

20 September 2019

Forcepoint Public

Forcepoint Insider Threat

Framework

**Table of Contents**

[Introduction 2](#_Toc19879975)

[The Fundamentals 2](#_Toc19879976)

[Defining the “Insider Threat” 3](#_Toc19879977)

[Instituting a Risk-Based Methodology 4](#_Toc19879978)

[Developing the Insider Threat Program Framework 4](#_Toc19879979)

[Implementing Foundational Information Security Controls 5](#_Toc19879980)

[Establishing scenario-driven program objectives and analytic frameworks 6](#_Toc19879981)

[Achieving organizational alignment 7](#_Toc19879982)

[Institutionalizing a Data-Driven Approach to Insider Threat 8](#_Toc19879983)

[Developing Primary Insider Threat Scenarios 9](#_Toc19879984)

[Deploying Analytics-Driven Baseline Insider Threat Models 10](#_Toc19879985)

[Baseline Analytics Controls 11](#_Toc19879986)

[Targeting the Appropriate Feeds and Data Sources 11](#_Toc19879987)

[List of Recommended Audited Events 11](#_Toc19879988)

[Windows Audit Logging Recommendations 13](#_Toc19879989)

[APPENDIX A – Pre-Defined Scenarios, Models and Sources 1](#_Toc19879990)

[APPENDIX B – Pre-Defined Features and Sources 1](#_Toc19879991)

[APPENDIX C – Pre-Defined Models and Scenarios 1](#_Toc19879992)

[Appendix D – Recommended Windows Events ID 1](#_Toc19879993)

Introduction

NIST, the National Institute of Standards and Technology, is among the most widely recognized voices for information security guidance. Specifically, NIST’s Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. **While this guidance was developed initially for federal information systems, it is applicable across most industries, public and private alike** . Among its many controls and recommendations, Revision 4 has introduced the concept of the insider threat, and recognized the need to establish formal controls to tackle this category of organizational risk. In fact, the document provides the following high level guidance with respect to developing specific contingency plans (emphasis added by Forcepoint):

*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*

*The organization coordinates contingency plan development with organizational elements responsible for related plans. Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans,* ***Insider Threat Implementation Plan*** *, and Occupant Emergency Plans.*

*(Source NIST Special Publication 800-53 Revision 4)*

This Forcepoint document provides organizations with a blueprint for implementation of a full spectrum insider threat program. It provides an overview of the fundamentals of insider threat management, initial steps in developing an insider threat program, as well as a detailed catalog of the controls and analytic models required to develop a robust insider threat mitigation program.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

The Fundamentals

As organizations strive to tackle the risk of malicious, negligent, and compromised insiders, it isimportant to understand that the successful insider threat program:

**Creates a CULTURE OF COMPLIANCE:** Openness about oversight and continuous reinforcement of policies will have a positive effect on compliance

**Tailors evaluation of risk to FACTOR IN MOTIVATION:** Identify ways to capture sentiment and behavioral risk indicators

**Achieves ORGANIZATIONAL ALIGNMENT:** Buy-in from C-Suite, HR, physical security, legal, information security, and data owners

**Focuses on HIGH RISK PEOPLE and HIGH VALUE ASSETS:** Identify, through organizational data and analytics, high risk populations (individuals with privileged access to sensitive information) and at-risk corporate assets (information, facilities, people).

To reach this state, organizations must take a deliberate approach to developing a program for responsible oversight of employees, and policy-driven response to potential insider risks. This document will address the following key focus areas:

* Defining the Insider Threat
* Instituting a Risk-Based Methodology
* Developing the Insider Threat Program Framework
* Institutionalizing a Data-Driven Approach to Insider Threat
* Developing Primary Insider Threat Scenarios
* Deploying Baseline Insider Threat Models
* Implementing Standard Insider Threat Controls
* Targeting Appropriate Feeds and Data Sources

Defining the “Insider Threat”

The CERT devision at Carnegie Mellon’s Software Engineering Institute (<https://www.sei.cmu.edu/about/divisions/cert/>) defines the insider threat as follows:

*Current or former employee, contractor, and even business partner who has or had access to an organization’s system, network, or data. The insider has intentionally exceeded or used that access in a manner that typically negatively affected the confidentiality, integrity, or the availability of the organization’s information or information system.*

This provides a broad basis to include anyone across the “extended enterprise” who has had some form of access to the digital assets of the organization, and focuses in on intentional actions to perform harm.

Also, to reinforce CERT’s point on “intentional” damage, there are three basic categories of “damaging” actors that should be targeted by an insider program:

|  |  |  |
| --- | --- | --- |
| **Malicious**  Intent/Motivation  Psychology indicators  Environment triggers | **Negligent**  Sloppiness  Non-compliance  Poos controls | **Compromised**  “Partly” normal  Normal psychology  Specific anomalies |

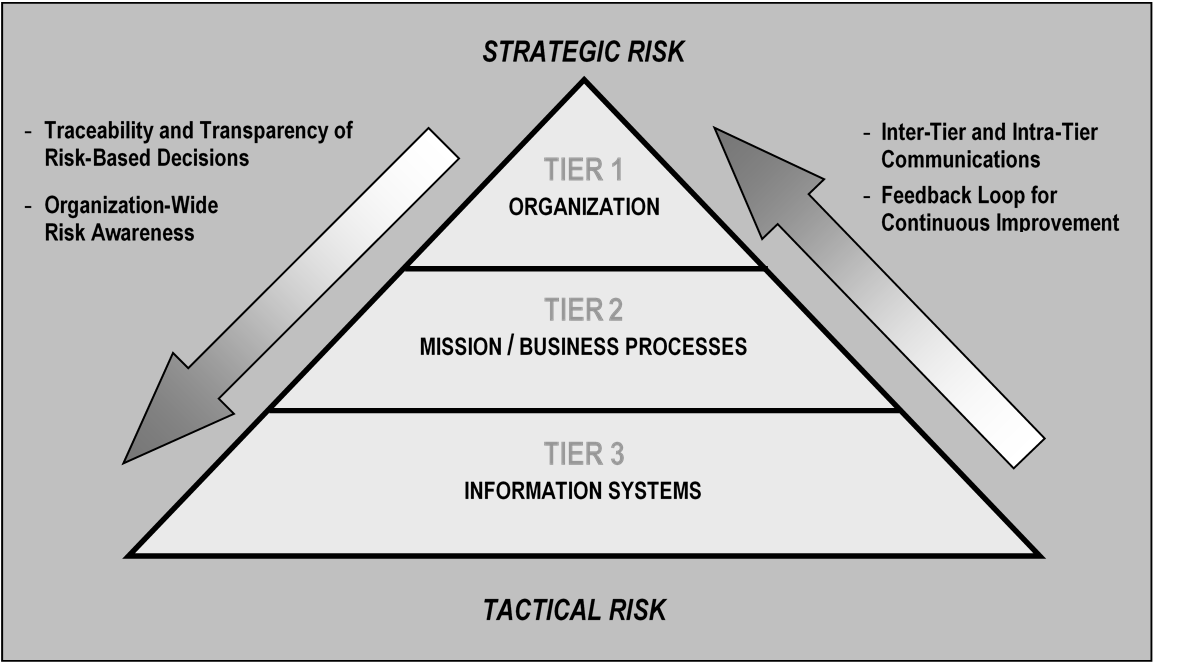
Forcepoint defines malicious activity as that for which there is intent to do harm, often reinforced and exacerbated (but not necessarily) by underlying psychologic factors and affected by environmental triggers. This differs from non-malicious, accidental activity, and even from “compromised” situations in which a malicious outsider asquerades as an insider.

There is significant reason to pay close attention to all three use actor scenarios. Of note, there is an increasingly strong voice of analysts who believe that non-malicious sloppiness, left unchecked, can “lead” people into malicious situations because they believe it highly unlikely to be caught in nefarious acts. **This suggests that providing a response/feedback mechanism to discover non-malicious and potentially compromised activities should be a cornerstone of any program.**

Instituting a Risk-Based Methodology

NIST Special Publication 800-53 rev 4 outlines a risk-based methodology for implementing security and privacy controls. This methodology, quoted below, is equally relevant to the development of an insider threat program:

*The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program for the management of risk—that is, the risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation of information systems. Risk-based approaches to security control selection and specification consider effectiveness, efficiency, and constraints due to applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines. To integrate the risk management process throughout the organization and more effectively address mission/business concerns, a three-tiered approach is employed that addresses risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. The risk management process is carried out across the three tiers with the overall objective of continuous improvement in the organization’s risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization.*



**FIGURE 1 – THREE-TIERED RISK MANAGEMENT APPROACH**

Developing the Insider Threat Program Framework

When developing the blueprint for an insider threat program, organizations must first consider how closely this risk management approach applies to this domain:

**Tier 1: Organization**

*Privileged insiders* – those from whom the insider risk originates, including executives, engineers, contractors, etc.

