2

TA0004: Privilege Escalation

Privilege Escalation techniques which are covered.

- T1548: Abuse elevation control mechanism
- T1134: Access Token Manipulation
- T1547: Boot or Logon Autostart Execution
- T1037: Boot or Logon Initialization Scripts
- T1543: Create or Modify System Process
- T1546: Event Triggered Execution
- T1574: Hijack Execution Flow
- T1053: Scheduled Task/Job
- T1078: Valid Accounts

T1548: Abuse elevation control mechanism

- T1548.001: Setuid and Setgid
- T1548.002: Bypass User Account Control
- T1548.003: Sudo and Sudo Caching
- T1548.004: Elevated Execution with Prompt

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1134: Access Token Manipulation

- T1134.001: Token Impersonation/Theft
- T1134.002: Create Process with token
- T1134.003: Make and Impersonate tokens
- T1134.004: Parent PID spoofing
- T1134.005: SID-History Injection

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1547: Boot or Logon Autostart Execution

- T1547.001: Registry Run Keys / Startup Folder
- T1547.002: Authentication Package
- T1547.003: Time Providers
- T1547.004: Winlogon Helper DLL
- T1547.005: Security Support Provider
- T1547.006: Kernel Modules and Extensions
- T1547.007: Re-opened Applications
- T1547.008: LSASS Driver
- T1547.009: Shortcut Modification
- T1547.010: Port Monitors
- T1547.011: Plist Modification
- T1547.012: Print Processors
- T1547.013: XDG Autostart Entries

- T1547.014: Active Setup
- T1547.015: Login Items

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1037: Boot or Logon Initialization Scripts

- T1037.001: Logon Script (Windows)
- T1037.002: Logon Script (Mac)
- T1037.003: Network Logon Script
- T1037.004: RC Scripts
- T1037.005: Startup Items

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4

Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1543: Create or Modify System Process

- T1543.001: Launch Agent
- T1543.002: Systemd Service
- T1543.003: Windows Service
- T1543.004: Launch Daemon

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4

T1546: Event Triggered Execution

- T1546.001: Change Default File Association
- T1546.002: Screensaver
- T1546.003: Windows Management Instrumentation Event Subscription
- T1546.004: Unix Shell Configuration Modification

- T1546.005: Trap
- T1546.006: LC_LOActive Directory_DYLIB Addition
- T1546.007: Netsh Helper DLL
- T1546.008: Accessibility Features
- T1546.009: AppCert DLLs
- T1546.010: AppInit DLLs
- T1546.011: Application Shimming
- T1546.012: Image File Execution Options Injection
- T1546.013: PowerShell Profile
- T1546.014: Emond
- T1546.015: Component Object Model Hijacking

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1574: Hijack Execution Flow

- T1574.001: DLL Search Order Hijacking
- T1574.002: DLL Side-Loading
- T1574.004: Dylib Hijacking
- T1574.005: Executable Installer File Permissions Weakness

- T1574.006: Dynamic Linker Hijacking
- T1574.007: Path Interception by PATH Environment Variable
- T1574.008: Path Interception by Search Order Hijacking
- T1574.009: Path Interception by Unquoted Path
- T1574.010: Services File Permissions Weakness
- T1574.011: Services Registry Permissions Weakness
- T1574.012: COR_PROFILER

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1053: Scheduled Task/Job

- T1053.001: At (Linux)
- T1053.002: At (Windows)
- T1053.003: Cron
- T1053.004: Launchd [MacOS]
- T1053.005: Scheduled Task
- T1053.006: Systemd Timers
- T1053.007: Container Orchestration Job

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4

T1078: Valid Accounts

- T1078.001 Default Accounts
- T1078.002 Domain Accounts
- T1078.003 Local Accounts
- T1078.004 Cloud Accounts

Types of Data Sources Required

- Endpoint
- Authentication
- Access
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Authentication, Access, Web Proxy	Anomalous working hours/days	2
Endpoint, Authentication, Access, Web Proxy	Impossible travel	1
Endpoint	Rare service machine	1
Endpoint	Rare service	2
Authentication	Unusual number of successful login attempts [per destination]	8
Access	Unusually high number of resources being accessed by a user	4
Access	Inactive resources access	1
Access	Rare resource	2
Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2
Access	Unusual number of distinct resources accessed for a neighbourhood	6
Web Proxy	Rare browser	2
Web Proxy	Rare device	2

TA0005: Defense Evasion

Defense Evasion techniques which are covered.