**Tier 2: Mission/Business Processes**

*Critical assets* – the ‘crown jewels’ against which the insider threat must be mitigated.

**Tier 3: Information Systems**

*Insider threat pathways* – the critical network and electronic resources insiders exploit to gain access to their objectives and carry out their plans. These pathways provide the raw data required to build a comprehensive insider threat analytics program.

Based on these concepts, an organization has the fundamental drivers to develop a comprehensive plan that should focus on:

* Implementing foundational information security controls (e.g. NIST 800-53)
* Establishing scenario-driven program objectives and analytic frameworks
* Achieving organizational alignment

Implementing Foundational Information Security Controls

Before an organization can develop an effective Insider Threat Program, it must first have instituted a comprehensive baseline set of information security controls and processes. Forcepoint urges organizations to consider basing this fundamental capability on the controls detailed in NIST Special Publication 800-53 rev 4 . In addition to identifying the critical controls of information security, it is important for organizations seeking to implement an insider threat program to pay special attention to NIST’s high level guidance on Insider Threat Program development:

*PM-12 INSIDER THREAT PROGRAM*

*Control: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.*

*Supplemental Guidance: Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems.*

*Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program.* ***In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture****.*

*Insider threat programs* ***can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and othercolleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines.***

(Source NIST Special Publication 800-53 Revision 4)

While NIST’s guidance is specifically written for federal agencies dealing in classified information, this is equally relevant to commercial organizations who handle, process, and store any form of proprietary and sensitive information, including:

* Proprietary intellectual property, such as design schemes, source code, etc.
* Materially non-public information (MNPI), such as mergers and acquisitions plans, cash flow projections, impending regulatory approvals, etc., which can be used for the purposes of insider trading.
* Client data, specifically Personally Identifiable Information (PII) such as social security numbers, dates of birth, financial details, etc.
* Patient data, specifically Protected Health Information (PHI) such as health status, provision of health care, or payment for health care.

Establishing scenario-driven program objectives and analytic frameworks

Two critical initial exercises must be undertaken in order to develop a scenario-driven foundation for

a successful insider threat program:

1. **Critical asset identification:** The starting point for a risk-based approach is the identification and prioritization of the assets upon which an organization’s success depends. These might include:
2. People (e.g. key engineers, executives)
3. Engineering plans
4. Source code
5. Client or patient information
6. Financial information
7. **Threat actor persona development:** An organization must take stock of its employee (and non-employee) population, and make initial judgements on potential sources of risk. These might include:
8. Privileged systems administrators
9. Software engineers with elevated access to source code
10. Executives with access to non-public financial data
11. Supply chain participants (such as sub-contractors or off-shore development teams) with access to network resources and proprietary information

Once the threat actor and critical asset landscape has been assessed, an organization can move into developing a framework to measure potential risk. Forcepoint has drawn from, and extended, a common homeland security-related risk framework that originally talked about “Risk” as a function of:

**THREAT \* EXPOSURE \* VULNERABILITY**

In other words, the potential damage of an insider attack vector (or any attack, for that matter) can be measured by the potential damage of that attack, the amount of firm-wide exposure that exists, and how vulnerable each of those exposure points actually is to the attack vector. However, this should be extended in two ways — first, it should be reinforced that resilience is a critical denominator — systems that are fault-tolerant, by design, can withstand being degraded or damaged because another is ready to take its place. Second, in the digital age, it must be asserted that detectability is also important - especially in light of increasingly complex, long-term embedded threat scenarios. Increasing visibility of digital activity, especially in the detection of anomalous activities and behaviors, even when small, is a large component of this, and is a key takeaway of this analysis.

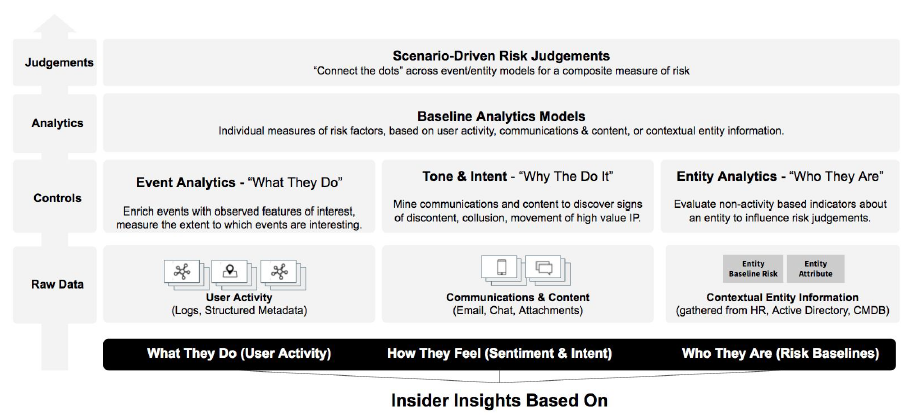
Achieving organizational alignment

No insider threat program can be successful without the full backing and awareness of critical parts of the organization. This comes down to the following essential requirements:

* Achieving cross-functional buy-in from all decision-making parts of the organization, including executive leadership/C-suite, human resources, legal/privacy, information security, and physical security.
* Identifying key organizational stakeholders (and ensuring a well-defined information and decision making flow across those stakeholders)
* Assigning a dedicated, compartmentalized analytic team
* Developing a well documented investigation and response framework, which incorporates the needs of cross-functional stakeholders such as HR, legal, SOC, etc.
* Tying success to measurable indicators of progress (for instance, starting with quantifiably improved adherence to corporate policies governing information use)

Institutionalizing a Data-Driven Approach to Insider Threat

In order to develop a comprehensive, full spectrum program for discovery of insider threat, it is important for organizations to develop a strong foundation of data collection, implement a standardized library of auditable controls, implement robust analytics, and form data-driven risk judgements.



As illustrated above, it begins by focusing on the right kinds of raw data collection that will form the foundation for beginning to understand the following key components of insider behaviors:

* **What they do:** User activity, such as entering facilities, authenticating into sensitive systems, visiting websites, printing files, copying files to portable storage devices, etc.
* **How they feel:** Mining communications and content for signs of sentiment and intent. This might include increasing patterns of abusive communications, signs of withdrawal or collusion, and unusual usage of business sensitive or confidential keywords.
* **What they are:** In addition to user activity and communications (which represent actions with specific temporal qualities), contextual entity information such as organizational data, performance data, derogatory history (IT, HR violations), provide a foundation for assessing which actors are more likely to engage in risky and illicit behavior.

Specific recommended types of data collection are detailed below, by Collection Group. The “Requirement Level” distinguishes between the data sources that are essential to a day one capability, versus those that are important to an enhanced insider threat capability.

|  |  |  |  |
| --- | --- | --- | --- |
| **Collection Group** | **Data Collection Type** | **Typical Source** | **Requirement Level** |
| User Activity | Authentication | Windows, Endpoint Logs | Baseline |
| VPN Authentication | VPN Logs |
| Web Activity | Proxy Logs, Endpoint Logs |
| File Operations | Windows Logs, Endpoint Logs |
| Print Activities | Windows Logs, Endpoint Logs |
| Account Management | Windows Logs |
| System Administration | Windows Logs |
| Email Activity | Exchange, Office 365, Archiver extract, Endpoint Logs |  |
| Process Activity | Windows Logs, Endpoint Logs | Supplemental |
| Physical Badge Access | Badge Access Logs |
| DLP Alerts | DLP Logs |
| Malware Alerts | Malware Logs |
| Financial Transaction Alerts | Transaction Logs |
| Contextual Entity Information | Identifiers (user ID, email, name...) | Active Directory, CMDB, CRM | Baseline |
| Title / Role | Active Directory, Employee DB |
| Business Unit | Active Directory, Employee DB |
| Office Location | Active Directory, Employee DB |
| Supervisor | Active Directory, Employee DB |
| Performance Ratings | Human Resources (i.e. Workday) | Supplemental |
| Promotion/Bonus History | Human Resources (i.e. Workday) |
| Non-compliance History | Human Resources (i.e. Workday) |
| Public Records - Financial | 3rd Party (i.e. Thomson Reuters) |
| Public Records - Criminal | 3rd Party (i.e. Thomson Reuters) |
| Communications & Content | Email | Exchange, Office 365, Archiver extract | Supplemental |
| Corporate Chat | Exchange, Office 365, Archiver extract |
| Transcribed Voice | 3rd Party (i.e. Veritn) |
| Files/Attachments (PDFs, Word, etc.) | Varied |

**Some data collection types should be considered critical for deploying an initial, effective insider threat program. These are assigned a “Baseline” requirement level. These sources should always be targeted for an effective day one capability.**

Other collection types above are listed as “Supplemental”, indicating that for many organizations they are not critical for day one success, and for some organizations, particular supplemental data sources may prove challenging for day one organizational buy-in. For example, communications data such as email and chat can introduce privacy and legal hurdles for some organizations.

Developing Primary Insider Threat Scenarios

While each organization faces its own unique risks, it is important to build a solid foundation for insider threat mitigation based on generalized, baseline scenarios that span organizations of all types and sizes. By adequately implementing controls and policies tied to the following scenarios, most organizations will have put in place a program that covers the vast majority of insider risk:

|  |  |
| --- | --- |
| **Scenario** | **Description** |
| **Data Exfiltration (DE)** | Individuals engaged in illicit attempts to discover, gather, obfuscate, exfiltrate sensitive and/or classified data, and remove all auditable traces of the exfiltration event. |
| **Malicious User (MU)** | Typically disgruntled, privileged users who are attempting to inflict virtual orphysical harm to an organization’s infrastructure through malicious, intentional acts of sabotage. This might include, for examples, attempts to compromise an organization’s internal computer network, or to disrupt the operations of critical physical control systems. |
| **Compromised User (CU)** | Individuals whose credentials have been taken over by malicious, third party actors, and whose network identities are used surreptitiously to cause significant harm to an organization’s security. |
| **Negative Workplace Behavior (NB)** | Individuals in violation of corporate policy for an array of reasons, such as workplace violence, sexual harassment, corporate espionage, whistleblowing, and at risk of leaving. |
| **Illicit Workplace Behavior (IB)** | Individuals putting the corporation at risk through unlawful behaviors, such as insider trading, espionage, market manipulation, organizational conflict of interests (OCI), legal malpractice, and PII leakage. |

These scenarios provide logical groupings of the following analytic models and underlying controls.

As such, the two letter code associated with each Scenario (DE, MU, CU, NB, IB) serves as the prefix for the controls and models that are most closely associated with that Scenario.

Deploying Analytics-Driven Baseline Insider Threat Models

Insider Threat Scenarios constitute multi-faceted combinations of risk indicators and user behaviors. These might include collections of User Activity, Communications & Content, and Contextual Entity Information.

Forcepoint has developed baseline insider threat models, which when deployed on combination can deliver a more complete view of the high level Insider Threat Scenarios. The list of pre-defined Models and Scenarios is included in Appendix C.

The implementation of these models requires first and foremost, a data processing capability that can enforce the baseline analytics controls described below. On top of that, this approach entails a data analytics capability that can apply combinations of scoring techniques including:

* Basic counting of specific families of flagged events
* Identifying highest individual scoring events of certain types, based on the severity and combinations of controls triggered by those events.
* Identifying highest aggregate scoring event sets of certain types, based on the severity and combinations of controls triggered by those events.
* Calculating max and sums of specific attributes (like file sizes, pages printed, session durations) of specific families of events, identified by the characteristics of those events and the types of controls triggered by events.
* Calculating outlier behaviors (e.g. unusual deviations from the norm) of specific patterns of activity, as identified by certain families and types of events.

Baseline Analytics Controls

In order to successfully implement the above Baseline Analytics Models, Forcepoint has identified the critical set of baseline analytic controls (also referred to as event features), which must be configured in order to detect fundamental activity-based signals in user activity, communications, and content data.

All organizations, in the course of their self-assessment, should consider what additional controls are needed based on anticipated threat actors and identified critical assets, however, these baseline controls provide the necessary starting point for analysis. The list of pre-defined Features is included in Appendix B.

Targeting the Appropriate Feeds and Data Sources

Forcepoint UEBA has produced detailed insider threat audit guidance, known as the Forcepoint UEBA Audit Guidance (Forcepoint UEBA AG). The overarching objective of the Forcepoint UEBA AG is to provide our clients with a baseline set of auditable events and their corresponding use cases to incorporate into their insider threat mission. Forcepoint UEBA AG is the culmination of numerous insider threat compliance requirements, insider threat domain expertise, and the latest industry trends from an incident perspective; much of which is based on federal, intelligence community guidelines (including Intelligence Community Standard 500-27).

List of Recommended Audited Events

|  |  |
| --- | --- |
| Account Management | * User Management Events (Success & Failure)   + User Create   + User Delete   + User Modify   + User Lock   + User Enable   + User Disable * Group Management Events (Success & Failure)   + Group Create   + Group Delete   + Group Modify |
| Authentication | * Logons (Success & Failure)   + Local Logon   + Remote Logon   + Cached Logon   + Network Logon   + Privileged Logon * Logoffs (Success & Failure) |
| Web | * Web Downloads * Web Uploads * Web Searches |
| Email | * Email Sent * Email Received |
| Data Movement | * Data Exfiltration (Success & Failure)   + Upload to External Media (USB, CDRW)   + Print to FIle   + Print to Device   + Upload to Web   + Download from Corporate Web (SharePoint, GitHub, Proprietary Applications) * Data Infiltration (Success & Failure)   + Download from External Media   + Download from Web * Data Transfer (Success & Failure)   + Network Transfer |
| File Operation | * File Operation (Success & Failure)   + File Created   + File Accessed   + File Share Accessed   + File Deleted   + File Modified     - File Moved     - File Write     - File Renamed     - File Permission Modification     - File Ownership Modification   + File Search   + File Compression   + File Encryption |
| Malware | * Malware Status (Success & Failure)   + Malicious Code Detection   + Malicious Code Removal   + Malicious Code On-Demand Scan (Non-Scheduled Scans) |
| Physical | * Physical Access   + Badge Access * System Management (Success & Failure)   + System Reboot   + System Shutdown   + System Restart |
| Process | * Application Status (Success & Failure)   + Application Starts     - Privileged Escalation ("Run As Admin")   + Application Stops * Command Line Interaction (Success & Failure) |
| Systems Administration | * Admin Activity (Success & Failure)   + Disabling the Auditing Mechanism   + Audit Log Data Access * System Changes (Success & Failure)   + Audit Policy Changes   + Security Policy Changes   + Configuration Changes   + Registry Changes |

Windows Audit Logging Recommendations

Specifically, with respect to Windows Audit Logging, Forcepoint UEBA recommends the logging and analysis of the Windows Event Codes included in the Appendix D. These event types maximize the full potential of Forcepoint UEBA to help organizations detect the widest variety of insider threats.

APPENDIX A – Pre-Defined Scenarios, Models and Sources

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Data Exfiltration (DE)** | **Compromised User (CU)** | **Malicious User (MU)** | **Negative Behaviour (NB)** | **Illicit Behaviour (IB)** |
| **Models** | DE1A Internal Data Movement (Volumetric)  DE1B Internal Data Movement (Features)  DE2A External Data Movement (Volumetric)  DE2B External Data Movement (Features)  DE3 Email Data Movement  DE4 File Operations  DE5 File Share Cardinality  DE6 Data Reconnaissance  DE7 Data Loss (DLP) | CU1 Malware Threat  CU2 AntiVirus Match  CU3 Remote Logon  CU4 Source Country Cardinality  CU5 Phishing  CU6 Negligent Browsing  CU7 Configuration Deviation  CU8 Redirected Internet Traffic  CU9 Port Cardinality  CU10 Destination IP Cardinality | MU1 Network Reconnaissance  MU2 Systems Administration  MU3 Malicious Authentication  MU4 Destination Cardinality  MU5 Explicit Account Cardinality  MU6 Authenticated Process Cardinality  MU7 Process Activity  MU8 Malicious Research  MU9 Configuration Deviation  MU10 Physical Access  MU11 Access Request  MU12 Account Management  MU-13 Core System Components | NB1 Sexual Harassment  NB2 Workplace Violence  NB3 Obscene Content  NB4A Flight Risk Comms  NB4B Flight Risk Web  NB5 Decreased Productivity  NB6A Corporate Disengagement  NB6B Recipient Cardinality  NB7A Financial Distress Comms  NB7B Financial Distress Web  NB8 Negative Sentiment  NB9 Oversight Evasion  NB10 IT Oversight Evasion | IB1 Espionage  IB2 Corporate Espionage  IB4 Clearance Evasion |
| **Data Sources** | Web  Email (metadata or full body)  Windows/Linux Processes  Windows/Linux File Operations  DLP (Native integration with Forcepoint DLP)  Endpoint Monitoring (FIT) | Anti-Malware  Web  Email (metadata or full body)  Next-Gen Firewall (Users)  VPN Logs  Windows/Linux Processes  Endpoint Monitoring (FIT) | Windows/Linux Authentication  Windows/Linux System Administration  Windows/Linux Account Management  Windows/Linux Processes  Windows/Linux File Operations  Next-Gen Firewall (Users)  Endpoint Monitoring (FIT)  Email/Chat (full body) | Web  Email/Chat (full body)  Windows/Linux System Administration  Endpoint Monitoring (FIT) | Email/Chat (full body)  Web  Endpoint Monitoring (FIT) |