- T1548 Abuse Elevation Control Mechanism
- T1134 Access Token Manipulation
- T1197 BITS Jobs
- T1612 Build Image on Host
- T1140 Deobfuscate/Decode Files or Information
- T1610 Deploy Container
- T1006 Direct Volume Access
- T1480 Execution Guardrails
- T1222: File and Directory Permissions Modification
- T1564: Hide Artifacts
- T1574: Hijack Execution Flow
- T1562: Impair Defenses
- T1070: Indicator Removal on Host
- T1202 Indirect Command Execution
- T1036: Masquerading
- T1556: Modify Authentication Process
- T1578: Modify Cloud Compute Infrastructure
- T1112: Modify Registry
- T1601: Modify System Image
- T1599 Network Boundary Bridging
- T1027 Obfuscated Files or Information
- T1207 Rogue Domain Controller
- T1014 Rootkit
- T1216 Signed Script Proxy
- T1553 Subvert Trust Controls
- T1221 Template Injection
- T1205 Traffic Signaling
- T1127 Trusted Developer Utilities Proxy Execution
- T1535 Unused/Unsupported Cloud Regions

- T1550 Use Alternate Authentication Material
- T1078 Valid Accounts
- T1497 Virtualization/Sandbox Evasion
- T1220 XSL Script Processing

T1548: Abuse Elevation Control Mechanism

- T1548.001: Setuid and Setgid
- T1548.002: Bypass User Account Control
- T1548.003: Sudo and Sudo Caching
- T1548.004: Elevated Execution with Prompt

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare service machine	1
Endpoint	Rare service	2

T1134: Access Token Manipulation

- T1134.001: Token Impersonation/Theft
- T1134.002: Create Process with token
- T1134.003: Make and Impersonate tokens
- T1134.004: Parent PID spoofing
- T1134.005: SID-History Injection

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1197: BITS Jobs

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Web Proxy	Anomalous working hours/days	2
Endpoint, Web Proxy	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1612: Build Image on Host

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Unusual total inbound bytes received	2
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual amount of data accessed	4

T1140: Deobfuscate/Decode Files or Information

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1610: Deploy Container

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Unusual number of events of a type	4

T1006: Direct Volume Access

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Rare volume type access	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1480: Execution Guardrails

- T1480.001: Environmental Keying

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1222: File and Directory Permissions Modification

- T1222.001: Windows File and Directory Permissions Modification
- T1222.002: Linux and Mac File and Directory Permissions Modification

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1564: Hide Artifacts

- T1564.001: Hidden Files and Directories
- T1564.002: Hidden Users

- T1564.003: Hidden Window
- T1564.004: NTFS File Attributes
- T1564.005: Hidden File System
- T1564.006: Run Virtual Instance
- T1564.007: VBA Stomping
- T1564.008: Email Hiding Rules
- T1564.009: Resource Forking

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1574: Hijack Execution Flow

- T1574.001: DLL Search Order Hijacking
- T1574.002: DLL Side-Loading
- T1574.004: Dylib Hijacking
- T1574.005: Executable Installer File Permissions Weakness
- T1574.006: Dynamic Linker Hijacking
- T1574.007: Path Interception by PATH Environment Variable
- T1574.008: Path Interception by Search Order Hijacking
- T1574.009: Path Interception by Unquoted Path
- T1574.010: Services File Permissions Weakness
- T1574.011: Services Registry Permissions Weakness
- T1574.012: COR_PROFILER

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1562: Impair Defenses

- T1562.001: Disable or Modify Tools
- T1562.002: Disable Windows Event Logging
- T1562.003: Impair Command History Logging
- T1562.004: Disable or Modify System Firewall
- T1562.006: Indicator Blocking
- T1562.007: Disable or Modify Cloud Firewall
- T1562.008: Disable Cloud Logs
- T1562.009: Safe Mode Boot
- T1562.010: Downgrade Attack

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1070: Indicator Removal on Host

- T1070.001: Clear Windows Event Logs
- T1070.002: Clear Linux or Mac System Logs
- T1070.003: Clear Command History
- T1070.004: File Deletion
- T1070.005: Network Share Connection Removal
- T1070.006: Timestomp

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1202: Indirect Command Execution

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1036: Masquerading

- T1036.001: Invalid Code Signature
- T1036.002: Right-to-Left Override
- T1036.003: Rename System Utilities
- T1036.004: Masquerade Task or Service
- T1036.005: Match Legitimate Name or Location
- T1036.006: Space after Filename
- T1036.007: Double File Extension

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1556: Modify Authentication Process

- T1556.001: Domain Controller Authentication
- T1556.002: Password Filter DLL
- T1556.003: Pluggable Authentication Modules
- T1556.004: Network Device Authentication

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1578: Modify Cloud Compute Infrastructure