APPENDIX B – Pre-Defined Features and Sources

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scenario (Collection)** | **Event Feature (Feature)** | **Feature Description** | **Type** | **Modes** | **Logs** |
| **Data Exfiltration (DE)** | **Internal Site Download  DE-1.1** | Download corporate files from internal company sites, such as Confluence or SharePoint. | Advanced | Web (Gets from Internal Sites) Data Movement (Web Servers, Web Repositories logs) | Web: Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) Data Movement: Internal Web Services Logs |
| **File Copy DE-1.2** | File copy activity, where the data is remaining inside the company network. | Advanced | File Operations | Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) |
| **File Copy File Share  DE-1.2.1** | Copying files from a file share. | Advanced | File Operations | Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) |
| **File Copy Remote Desktop  DE-1.2.2** | Copying files from a remote resource during a remote desktop session. | Advanced | File Operations | Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) |
| **File Copy Command Line  DE-1.2.3** | Copying files via command line. | Advanced | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Move DE-1.3** | Moving files within the company network. | Advanced | File Operations Processes | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Cloud Storage Upload  DE-2.1** | Uploading Content in a Cloud Storage Website | Advanced | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Print Activity  DE-2.2** | Printing documents. | Advanced | Data Movement (Print Logs) | Windows Events (307) and Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Print) |
| **USB Transfer  DE-2.3** | Transferring files to a USB drive. | Advanced | Data Movement (Removable Media) | Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) |
| **CD/DVD Burn DE-2.4** | Burning company files to a CD/DVD. | Advanced | Data Movement (Removable Media) | Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) |
| **Email to External Domain  DE-3.1** | Emails to non-internal domains with an attachment. | Advanced/Lexicon | Email (metadata or full body) | Mail Server or Email Gateway |
| **File Access DE-4.1** | Opening company files. | Advanced | File Operations Processes | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Compression  DE-4.2** | Compressing a file or directory. | Advanced | File Operations Processes | File Operations: Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Delete DE-4.3** | Deleting company files. | Advanced | File Operations Processes | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Encryption  DE-4.4** | Encyrpting a file. | Advanced | File Operations Processes | File Operations: Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Modification DE-4.5** | Modifying company files. | Advanced | File Operations Processes | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Rename  DE-4.6** | Renaming a file. | Advanced | File Operations Processes | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Share Access DE-4.7** | Accessing a file share, only listing its contents. | Advanced | File Operations Processes | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Decompression DE-4.8** | Files being unarchived or decompressed. | Advanced | File Operations Processes | File Operations: Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Search  DE-6.1** | Searching for confidential files, via Windows Explorer or command line. | Advanced/Lexicon | File Operations Processes | File Operations: Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **File Properties Check DE-6.2** | Checking the file size, permissions, and other metadata . | Advanced | File Operations Processes | File Operations: Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) Processes: Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Data Reconnaissance Process  DE-6.3** | Running a data searching process. | Advanced/Lexicon | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **DLP Print Alert  DE-7.1** | Printing documents that contain PII information, such as SSNs, Credit Card numbers, etc. | Advanced | Data Leakage | DLP Solution |
| **DLP Upload Alert  DE-7.2** | Uploading docuemnts to the web that contain PII information, such as SSNs, Credit Card numbers, etc. | Advanced | Data Leakage | DLP Solution |
| **DLP Email Alert  DE-7.3** | Emailing docuemnts that contain PII information, such as SSNs, Credit Card numbers, etc. | Advanced | Data Leakage | DLP Solution |
| **DLP Transfer Alert  DE-7.4** | Transferring files to a USB drive Emailing docuemnts that contain. | Advanced | Data Leakage | DLP Solution |
| **DLP Matches DE-7.5** | The number of DLP findings in a given document. | Numeric Field | Data Leakage | DLP Solution |
| **Malicious User (MU)** | **Network Reconnaissance Process  MU-1.1** | Initializing a process that maps and discovers assets on the network. | Advanced/Lexicon | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Network Reconnaissance Port  MU-1.2** | Port activity for network reconnasiance activity. | Advanced/Lexicon | Network | Next-Gen Firewall (User) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Firewall) |
| **Audit Policy Change  MU-2.1** | Making changes to the system audit policy, such as auditd or advance audit policies. | Advanced | System Administration | System Administration:Windows Events (1102, 1074, 4657, 4674, 4704, 4705, 4713, 4714, 4715, 4717, 4718, 4719, 4739, 4817, 4907, 4912, 4946, 4947, 4948, 4954) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (System Administration) |
| **Security Policy Change  MU-2.2** | Making changes to the system security policies, such as firewall settings. | Advanced | System Administration | System Administration:Windows Events (1102, 1074, 4657, 4674, 4704, 4705, 4713, 4714, 4715, 4717, 4718, 4719, 4739, 4817, 4907, 4912, 4946, 4947, 4948, 4954) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (System Administration) |
| **Configuration Change  MU-2.3** | Making changes to the system configuration settings, such as process initilaization settings. | Advanced | System Administration | System Administration:Windows Events (1102, 1074, 4657, 4674, 4704, 4705, 4713, 4714, 4715, 4717, 4718, 4719, 4739, 4817, 4907, 4912, 4946, 4947, 4948, 4954) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (System Administration) |
| **Registry Change  MU-2.4** | Making changes to the Windows registry. | Advanced | System Administration | System Administration:Windows Events (1102, 1074, 4657, 4674, 4704, 4705, 4713, 4714, 4715, 4717, 4718, 4719, 4739, 4817, 4907, 4912, 4946, 4947, 4948, 4954) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (System Administration) |
| **System Shutdown  MU-2.5** | Shutting down a system, either via restart, shutdown, or power-off. | Advanced | System Administration | System Administration:Windows Events (1102, 1074, 4657, 4674, 4704, 4705, 4713, 4714, 4715, 4717, 4718, 4719, 4739, 4817, 4907, 4912, 4946, 4947, 4948, 4954) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (System Administration) |
| **Domain Logon  MU-3.1** | Logon attempts. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Failure Non-Existing User MU-3.2.1** | Failure to login because of a erroneous username. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Failure Logon Permissions MU-3.2.2** | Failure to logon because of a workstation or server restriction. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Failure Logon Hours MU-3.2.3** | Failure to logon because of logon hours restriction. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Failure Logon Type MU-3.2.4** | Failure to logon because of a logon type restriction. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Service Account Logon  MU-3.3** | Interactively logging on via a service account. Interactive logons equate to being able to view the GUI or CLI. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Privileged Logon  MU-3.4** | Loggon on with escalated privileges. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Interactive Logon MU-3.5** | Logging into a computer with the local account. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Remote Desktop Logon MU-3.6** | Logging into a computer via remote desktop session. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Explicit Logon MU-5.1** | Attempting to use specific credentials when logging in. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Process Start MU-7.1** | Failing to start a process or application. | Advanced | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Failure Insufficient Privileges MU-7.2** | Failing to start a process or application because of a lack of privileges. | Advanced | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Privileged Process Start MU-7.3** | Running a process with elevated privileges, that is rare for the specific user. | Rare Combination  Entity Pivots:  User → Privilege → Process | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Administrative Process Start  MU-7.4** | Running adminsitrative process, such as the MMC snap-in or services.msc. | Advanced/Lexicon | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Hacking Research Web Search  MU-8.1** | Searching the web for hacking techniques. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Hacking Research Website  MU-8.2** | Viewing hacking websites. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Baseline Process Stop  MU-9.1** | Stopping a process that is on the list of baseline processes for the company's workstations. | Advanced/Lexicon | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Off Baseline Process Start  MU-9.2** | Running a process that is not on the list of baseline processes for the company's workstations. | Advanced/Lexicon | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Off Baseline User Agent String  MU-9.3** | Using a browser that has a user agent string that is not on the approved user agent string list. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Physical Access  MU-10.1** | Failure to badge into any location. | Advanced/Lexicon | Physical | Badging System |
| **Restricted Physical Access  MU-10.2** | Badging into restricted areas. | Advanced/Lexicon | Physical | Badging System |
| **Local Admin Logon  MU-10.3** | Logging on with the local admin account. | Advanced/Lexicon | Authentication | Authentication:Windows Events (4624, 4625, 4634, 4647, 4648, 4740, 4672, 4768, 4778, 4779, 4800, 4801) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Authentication) |
| **Local Shutdown  MU-10.4** | Shutting down a high value asset while physically being at the keyboard. | Advanced/Lexicon | System Administration | System Administration:Windows Events (1102, 1074, 4657, 4674, 4704, 4705, 4713, 4714, 4715, 4717, 4718, 4719, 4739, 4817, 4907, 4912, 4946, 4947, 4948, 4954) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (System Administration) |
| **Safe Mode MU-10.5** | Users putting their computer into safe mode. | Advanced | System Administration | System Administration:Windows Events (1102, 1074, 4657, 4674, 4704, 4705, 4713, 4714, 4715, 4717, 4718, 4719, 4739, 4817, 4907, 4912, 4946, 4947, 4948, 4954) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (System Administration) |
| **Help Desk Permissions Request  MU-11.1** | Requesting a increase in privileges or permissions from the help desk. | Advanced/Lexicon | Email (Full body) | Mail Server or Email Gateway |
| **Improper Access MU-11.2** | Requesting access through unapproved channels. | Advanced/Lexicon | Voice (Transcription), Email (Full body), Chat (Conversation) | Voice Transcription Logs Email Journaling Chat Journaling |
| **Account Created MU-12.1** | Looking for user or computer accounts being created | Advanced | Account Management | Account Management:Windows Events (4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4754, 4755, 4756, 4757, 4758, 4764, 4767, 4781) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Account Management) |
| **Account Deleted MU-12.2** | Looking for user or computer accounts being deleted | Advanced | Account Management | Account Management:Windows Events (4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4754, 4755, 4756, 4757, 4758, 4764, 4767, 4781) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Account Management) |
| **Account Modified MU-12.3** | Looking for user or computer accounts being modified | Advanced | Account Management | Account Management:Windows Events (4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4754, 4755, 4756, 4757, 4758, 4764, 4767, 4781) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Account Management) |
| **Account Disabled MU-12.4** | Looking for user or computer accounts being disabled | Advanced | Account Management | Account Management:Windows Events (4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4754, 4755, 4756, 4757, 4758, 4764, 4767, 4781) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Account Management) |
| **Account Enabled MU-12.5** | Looking for user or computer accounts being enabled | Advanced | Account Management | Account Management:Windows Events (4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4754, 4755, 4756, 4757, 4758, 4764, 4767, 4781) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Account Management) |
| **Password Reset MU-12.6** | Looking for user or computer accounts password resets | Advanced | Account Management | Account Management:Windows Events (4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4754, 4755, 4756, 4757, 4758, 4764, 4767, 4781) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Account Management) |
| **Account Lockout MU-12.7** | A user being locked out because of multiple failed logon attempts. | Advanced | Account Management | Account Management:Windows Events (4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4754, 4755, 4756, 4757, 4758, 4764, 4767, 4781) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Account Management) |
| **Account Unlocked MU-12.8** | Looking for user or computer accounts being unlocked | Advanced | Account Management | Account Management:Windows Events (4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4754, 4755, 4756, 4757, 4758, 4764, 4767, 4781) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Account Management) |
| **SYSVOL MU-13.1** | Any interaction with the Windows SYSVOL directory. | Advanced | File Operations | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) |
| **Configuration File MU-13.2** | Any interaction with a configuration file. | Advanced | File Operations | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) |
| **Boot File MU-13.3** | Any interaction with a machines boot file. | Advanced | File Operations | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) |
| **Core DLL File MU-13.4** | Any interaction with core system DLLs. | Advanced/Lexicon | File Operations | File Operations:Windows Events (4663, 4670, 5136, 5137, 5141, 5142, 5143, 5144) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (File Operations) |
| **Compromised User Account (CU)** | **Malicious Network Port  CU-1.1** | Network port activity that is commonly tied to a specifc malware signautre. | Advanced/Lexicon | Network | Next-Gen Firewall (User) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Firewall) |
| **Malicious Process Start  CU-1.2** | Process activity that is tied to a specific malare signature. | Advanced/Lexicon | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Malicious Network IP  CU-1.3** | Network activity that is from or heading to a malicous IP address. | Advanced/Lexicon | Network | Network: Next-Gen Firewall (User) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Firewall) |
| **Malicious Hash  CU-1.4** | Known malicious certificate hashes detected within network activity. | Advanced/Lexicon | Network Web | Network: Next-Gen Firewall (User) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Firewall) Web: Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Malware Infection  CU-2.1** | A workstation being infected with malware, alerted by the anti-virus software. | Advanced | Malware | Anti-Malware Logs |
| **On-Demand Malware Scan  CU-2.2** | A quesitonable file residing on a workstation, to the point where the anti-virus software initiates a scan. | Advanced | Malware | Anti-Malware Logs |
| **Foreign Country Logon  CU-3.1** | A user logging onto a company resource from a foreign country. | Advanced | Authentication | VPN Logs |
| **Remote Access Logon CU-4.1** | A user logging in from multiple unqiue countries in a given day | Advanced | Authentication | VPN Logs |
| **Email Hyperlink  CU-5.1** | An email that has an attachment with a extension that is conducive with phishing emails or has a hyper link. | Advanced/Lexicon | Email (metadata or full body) | Mail Server or Email Gateway |
| **Phishing Language  CU-5.2** | Phishing language detected within an email. | Advanced/Lexicon | Email (metadata or full body) | Mail Server or Email Gateway |
| **Phishing Attachment Extension CU-5.3** | Extensions commonly assoicated with phishing campaigns. | Advanced/Lexicon | Email (metadata or full body) | Mail Server or Email Gateway |
| **Phishing Attachment Name CU-5.4** | Common phishing attachment names. | Advanced/Lexicon | Email (metadata or full body) | Mail Server or Email Gateway |
| **Uncommon Website  CU-6.1** | Accessing a site that is rare globally rare, impacting the risk for the user tied to the event. | Rare Combination  Entity Pivots:  Site | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Malicious Website  CU-6.2** | Accessing a website that is on the list on known malicious websites. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Baseline Process Stop  CU-7.1** | Stopping a process that is on the list of baseline processes for the company's workstations. | Advanced/Lexicon | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Off Baseline Process Start  CU-7.2** | Running a process that is not on the list of baseline processes for the company's workstations. | Advanced/Lexicon | Processes | Windows Events (4688) Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Processes, Command Line) |
| **Off Baseline User Agent String  CU-7.3** | Using a browser that has a user agent string that is not on the approved user agent string list. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Website Redirect CU-8.1** | Website Redirected | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Negative Workplace Behavior (NB)** | **Explicit Communications  NB-1.1** | Communications with other employees that contains sexually explicit language. | Advanced/Lexicon | Voice (Transcription), Email (Full body), Chat (Conversation) | Voice Transcription Logs Email Journaling Chat Journaling |
| **Violent Communications  NB-2.1** | Communications with other employees that contains violent language. | Advanced/Lexicon | Voice (Transcription), Email (Full body), Chat (Conversation) | Voice Transcription Logs Email Journaling Chat Journaling |
| **NSFW Web Search  NB-3.1** | Searching the internet for sexually explciit content. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **NSFW Website  NB-3.2** | Browsing sexually explicit websites. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Flight Risk Communications  NB-4.1** | Communications that are conducive with thinking about leaving the company. | Advanced/Lexicon | Voice (Transcription), Email (Full body), Chat (Conversation) | Voice Transcription Logs Email Journaling Chat Journaling |
| **Flight Risk Web Search NB-4.2** | Job search related web searches. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Flight Risk Website  NB-4.3** | Browsing job search websites. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Online Media Usage  NB-5.1** | Increase in time spent viewing media online, such as Netflix, YouTube, or Hulu. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Social Media Usage  NB-5.2** | Increase in time spent viewing social media online, such as Facebook, Twiiter, or Instagram. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Corporate Web Activity  NB-6.1** | Decrease in the number of times a user has accessed the internal company shared resource site, such as Confluence or SharePoint | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Financial Distress Communications NB-7.1** | Communications that are conducive with a employee being in a hard financial situation. | Advanced/Lexicon | Voice (Transcription), Email (Full body), Chat (Conversation) | Voice Transcription Logs Email Journaling Chat Journaling |
| **Financial Distress Web Search NB-7.2** | Web searches that are conducive with a employee being in a hard financial situation. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Financial Distress Website  NB-7.3** | Viewing websites that are conducive with hard financial situations. | Advanced/Lexicon | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Negative Sentiment  NB-8.1** | Looking for negative sentime across comnnunications and web activity. | Sentiment | Voice (Transcription), Email (Full body), Chat (Conversation) | Voice Transcription Logs Email Journaling Chat Journaling |
| **Evade Oversight Communications NB-9.1** | Looking for communications between employees discussing oversight evasion. | Advanced/Lexicon | Voice (Transcription), Email (Full body), Chat (Conversation) | Voice Transcription Logs Email Journaling Chat Journaling |
| **Audit History Edit  NB-10.1** | Clearing your audit logs, such as bash history of event logs. | Advanced | System Administration | Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Audit Edit) |
| **Internet Browser History Edit  NB-10.2** | Clearing your internet browser history, thinking it is covering your tracks. | Advanced | System Administration | Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Audit Edit) |
| **IT Oversight Evasion  NB-10.3** | Researching ways to cover your IT tracks. | Advanced/Lexicon | Voice (Transcription), Email (Full body), Chat (Conversation) | Voice Transcription Logs Email Journaling Chat Journaling |
| **Proxy Avoidance  NB-10.4** | Avoiding proxy actions and oversight through proxy websites. | Advanced | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Private Internet Browsing  NB-10.5** | Browsing the internet in privacy mode. | Advanced | Web | Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) |
| **Illicit Workplace Behavior (IB)** | **Email to Foreign Domain IB-1.1** | Emails where the recipient is a foreign domain. | Advanced/Lexicon | Email (metadata or full body) | Mail Server or Email Gateway |
| **Call to Foreign Country IB-1.2** | Calls that have destinations outside of the U.S. | Advanced/Lexicon | Voice | Voice Transcription Logs |
| **Email to Competitor Domain  IB-2.1** | Email communications to competior email domains that contain confidential words. | Advanced/Lexicon | Email (metadata or full body) | Mail Server or Email Gateway |
| **Email to Media Domain  IB-3.1** | Email communications to media domains. | Advanced/Lexicon | Email (metadata or full body) | Mail Server or Email Gateway |
| **Secuirty Clearance Research  IB-4.1** | Browsing websites or communications that contain strings conducive with deceiving a security investigator. | Advanced/Lexicon | Web Voice (Transcription), Email (Full body), Chat (Conversation) | Web: Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) Voice Transcription Logs Email Journaling Chat Journaling |
| **Polygraph Research  IB-4.2** | Research polygraph avoidance techniques. | Advanced/Lexicon | Web Voice (Transcription), Email (Full body), Chat (Conversation) | Web: Proxy and/or Endpoint Monitoring (Forcepoint Insider Threat or 3rd party) (Web) Voice Transcription Logs Email Journaling Chat Journaling |
| **Wildcard Features** | **Confidential Content WC-1** | Looking for confidential company information in the content field. | Advanced | Wildcard | Every Log that contains this feature |
| **Secret Content WC-2** | Looking for secret company information in the content field or flagged in an alert from another vendor. | Advanced | Wildcard | Every Log that contains this feature |
| **Top Secret Content WC-3** | Looking for top secret company information in the content field or flagged in an alert from another vendor. | Advanced | Wildcard | Every Log that contains this feature |
| **Off Hours WC-4** | Looking for activity occuring during non-work hours. | Time Grouping | Wildcard | Every Log that contains this feature |
| **Weekend WC-5** | Looking for activity ocurring during the weekend. | Time Grouping | Wildcard | Every Log that contains this feature |
| **High Value Asset WC-6** | Looking for any activity where a High Value Asset is involved, either as the Destination or Source. | Advanced/Lexicon | Wildcard | Every Log that contains this feature |
| **Has Attachment WC-7** | Whether or not the event included an attachment. | Attachment | Wildcard | Every Log that contains this feature |
| **Bytes WC-8** | Looking for outlier bytes | Numeric Field | Wildcard | Every Log that contains this feature |
| **Bytes In WC-9** | Looking for outlier bytes in | Numeric Field | Wildcard | Every Log that contains this feature |
| **Bytes Out WC-10** | Looking for outlier bytes out | Numeric Field | Wildcard | Every Log that contains this feature |
| **Source Code Content WC-11** | Looking for company source code in the content field. | Lexicon | Wildcard | Every Log that contains this feature |
| **Alexa Ranking WC-12** | Looking for uncommon websites via the alexa domain ranking. | Numeric Field | Wildcard | Every Log that contains this feature |
| **Failure WC-13** | A failure event. | Advanced | Wildcard | Every Log that contains this feature |
| **Success WC-14** | A success event. | Advanced | Wildcard | Every Log that contains this feature |
| **Severity WC-15** | The numerical value for the severity of the event. | Numeric Field | Wildcard | Every Log that contains this feature |
| **Untitled Content WC-16** | Looking for documents that are untitled. | Advanced | Wildcard | Every Log that contains this feature |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | = | Possible in PoCs (if relevant ingestion feeds are available) |  |  |  |