- T1578.001: Create Snapshot
- T1578.002: Create Cloud Instance
- T1578.003: Delete Cloud Instance
- T1578.004: Revert Cloud Instance

Types of Data Sources Required

- All

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
all	Anomalous working hours/days	2

T1112: Modify Registry

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1601: Modify System Image

- T1601.001: Patch System Image
- T1601.002: Downgrade System Image

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1599: Network Boundary Bridging

- T1599.001: Network Address Translation Traversal

Types of Data Sources Required

- Web Proxy
- VPN

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy, VPN	Impossible travel	1
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2
Web Proxy	Rare device	2
VPN	Unusual number of failed VPN logins	4
VPN	Unusual number of successful VPN logins	4
VPN	Unusual number of VPN login attempts	4
VPN	Rare successful VPN login type	1
VPN	Rare failed VPN login type	1
VPN	Login attempts to an unusual number of countries	4

VPN	Rare country	1
VPN	Unusual number of users accessing from a country	1
VPN	Unusual number of IP addresses	4

T1027: Obfuscated Files or Information

- T1027.001: Binary Padding
- T1027.002: Software Packing
- T1027.003: Steganography
- T1027.004: Compile After Delivery
- T1027.005: Indicator Removal from Tools
- T1027.006: HTML Smuggling

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1207: Rogue Domain Controller

Types of Data Sources Required

- Authentication

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Authentication	Anomalous working hours/days	2
Authentication	Inactive Destination Access	1

T1014: Rootkit

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2
Endpoint	Rare process	2
Endpoint	Rare service	2

T1216: Signed Script Proxy

- T1216.001: PubPrn

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2
Endpoint	Rare service	2

T1553: Subvert Trust Controls

- T1553.001: Gatekeeper Bypass
- T1553.002: Code Signing
- T1553.003: SIP and Trust Provider Hijacking
- T1553.004: Install Root Certificate
- T1553.005: Mark-of-the-Web Bypass
- T1553.006: Code Signing Policy Modification

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1

T1221: Template Injection

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2
Endpoint	Rare service	2

T1205: Traffic Signaling

T1205.001: Port Knocking

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Web Proxy	Anomalous working hours/days	2
Endpoint, Web Proxy	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2

T1127: Trusted Developer Utilities Proxy Execution

T1127.001: MSBuild

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2

T1535: Unused/Unsupported Cloud Regions

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
all	Impossible travel	1

T1550: Use Alternate Authentication Material

- T1550.001: Application Access Token
- T1550.002: Pass the Hash
- T1550.003: Pass the Ticket
- T1550.004: Web Session Cookie

Types of Data Sources Required

- Endpoint
- Authentication

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Authentication	Rare login attempt by a user [per destination]	2
Authentication	Rare login fail of a specific type [per destination]	2
Authentication	Rare login success of a specific type [per destination]	2

T1078: Valid Accounts

- T1078.001 Default Accounts
- T1078.002 Domain Accounts
- T1078.003 Local Accounts
- T1078.004 Cloud Accounts

Types of Data Sources Required

- Endpoint
- Authentication
- Access
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Authentication, Access, Web Proxy	Anomalous working hours/days	2

Endpoint, Authentication, Access, Web Proxy	Impossible travel	1
Endpoint	Rare service machine	1
Endpoint	Rare service	2
Authentication	Unusual number of successful login attempts [per destination]	8
Access	Unusually high number of resources being accessed by a user	4
Access	Inactive resources access	1
Access	Rare resource	2
Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2
Access	Unusual number of distinct resources accessed for a neighbourhood	6
Web Proxy	Rare browser	2
Web Proxy	Rare device	2

T1497: Virtualization/Sandbox Evasion

- T1497.001: System Checks
- T1497.002: User Activity Based Checks
- T1497.003: Time Based Evasion

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1

T1220: XSL Script Processing

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Rare volume type access	1

TA0006: Credential Access

Credential Access techniques which are covered.

- T1110: Brute Force
- T1555: Credentials from Password Stores
- T1212: Exploitation for Credential Access
- T1606: Forge Web Credentials
- T1056: Input Capture
- T1557: Man-in-the-Middle
- T1556: Modify Authentication Process
- T1040: Network Sniffing
- T1003: OS Credential Dumping
- T1528: Steal Application Access Token
- T1558: Steal or Forge Kerberos Tickets
- T1539: Steal Web Session Cookie
- T1552: Unsecured Credentials

T1110: Brute Force

- T1110.001: Password Guessing
- T1110.002: Password Cracking
- T1110.003: Password Spraying
- T1110.004: Credential Stuffing

Types of Data Sources Required

- Authentication

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Authentication	Anomalous working hours/days	2