APPENDIX C – Pre-Defined Models and Scenarios

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Scenarios** | **Behavioral Model (Model)** | **Model Description** | **Primary Role** | **Secondary Role** | **Aggregation Method** | **Attribute** | **Calculate Outliers and Outlier Direction** | **Model RQL Query** | **Event Feature (Feature)** |
| **Data Exfiltration (DE)** | **DE1A Internal Data Movement** | Looking for anomalous movement of data within the enterprise, conducive with gathering data before it is exfiltrated. | User | Destination | Attribute Sum | Bytes | TRUE Above | **Internal Site Download**  **DE-1.1**  **File Copy**  **DE-1.2**  **File Move**  **DE-1.3** | N/A |
| **DE1B Internal Data Movement** | Looking for anomalous movement of data within the enterprise, conducive with gathering data before it is exfiltrated. | User | Destination | Max Model Event Score | N/A | FALSE | **Internal Site Download  DE-1.1  File Copy DE-1.2  File Move DE-1.3** | **Internal Site Download  DE-1.1** |
| **File Copy  DE-1.2** |
| **File Copy Remote Desktop  DE-1.2.2** |
| **File Copy Command Line  DE-1.2.3** |
| **File Move DE-1.3** |
| **Confidential Content WC-1** |
| **Secret Content WC-2** |
| **Top Secret Content WC-3** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **Bytes WC-8** |
| **Source Code Content WC-11** |
| **Failure WC-13** |
| **Success WC-14** |
| **Untitled Content WC-16** |
| **DE2A External Data Movement** | Looking for anomalous data volumes moving outside of the network. This can be considered the actual exfiltration event/action. | User | Destination | Attribute Sum | Bytes | True Above | **Cloud Storage Upload  DE-2.1  Print Activity  DE-2.2  USB Transfer  DE-2.3  CD/DVD Burn DE-2.4** | N/A |
| **DE2B External Data Movement** | Looking for anomalous movement of data outside of the network. This can be considered the actual exfiltration event/action. | User | Destination | Max Model Event Score | N/A | FALSE | **Cloud Storage Upload  DE-2.1  Print Activity  DE-2.2  USB Transfer  DE-2.3  CD/DVD Burn DE-2.4** | **Cloud Storage Upload  DE-2.1** |
| **Confidential Content WC-1** |
| **Secret Content WC-2** |
| **Top Secret Content WC-3** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **Bytes WC-8** |
| **Source Code Content WC-11** |
| **Failure WC-13** |
| **Success WC-14** |
| **Untitled Content WC-16** |
| **DE3 Email Data Movement** | Looking for anomalous movement of data outside of the network. This can be considered the actual exfiltration event/action. | Sender | Recipient | Max Model Event Score | N/A | FALSE | **Email to External Domain  DE-3.1** | **Email to External Domain  DE-3.1** |
| **Confidential Content WC-1** |
| **Secret Content WC-2** |
| **Top Secret Content WC-3** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **Has Attachment WC-7** |
| **Source Code Content WC-11** |
| **Failure WC-13** |
| **Success WC-14** |
| **Untitled Content WC-16** |
| **DE4 File Operations** | Looking for anomalous interactions with files, such as opening them to check the contents of the file, accessing a file share to see if anything of interest is there, or augmented the file to prepare for exfiltration. | User | Destination | Event Count | N/A | TRUE Above | **File Access DE-4.1  File Compression  DE-4.2  File Delete DE-4.3  File Encryption  DE-4.4  File Modification DE-4.5  File Rename  DE-4.6  File Share Access DE-4.7  File Decompression DE-4.8** | N/A |
| **DE5 File Share Cardinality** | Looking for anomalous number of distinct file shares accessed per user. | User | File Share | Secondary Role Cardinality | N/A | TRUE Above | ***File Operations Mode*** | N/A |
| **DE6 Data Reconnaissance** | Looking for activity conducive with searching for data throughout the enterprise. This can be considered the behavior associated with finding high-value data amongst all of the enterprise's data. | User | Destination | Aggregate Model Event Score | N/A | FALSE | **File Search  DE-6.1  File Properties Check DE-6.2  Data Reconnaissance Process  DE-6.3** | **File Search  DE-6.1** |
| **File Properties Check DE-6.2** |
| **Data Reconnaissance Process  DE-6.3** |
| **Confidential Content WC-1** |
| **Secret Content WC-2** |
| **Top Secret Content WC-3** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **High Value Asset WC-6** |
| **Source Code Content WC-11** |
| **Failure WC-13** |
| **Success WC-14** |
| **DE7 Data Loss** | Looking for employees who are leaking sensitive information. | User | Destination | Max Model Event Score | N/A | FALSE | **DLP Print Alert  DE-7.1  DLP Upload Alert  DE-7.2  DLP Email Alert  DE-7.3  DLP Transfer Alert  DE-7.4** | **DLP Print Alert  DE-7.1** |
| **DLP Upload Alert  DE-7.2** |
| **DLP Email Alert  DE-7.3** |
| **DLP Transfer Alert  DE-7.4** |
| **DLP Matches DE-7.5** |
| **Confidential Content WC-1** |
| **Secret Content WC-2** |
| **Top Secret Content WC-3** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **Bytes WC-8** |
| **Source Code Content WC-11** |
| **Failure WC-13** |
| **Success WC-14** |
| **Severity WC-15** |
| **Malicious User (MU)** | **MU1 Network Reconnaissance** | Looking for activity conducive with exploring the network to discover assets of interest. | User | Destination | Aggregate Model Event Score | N/A | FALSE | **Network Reconnaissance Process  MU-1.1  Network Reconnaissance Port  MU-1.2** | **Network Reconnaissance Process  MU-1.1** |
| **Network Reconnaissance Port  MU-1.2** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **High Value Asset WC-6** |
| **MU2 Systems Administration** | Looking for activity conducive with with either damaging system configurations or enabling various settings to allow that damage to occur. | User | Destination | Max Model Event Score | N/A | TRUE Above | **Audit Policy Change  MU-2.1  Security Policy Change  MU-2.2  Configuration Change  MU-2.3  Registry Change  MU-2.4  System Shutdown  MU-2.5** | **Audit Policy Change  MU-2.1** |
| **Security Policy Change  MU-2.2** |
| **Configuration Change  MU-2.3** |
| **Registry Change  MU-2.4** |
| **System Shutdown  MU-2.5** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **High Value Asset WC-6** |
| **Failure WC-13** |
| **Success WC-14** |
| **MU3 Malicious Authentication** | Looking for abnormal authentication activity that be conducive with asset discovery or special logons that enable malicious actions. | User | Destination | Aggregate Model Event Score | N/A | FALSE | **Domain Logon  MU-3.1** | **Domain Logon  MU-3.1** |
| **Failure Non-Existing User MU-3.2.1** |
| **Failure Logon Permissions MU-3.2.2** |
| **Failure Logon Hours MU-3.2.3** |
| **Failure Logon Type MU-3.2.4** |
| **Service Account Logon  MU-3.3** |
| **Privileged Logon  MU-3.4** |
| **Interactive Logon MU-3.5** |
| **Remote Desktop Logon MU-3.6** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **High Value Asset WC-6** |
| **Failure WC-13** |
| **Success WC-14** |
| **MU4 Destination Cardinality** | Looking for anomalous number of unique workstations and servers logged into per user. | User | Destination | Secondary Role Cardinality | N/A | TRUE Above | ***Authentication Mode*** | N/A |
| **MU5 Explicit Account Cardinality** | Looking for anomalous number of accounts explicitily logged into per user. | User | Account | Secondary Role Cardinality | N/A | TRUE Above | **Explicit Logon MU-5.1** | N/A |
| **MU6 Authenticated Process Cardinality** | Looking for anomalous number of processes authenticated per user. | User | Process | Secondary Role Cardinality | N/A | TRUE Above | ***Authentication Mode*** | N/A |
| **MU7 Process Activity** | Looking for privileged activity that could facilitate the malicious actions. | User | Process | Aggregate Model Event Score | N/A | FALSE | **Process Start MU-7.1** | **Process Start MU-7.1** |
| **Failure Insufficient Privileges MU-7.2** |
| **Privileged Process Start MU-7.3** |
| **Administrative Process Start  MU-7.4** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **High Value Asset WC-6** |
| **Failure WC-13** |
| **Success WC-14** |
| **MU8 Malicious Research** | Looking for people researching ways to commit malicious actions. | User | Destination | Event Count | N/A | TRUE Above | **Hacking Research Web Search  MU-8.1  Hacking Research Website  MU-8.2** | N/A |
| **MU9 Configuration Deviation** | Looking for deviations from the approved machine baseline, that can be conducive with damaging processes or detection avoidance. | User | Destination | Aggregate Model Event Score | N/A | FALSE | **Baseline Process Stop  MU-9.1  Off Baseline Process Start  MU-9.2  Off Baseline User Agent String  MU-9.3** | **Baseline Process Stop  MU-9.1** |
| **Off Baseline Process Start  MU-9.2** |
| **Off Baseline User Agent String  MU-9.3** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **High Value Asset WC-6** |