Authentication	Unusual number of failed login attempts [per destination]	8
Authentication	Unusual number of login attempts	2
Authentication	Unusual number of login failures	2
Authentication	Unusual number of login attempts to a destination by rare users	2
Authentication	Login attempt to a rare workstation by a user	1
Authentication	Login failure of a specific type to a rare workstation by a user	1
Authentication	Login of a specific type to a rare workstation by a user	1

T1555: Credentials from Password Stores

- T1555.001: Keychain
- T1555.002: Securityd Memory
- T1555.003: Credentials from Web Browsers
- T1555.004: Windows Credential Manager
- T1555.005: Password Managers

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1212: Exploitation for Credential Access

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1606: Forge Web Credentials

- T1606.001: Web Cookies
- T1606.002: SAML Tokens

Types of Data Sources Required

- Authentication

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Authentication	Activity from Rare User	1
Authentication	Unusual number of failed login attempts [per destination]	8
Authentication	Unusual number of successful login attempts [per destination]	8

Authentication	Unusual number of total login attempts [per destination]	8
Authentication	Inactive Destination Access	1
Authentication	Unusual number of destinations with a failed login	2
Authentication	Unusual number of destinations with a successful login	2
Authentication	Unusual number of destinations with a total login	2
Authentication	Rare login attempt by a user [per destination]	2
Authentication	Rare login fail of a specific type [per destination]	2
Authentication	Rare login success of a specific type [per destination]	2
Authentication	Spike in number of users attempting to log into a destination	2
Authentication	Spike in number of users failing to log into a destination	2
Authentication	Unusual number of login attempts	2
Authentication	Unusual number of login failures	2
Authentication	Unusual number of login attempts to a destination by rare users	2
Authentication	Login attempt to a rare workstation by a user	1
Authentication	Login failure of a specific type to a rare workstation by a user	1
Authentication	Login of a specific type to a rare workstation by a user	1

T1056: Input Capture

- T1056.001: Keylogging
- T1056.002: GUI Input Capture
- T1056.003: Web Portal Capture
- T1056.004: Credential API Web Hooking

Types of Data Sources Required

- Endpoint
- Access
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Access	Inactive resources access	1
Access	Unusual number of distinct resources accessed for a neighbourhood	6
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1557: Man-in-the-Middle

- T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay
- T1557.002: ARP Cache Poisoning

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2

Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1556: Modify Authentication Process

- T1556.001: Domain Controller Authentication
- T1556.002: Password Filter DLL
- T1556.003: Pluggable Authentication Modules
- T1556.004: Network Device Authentication

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1040: Network Sniffing

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1003: OS Credential Dumping

- T1003.001: LSASS Memory
- T1003.002: Security Account Manager
- T1003.003: NTDS
- T1003.004: LSA Secrets
- T1003.005: Cached Domain Credentials
- T1003.006: DCSync
- T1003.007: Proc Filesystem
- T1003.008: /etc/passwd and /etc/shadow

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1528: Steal Application Access Token

Types of Data Sources Required

- Authentication

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Authentication	Unusual number of login attempts	2
Authentication	Unusual number of login failures	2
Authentication	Unusual number of login attempts to a destination by rare users	2

T1558: Steal or Forge Kerberos Tickets

- T1558.001: Golden Ticket
- T1558.002: Silver Ticket
- T1558.003: Kerberoasting
- T1558.004: AS-REP Roasting

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1539: Steal Web Session Cookie

Types of Data Sources Required

- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Access	Access by a user to a collection was unusual for his neighbourhood	2
Access	Successful access by a user to a shared resource was unusual for his neighbourhood.	2
Access	Failed access by a user to a collection was unusual for his neighbourhood	2

T1552: Unsecured Credentials

- T1552.001: Credentials in Files
- T1552.002: Credentials in Registry
- T1552.003: Bash History
- T1552.004: Private Keys
- T1552.005: Cloud Instance Metadata API
- T1552.006: Group Policy Preferences
- T1552.007: Container API

Types of Data Sources Required

- Access
- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Access	Access by a user to a collection was unusual for his neighbourhood	2
Access	Successful access by a user to a shared resource was unusual for his neighbourhood.	2
Access	Failed access by a user to a collection was unusual for his neighbourhood	2

TA0007: Discovery

Discovery techniques which are covered.

- T1087: Account Discovery
- T1010: Application Window Discovery
- T1217: Browser Bookmark Discovery
- T1580: Cloud Infrastructure Discovery
- T1538: Cloud Service Dashboard
- T1526: Cloud Service Discovery
- T1613: Container and Resource Discovery
- T1482: Domain Trust Discovery
- T1083: File and Directory Discovery
- T1046: Network Service Scanning
- T1135: Network Share Discovery
- T1040: Network Sniffing
- T1201: Password Policy Discovery
- T1120: Peripheral Device Discovery
- T1069: Permission Groups Discovery
- T1057: Process Discovery
- T1012: Query Registry
- T1018: Remote System Discovery
- T1518: Security Software Discovery
- T1082: System Information Discovery
- T1614: System Location Discovery
- T1016: System Network Configuration Discovery
- T1049: System Network Connections Discovery
- T1033: System Owner/User Discovery
- T1007: System Service Discovery
- T1124: System Time Discovery
- T1497: Virtualization/Sandbox Evasion

T1087: Account Discovery

- T1087.001: Local Account
- T1087.002: Domain Account
- T1087.003: Email Account
- T1087.004: Cloud Account

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1010: Application Window Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1217: Browser Bookmark Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4

T1580: Cloud Infrastructure Discovery

Types of Data Sources Required

- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Access	Anomalous working hours/days	2
Access	Unusually high number of resources being accessed by a user	4
Access	Inactive resources access	1
Access	Rare resource	2

Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2
Access	Unusual number of distinct resources accessed for a neighbourhood	6

T1538: Cloud Service Dashboard

Types of Data Sources Required

- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Access	Anomalous working hours/days	2
Access	Unusually high number of resources being accessed by a user	4
Access	Inactive resources access	1
Access	Rare resource	2
Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2
Access	Unusual number of distinct resources	6

T1526: Cloud Service Discovery

Types of Data Sources Required

- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Access	Anomalous working hours/days	2
Access	Unusually high number of resources being accessed by a user	4
Access	Inactive resources access	1
Access	Rare resource	2
Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2
Access	Unusual number of distinct resources	6

T1613: Container and Resource Discovery

Types of Data Sources Required

- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Access	Anomalous working hours/days	2
Access	Unusually high number of resources being accessed by a user	4
Access	Inactive resources access	1
Access	Rare resource	2

Access	Unusual number of login attempts to a resource by a rare user	2
Access	Unusual number of distinct rare resources accessed	2
Access	Unusual number of distinct resources	6

T1482: Domain Trust Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1083: File and Directory Discovery

Types of Data Sources Required

- Endpoint
- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Access	Anomalous working hours/days	2
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Unusually high number of events of a type	4

Endpoint	Rare process machine	1
Endpoint	Rare process	2
Endpoint	Unusual number of events of a type	4
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4
Access	Unusually high number of resources being accessed by a user	4
Access	Unusual number of distinct resources accessed for a neighbourhood	6

T1046: Network Service Scanning

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Potential victim of a port scan (hour|day)	4
Endpoint	Potential initiator of a port scan (hour|day)	4

T1135: Network Share Discovery

Types of Data Sources Required

- Endpoint
- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Access	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Access	Unusual number of days with a success access by a user across all collections	1
Access	Unusual number of days with a failed access attempt by a user across all collections	1
Access	Unusual number of days with a access attempt by a user across all collections	1
Access	Inactive collection access	1
Access	Unusual amount of collections with access attempts	4
Access	Unusual amount of assessed collections	4
Access	Unusual amount of successful accesses [per destination]	8
Access	Rare collection to attempt an access for a user	1
Access	Rare collection to fail to access for a user	1
Access	Rare collection to access for a user	1
Access	Unusual amount of drives accessed per hour by user compared to their neighbourhood	4
Access	Access by a user to a collection was unusual for his neighbourhood	2
Access	Successful access by a user to a shared resource was unusual for his neighbourhood.	2
Access	Failed access by a user to a collection was unusual for his neighbourhood	2

T1040: Network Sniffing

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1201: Password Policy Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1120: Peripheral Device Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1069: Permission Groups Discovery

- T1069.001: Local Groups
- T1069.002: Domain Groups
- T1069.003: Cloud Groups

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1057: Process Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1012: Query Registry

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1018: Remote System Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1518: Security Software Discovery

- T1518.001: Security Software Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1082: System Information Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2

Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1614: System Location Discovery

- T1614.001 System Language Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1016: System Network Configuration Discovery

- T1016.001: Internet Connection Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1049: System Network Connections Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1033: System Owner/User Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1007: System Service Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1124: System Time Discovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Rare process machine	1
Endpoint	Rare process	2

T1497: Virtualization/Sandbox Evasion

- T1497.001: System Checks
- T1497.002: User Activity Based Checks
- T1497.003: Time Based Evasion

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Anomalous working hours/days	2
Endpoint	Impossible travel	1
Endpoint	Rare process machine	1
Endpoint	Rare process	2

TA0008: Lateral Movement

Lateral Movement techniques which are covered.