| **MU10 Physical Access** | Looking for abnormal physical access to sensitive areas or at the keyboard of high valued assets. This can be considered the gaining access portion of the malicious incident. | User | Destination | Aggregate Model Event Score | N/A | FALSE | **Physical Access  MU-10.1  Local Admin Logon  MU-10.3  Local Shutdown  MU-10.4  Safe Mode MU-10.5** | **Physical Access  MU-10.1** |
| **Restricted Physical Access  MU-10.2** |
| **Local Admin Logon  MU-10.3** |
| **Local Shutdown  MU-10.4** |
| **Safe Mode  MU-10.5** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **High Value Asset WC-6** |
| **Failure WC-13** |
| **Success WC-14** |
| **MU11 Access Request** | Looking for activity conducive with requests a higher-level of privileges to commit the malicious action. | Sender | Recipient | Event Count | N/A | FALSE | **Help Desk Permissions Request  MU-11.1  Improper Access MU-11.2** | N/A |
| **MU12 Account Management** | Looking for outlier account management activity, uncovering account management activity by employees who usually do not have any account management activity. | User | Object | Event Count | N/A | TRUE Above | **Account Created MU-12.1  Account Deleted MU-12.2  Account Modified MU-12.3  Account Disabled MU-12.4  Account Enabled MU-12.5  Password Reset MU-12.6  Account Lockout MU-12.7  Account Unlocked MU-12.8** | N/A |
| **MU-13 Core System Components** | Looking for any interactions with core system files and components. | User | Destination | Max Model Event Score | N/A | FALSE | N/A | **SYSVOL MU-13.1** |
| **Configuration File MU-13.2** |
| **Boot File MU-13.3** |
| **Core DLL File MU-13.4** |
| **Compromised User Account (CU)** | **CU1 Malware Threat** | Looking for activity indicating a malware infection that has already occurred or could of potentially occurred. | User | Destination | Event Count | N/A | FALSE | **Malicious Network Port  CU-1.1  Malicious Process Start  CU-1.2  Malicious Network IP  CU-1.3  Malicious Hash  CU-1.4** | N/A |
| **CU2 AntiVirus Match** | Looking for activity indicating a malware infection that has already occurred or could of potentially occurred. | User | Signature | Event Count | N/A | FALSE | **Malware Infection  CU-2.1  On-Demand Malware Scan  CU-2.2** | N/A |
| **CU3 Remote Logon** | Looking for authentication activity that indicates an account has been taken over by a new person from a new location. | User | Source Country | Event Count | N/A | FALSE | **Foreign Country Logon  CU-3.1** | N/A |
| **CU4 Source Country Cardinality** | Looking for users with a high number of unqiue countries logged in from, via remote access. | User | Source Country | Secondary Role Cardinality | N/A | FALSE | **Remote Access Logon  CU-4.1** | N/A |
| **CU5 Phishing** | Looking for email activity conducive with a potential phishing campaign. | Recipient | Sender | Aggregate Model Event Score | N/A | FALSE | **Email Hyperlink  CU-5.1** | **Email Hyperlink CU-5.1** |
| **Phishing Language  CU-5.2** |
| **Phishing Attachment Extension CU-5.3** |
| **Phishing Attachment Name CU-5.4** |
| **CU6 Negligent Browsing** | Looking for internet browsing activity that could potentially put a person at greater risk of having their computer infected. | User |  | Event Count | N/A | FALSE | **Uncommon Website  CU-6.1  Malicious Website  CU-6.2** | N/A |
| **CU7 Configuration Deviation** | Looking for deviations from the approved machine baseline, that can be conducive with damaging processes or detection avoidance. | User | Destination | Event Count | N/A | FALSE | **Baseline Process Stop  CU-7.1  Off Baseline Process Start  CU-7.2  Off Baseline User Agent String Activity  CU-7.3** | N/A |
| **CU8 Redirected Internet Traffic** | Looking for users with a high-number of website redirect events. | User | Destination IP | Event Count | N/A | FALSE | **Website Redirect CU-8.1** | N/A |
| **CU9 Port Cardinality** | Looking for anomalous number of unique ports a user interacted with over the network. | User | Destination Port | Secondary Role Cardinality | N/A | TRUE Above | ***Network Mode*** | N/A |
| **CU10 Destination IP Cardinality** | Looking for anomalous number of unique destination IPs a user interacted with over the network. | User | Destination IP | Secondary Role Cardinality | N/A | TRUE Above | ***Network Mode*** | N/A |
| **Negative Workplace Behavior (NB)** | **NB1 Sexual Harassment** | Looking for communications conducive with a sexual harrassment incident. | Sender | Recipient | Event Count | N/A | FALSE | **Explicit Communications  NB-1.1** | N/A |
| **NB2 Workplace Violence** | Looking for violent communications that could indicate a work place violence incident. | Sender | Recipient | Event Count | N/A | FALSE | **Violent Communications  NB-2.1** | N/A |
| **NB3 Obscene Content** | Looking for obscene content activity, either through web searches or web browsing. | User | Destination | Event Count | N/A | FALSE | **NSFW Web Search  NB-3.1  NSFW Website  NB-3.2** | N/A |
| **NB4A Flight Risk Comms** | Looking for communications conducive with an employee leaving, such as emailing a resume or searching for a new job. | Sender | Recipient | Event Count | N/A | TRUE Above | **Flight Risk Communications  NB-4.1** | N/A |
| **NB4B Flight Risk Web** | Looking for activity conducive with an employee leaving, such as visiting job and resume websites. | User | Destination | Event Count | N/A | TRUE Above | **Flight Risk Web Search NB-4.2  Flight Risk Website  NB-4.3** | N/A |
| **NB5 Decreased Productivity** | Looking for employees spending a large amount of time doing non work related tasks. | User | Destination | Attribute Sum | Duration | TRUE Above | **Online Media Usage  NB-5.1  Social Media Usage  NB-5.2** | N/A |
| **NB6A Corporate Disengagement** | Looking for employees who are not interacting with core company assets. | User | Destination | Attribute Sum | Duration | TRUE Below | **Corporate Web Activity  NB-6.1** | N/A |
| **NB6B Recipient Cardinality** | Looking for users talking to less employees, compared to their previous baselined activity. | Sender | Recipient | Secondary Role Cardinality | N/A | TRUE Below | ***Chat Mode  Email Mode*** | N/A |
| **NB7A Financial Distress Comms** | Looking for communications activity indicative of financial turmoil and employees looking for a way to get resolve the issue. | Sender | Recipient | Event Count | N/A | FALSE | **Financial Distress Communications NB-7.1** | N/A |
| **NB7B Financial Distress Web** | Looking for web site activity indicative of financial turmoil and employees looking for a way to get resolve the issue. | User | Destination | Event Count | N/A | FALSE | **Financial Distress Web Search NB-7.2  Financial Distress Website  NB-7.3** | N/A |
| **NB8 Negative Sentiment** | Looking for negative sentiment and signs of improper discussions within communications. | Sender | Recipient | Aggregate Model Event Score | N/A | TRUE Above | N/A | **Negative Sentiment  NB-8.1** |
| **NB9 Oversight Evasion** | Looking for signs of oversight evasion attempts within communications. | Sender | Recipient | Event Count | N/A | FALSE | **Evade Oversight Communications NB-9.1** | N/A |
| **NB10 IT Oversight Evasion** | Looking for activity conducive with avoiding IT detection, either pre or post exfiltration. This can be considered covering tracks after the fact, or positioning to better avoid detection. | User | Destination | Event Count | N/A | FALSE | **Audit History Edit  NB-10.1  Internet Browser History Edit  NB-10.2  IT Oversight Evasion  NB-10.3  Proxy Avoidance  NB-10.4  Private Internet Browsing  NB-10.5** | N/A |
| **Illicit Workplace Behavior (IB)** | **IB1 Espionage** | Looking for employees who are showing signs of espionage. | Sender | Recipient | Max Model Event Score | N/A | TRUE Above | **Email to Foreign Domain IB-1.1  Call to Foreign Country IB-1.2** | **Email to Foreign Domain IB-1.1** |
| **Call to Foreign Country IB-1.2** |
| **Confidential Content WC-1** |
| **Secret Content WC-2** |
| **Top Secret Content WC-3** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **Has Attachment WC-7** |
| **Source Code Content WC-11** |
| **Failure WC-13** |
| **Success WC-14** |
| **Untitled Content WC-16** |
| **IB2 Corporate Espionage** | Looking for employees communicating with competitors while still at their current company, but specifically mentioning their current company IP and looking to join the competitor. | Sender | Recipient | Max Model Event Score | N/A | N/A | **Email to Competitor Domain  IB-3.1** | **Email to Competitor Domain  IB-2.1** |
| **Confidential Content WC-1** |
| **Off Hours WC-4** |
| **Weekend WC-5** |
| **Has Attachment WC-7** |
| **Bytes WC-8** |
| **Source Code Content WC-11** |
| **Failure WC-13** |
| **Success WC-14** |
| **Untitled Content WC-16** |
| **IB4 Clearance Evasion** | Looking for people researching ways to omit security clearance information or ways to deceive a polygraph. | User | Destination | Event Count | N/A | FALSE | **Secuirty Clearance Research  IB-4.1  Polygraph Research  IB-4.2** | N/A |