- T1210: Exploitation of Remote Services
- T1570: Lateral Tool Transfer
- T1563: Remote Service Session Hijacking
- T1021: Remote Services
- T1091: Replication Through Removable Media
- T1080: Taint Shared Content
- T1550: Use Alternate Authentication Material

T1210: Exploitation of Remote Services

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2

T1570: Lateral Tool Transfer

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1563: Remote Service Session Hijacking

- T1563.001: SSH Hijacking
- T1563.002: RDP Hijacking

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1021: Remote Services

- T1021.001: Desktop Protocol
- T1021.002: SMB/Windows Admin Shares
- T1021.003: Distributed Component Object Model
- T1021.004: SSH
- T1021.005: VNC
- T1021.006: Windows Remote Management

Types of Data Sources Required

- Authentication

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Authentication	Rare login attempt by a user [per destination]	2
Authentication	Rare login fail of a specific type [per destination]	2
Authentication	Rare login success of a specific type [per destination]	2

T1091: Replication Through Removable Media

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1080: Taint Shared Content

Types of Data Sources Required

- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Access	Unusually high number of resources being accessed by a user	4
Access	Unusual number of distinct rare resources accessed	2

T1550: Use Alternate Authentication Material

- T1550.001: Application Access Token
- T1550.002: Pass the Hash
- T1550.003: Pass the Ticket
- T1550.004: Web Session Cookie

Types of Data Sources Required

- Authentication

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Authentication	Rare login attempt by a user [per destination]	2
Authentication	Rare login fail of a specific type [per destination]	2
Authentication	Rare login success of a specific type [per destination]	2

TA0009: Collection

Collection techniques which are covered.

- T1560: Archive Collected Data
- T1123: Audio Capture
- T1119: Automated Collection
- T1115: Clipboard Data
- T1602: Data from Configuration Repository
- T1213: Data from Information Repositories
- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1025: Data from Removable Media
- T1074: Data Staged
- T1114: Email Collection
- T1056: Input Capture
- T1185: Man in the Browser
- T1557: Man-in-the-Middle
- T1113: Screen Capture
- T1125: Video Capture

T1560: Archive Collected Data

- T1560.001 Archive via Utility
- T1560.002 Archive via Library
- T1560.003 Archive via Custom Method

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare volume type access	1
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1123: Audio Capture

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare volume type access	1
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1119: Automated Collection

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Unusual number of events of a type	4
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1115: Clipboard Data

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1

T1602: Data from Configuration Repository

- T1602.001: SNMP (MIB Dump)
- T1602.002: Network Device Configuration Dump

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Potential victim of a port scan (hour|day)	4
Endpoint	Potential initiator of a port scan (hour|day)	4
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1213: Data from Information Repositories

- T1213.001: Confluence
- T1213.002: Sharepoint
- T1213.003: Code Repositories

Types of Data Sources Required

- Repository

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Repository	Large, Sudden Unusual Take Action [per project]	4

Repository	Sudden Mooch	1
Repository	Unusual Project Take	1
Repository	Inactive Project Take	1
Repository	Sudden Unusually Large Take	4
Repository	Unusual Number of Accessed Projects	4

T1005: Data from Local System

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Rare volume type access	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1039: Data from Network Shared Drive

Types of Data Sources Required

- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Access	Unusual number of days with a success access by a user across all collections	1
Access	Unusual number of days with a failed access attempt by a user across all collections	1
Access	Unusual number of days with a access attempt by a user across all collections	1
Access	Inactive collection access	1
Access	Unusual amount of collections with access attempts	4
Access	Unusual amount of collections with failed accesses	4
Access	Unusual amount of assessed collections	4
Access	Unusual amount of successful accesses [per destination]	8
Access	Rare collection to attempt an access for a user	1
Access	Rare collection to fail to access for a user	1
Access	Rare collection to access for a user	1
Access	Unusual amount of access attempts [per destination]	8
Access	Unusual amount of failed accesses [per destination]	8
Access	Unusual amount of drives accessed per hour by user compared to their neighbourhood	4
Access	Access by a user to a collection was unusual for his neighbourhood	2
Access	Failed access by a user to a collection was unusual for his neighbourhood	2

T1025: Data from Removable Media

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Rare volume type access	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process	2
Endpoint	Rare service	2
Endpoint	Unusual number of events of a type	4
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1074: Data Staged

- T1074.001: Local Data Staging
- T1074.002: Remote Data Staging

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Rare volume type access	1
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1114: Email Collection

- T1114.001: Local Email Collection
- T1114.002: Remote Email Collection
- T1114.003: Email Forwarding Rule

Types of Data Sources Required

- Endpoint
- Web Proxy
- VPN

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint, Web Proxy VPN	Impossible travel	1
Endpoint	Unusually high number of events of a type	4
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2
Endpoint	Unusual number of events of a type	4
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
VPN	Unusual number of IP addresses	4

T1056: Input Capture

- T1056.001: Keylogging
- T1056.002: GUI Input Capture

- T1056.003: Web Portal Capture
- T1056.004: Credential API Hooking

Types of Data Sources Required

- Endpoint
- Web Proxy
- Access

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare process	2
Access	Inactive resources access	1
Access	Unusual number of distinct resources accessed for a neighbourhood	6
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1185: Man in the Browser

Types of Data Sources Required

- Endpoint
- Authentication
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Authentication	Unusual number of destinations with a successful login	2
Authentication	Unusual number of destinations with a total login	2
Web Proxy	Rare HTTP method	2

T1557: Man-in-the-Middle

- T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay
- T1557.002: ARP Cache Poisoning

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1113: Screen Capture

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Unusually high number of events of a type	4
Endpoint	Unusual number of events of a type	4
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1125: Video Capture

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1

Endpoint	Unusual number of events of a type	4
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

TA0010: Exfiltration

Exfiltration techniques which are covered.

- T1020: Automated Exfiltration
- T1030: Data Transfer Size Limits
- T1041: Exfiltration Over C2 Channel
- T1029: Scheduled Transfer
- T1048: Exfiltration Over Alternative Protocol

T1020: Automated Exfiltration

- T1020.001: Traffic Duplication

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1030: Data Transfer Size Limits

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1048: Exfiltration Over Alternative Protocol

- T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol
- T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
- T1048.003: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1041: Exfiltration Over C2 Channel

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1029: Scheduled Transfer

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual total inbound bytes received	2
Endpoint	Unusual total outbound bytes sent	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

TA0011: Command and Control

Command and Control techniques which are covered.

- T1071: Application Layer Protocol
- T1092: Communication Through Removable Media
- T1132: Data Encoding
- T1001: Data Obfuscation
- T1573: Encrypted Channel
- T1008: Fallback Channels
- T1105: Ingress Tool Transfer
- T1104: Multi-Stage Channels
- T1095: Non-Application Layer Protocol
- T1571: Non-Standard Port
- T1572: Protocol Tunnelling
- T1090: Proxy
- T1219: Remote Access Software
- T1102: Web Service

T1071: Application Layer Protocol

- T1071.001: Web Protocols
- T1071.002: File Transfer Protocols
- T1071.003: Mail Protocols
- T1071.004: DNS

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Rare HTTP method	2
Web Proxy	Rare User Agent	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2
Web Proxy	Rare OS	2

T1092: Communication Through Removable Media

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual frequency of volume type accessed	2
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1132: Data Encoding

- T1132.001: Standard Encoding
- T1132.002: Non-Standard Encoding

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1001: Data Obfuscation

- T1001.001: Junk Data
- T1001.002: Steganography
- T1001.003: Protocol Impersonation

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2

Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1573: Encrypted Channel

- T1573.001: Symmetric Cryptography
- T1573.002: Asymmetric Cryptography

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2

T1008: Fallback Channels

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1105: Ingress Tool Transfer

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1104: Multi-Stage Channels

Types of Data Sources Required

- Web Proxy
- VPN

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Rare HTTP method	2
VPN	Unusual number of IP addresses	4

T1095: Non-Application Layer Protocol

Types of Data Sources Required

- Web Proxy
- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Potential victim of a port scan (hour|day)	4
Endpoint	Potential initiator of a port scan (hour|day)	4
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1571: Non-Standard Port

Types of Data Sources Required

- Web Proxy
- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Potential victim of a port scan (hour|day)	4
Endpoint	Potential initiator of a port scan (hour|day)	4
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1572: Protocol Tunnelling

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1090: Proxy

- T1090.001: Internal Proxy
- T1090.002: External Proxy
- T1090.003: Multi-hop Proxy
- T1090.004: Domain Fronting

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1219: Remote Access Software

Types of Data Sources Required

- Web Proxy
- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1102: Web Service

- T1102.001: Dead Drop Resolver
- T1102.002: Bidirectional Communication
- T1102.003: One-Way Communication

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

TA0040: Impact

Impact techniques which are covered.