Appendix D – Recommended Windows Events ID

| **Mode** | **Event ID** | **Legacy ID** | **Subject** |
| --- | --- | --- | --- |
| **Account Management** | **4720** | **624** | User account was created |
| **4722** | **626** | User account was enabled |
| **4723** | **627** | Attempted password change |
| **4724** | **628** | Attempted password reset |
| **4725** | **629** | User account was disabled |
| **4726** | **630** | User account was deleted |
| **4727** | **631** | Global security group created |
| **4728** | **632** | Added to global security group [**4732**] |
| **4729** | **633** | Removed from global security group [**4733**] |
| **4730** | **634** | Global security group deleted [**4734**] |
| **4731** | **635** | Local security group created |
| **4732** | **636** | Added to local security group |
| **4733** | **637** | Removed from local security group |
| **4734** | **638** | Local security group deleted |
| **4735** | **639** | Local security group was changed |
| **4737** | **641** | Global security group changed |
| **4738** | **642** | User account was changed |
| **4754** | **658** | Universal security group created |
| **4755** | **659** | Universal security group was changed |
| **4756** | **660** | Added to universal security group [**4732**] |
| **4757** | **661** | Removed from universal security group [**4733**] |
| **4758** | **662** | Universal security group deleted |
| **4764** | **668** | A group's type (Local vs. Global vs. Universal) was changed |
| **4767** | **671** | User account was unlocked |
| **4781** | **685** | Name of account changed |
| **Authentication** | **4624** | **528,540** | An account was successfully logged on |
| **4625** | **529-537,539** | An account failed to logon |
| **4634** | **538** | An account was logged off |
| **4647** | **551** | User initiated logoff |
| **4648** | **552** | A logon was attempted using explicit credentials |
| **4740** | **644** | User account was locked out |
| **4672** | **576** | Special privileges assigned to new logon |
| **4768** | **672,676** | Kerberos authentication ticket (TGT) was requested |
| **4778** | **682** | A session was reconnected to a Window Station |
| **4779** | **683** | A session was disconnected from a Window Station |
| **4800** | **N/A** | The workstation was locked |
| **4801** | **N/A** | The workstation was unlocked |
| **File Operations** | **4663** | **567** | An attempt was made to access an object |
| **4670** | **N/A** | Permissions on an object were changed |
| **5136** | **566** | A directory service object was modified |
| **5137** | **566** | A directory service object was created |
| **5141** | **N/A** | A directory service object was deleted |
| **5142** | **N/A** | A network share object was added |
| **5143** | **N/A** | A network share object was modified |
| **5144** | **N/A** | A network share object was deleted |
| **Process** | **4688** | **592** | A new process has been created |
| **Systems Administration** | **1102** | **517** | The audit log was cleared |
| **1074** | **N/A?** | System Restart |
| **4657** | **567** | A registry value was modified |
| **4674** | **578** | An operation was attempted on a privileged object |
| **4704** | **608** | A user right was assigned |
| **4705** | **609** | A user right was removed |
| **4713** | **617** | Kerberos policy changed |
| **4714** | **618** | Encrypted data recovery policy was changed |
| **4715** | **N/A** | The audit policy (SACL) on an object was changed |
| **4717** | **621** | System security access was granted to an account |
| **4718** | **622** | System security access was removed from an account |
| **4719** | **612** | System audit policy was changed |
| **4739** | **643** | Domain policy was changed |
| **4817** | **N/A** | Auditing settings on an object were changed |
| **4907** | **N/A** | Auditing settings on an object were changed |
| **4912** | **807** | Per user audit policy was changed |
| **4946** | **N/A** | Firewall rule added |
| **4947** | **N/A** | Firewall rule modified |
| **4948** | **N/A** | Firewall rule deleted |
| **4954** | **N/A** | Firewall GPO settings changed and applied |