- T1531: Account Access Removal
- T1485: Data Destruction
- T1486: Data Encrypted for Impact
- T1565: Data Manipulation
- T1499: Endpoint Denial of Service
- T1490: Inhibit System Recovery
- T1498: Network Denial of Service
- T1489: Service Stop
- T1529: System Shutdown/Reboot

T1531: Account Access Removal

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process	2

T1485: Data Destruction

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1486: Data Encrypted for Impact

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusually high number of events of a type	4
Endpoint	Rare process	2

T1565: Data Manipulation

- T1565.001: Stored Data Manipulation
- T1565.002: Transmitted Data Manipulation
- T1565.003: Runtime Data Manipulation

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Unusual number of events of a type	4
Endpoint	Unusual frequency of exfiltration	4
Endpoint	Unusual amount of data accessed	4

T1499: Endpoint Denial of Service

- T1499.001: OS Exhaustion Flood
- T1499.002: Service Exhaustion Flood
- T1499.003: Application Exhaustion Flood
- T1499.004: Application or System Exploitation

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Potential victim of a port scan (hour|day)	4
Endpoint	Potential initiator of a port scan (hour|day)	4
Endpoint	Unusual total inbound bytes received	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2

T1490: Inhibit System Recovery

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1498 Network Denial of Service

- T1498.001 Direct Network Flood
- T1498.002 Reflection or Amplification

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Potential victim of a port scan (hour|day)	4
Endpoint	Potential initiator of a port scan (hour|day)	4
Endpoint	Unusual total inbound bytes received	2
Web Proxy	Unusual total inbound bytes transferred from a destination	2

T1489: Service Stop

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

T1529: System Shutdown/Reboot

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process	2

TA0042: Resource Development

Resource Development techniques which are covered:

- T1587: Develop Capabilities
- T1588: Obtain Capabilities
- T1608: Stage Capabilities

T1587: Develop Capabilities

- T1587.001: Malware
- T1587.002: Code Signing Certificates
- T1587.003: Digital Certificates
- T1587.004: Exploits

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1588: Obtain Capabilities

- T1588.001: Malware
- T1588.002: Tool
- T1588.003: Code Signing Certificates
- T1588.004: Digital Certificates
- T1588.005: Exploits
- T1588.006: Vulnerabilities

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1608: Stage Capabilities

- T1608.001: Upload Malware
- T1608.002: Upload Tool
- T1608.003: Install Digital Certificate
- T1608.004: Drive-by Target
- T1608.005: Link Target

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source.

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

TA0043: Reconnaissance

Reconnaissance techniques which are covered:

- T1595: Active Scanning
- T1592: Gather Victim Host Information
- T1589: Gather Victim Identity Information
- T1590: Gather Victim Network Information
- T1598: Phishing for Information
- T1594. Search Victim-Owned Websites

T1595: Active Scanning

- T1595.001: Scanning IP Blocks
- T1595.002: Software

Types of Data Sources Required

- Endpoint
- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source:

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Potential victim of a port scan (hour|day)	4
Endpoint	Potential initiator of a port scan (hour|day)	4
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Rare HTTP method	2
Web Proxy	Rare User Agent	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

Web Proxy	Rare OS	2
Web Proxy	Rare browser	2
Web Proxy	Rare device	2

T1592: Gather Victim Host Information

- T1592.001: Hardware
- T1592.002: Software
- T1592.003: Firmware
- T1592.004: Client Configurations

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source:

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1589: Gather Victim Identity Information

- T1589.001: Credentials
- T1589.002: Email Addresses
- T1589.003: Employee Names

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source:

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1590: Gather Victim Network Information

- T1590.001: Domain Properties
- T1590.002: DNS
- T1590.003: Network Trust Dependencies
- T1590.004: Network Topology
- T1590.005: IP Addresses
- T1590.006: Network Security Appliances

Types of Data Sources Required

- Endpoint

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source:

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Endpoint	Rare process machine	1
Endpoint	Rare service machine	1
Endpoint	Rare process	2
Endpoint	Rare service	2

T1598: Phishing for Information

- T1598.001: Spearphishing Service
- T1598.002: Spearphishing Attachment
- T1598.003: Spearphishing Link

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source:

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total inbound bytes transferred from a destination	2
Web Proxy	Unusual total inbound bytes transferred to a destination	2
Web Proxy	Unusual high total outbound bytes transferred to a rare destination	2

T1594. Search Victim-Owned Websites

Types of Data Sources Required

- Web Proxy

Intelligence Analytics Coverage

The following are the behavioral indicators and the total number of analytical models used to detect them for each type of data source:

Applicable Data Source	Behavioral Indicators	Number of Models used in Detection
Web Proxy	Unusual total outbound bytes transferred per HTTP method	2
Web Proxy	Rare HTTP method	2
Web Proxy	Rare User Agent	2
Web Proxy	Rare OS	2
Web Proxy	Rare browser	2
Web Proxy	Rare device	2

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/

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 MITRE ATT&CK Coverage Guide (Intelligence SaaS 1.0)

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!