SOC Process Knowledgebase

Contents

[**SOC Main 4**](#_yd5aqciizh35)

[Process & Procedures by Category 4](#_30j0zll)

[Additional Categories 4](#_1fob9te)

[Procedure Flow 5](#_3znysh7)

[**SOC Contacts 6**](#_feebw2nfecjx)

[SOC Contacts 6](#_le7copawo6b2)

[SOC Workstations 6](#_axaer6b3zf58)

[Pager Contact Information for Security 6](#_c34qubkhhej)

[General IT & Emergency Contacts 6](#_40mivh5egnsr)

[Departmental Contacts 6](#_ozjhiucdyvu7)

[Email Distribution Lists 6](#_hg12y9d0eftr)

[External Contacts 6](#_f0pozqut68lq)

[Internal Contacts 7](#_sxextgeakhce)

[**SOC Process Hierarchy 7**](#_p3ajk7b85i7l)

[Purpose 7](#_92kvnluqpusx)

[Description 7](#_ceihgisehoy9)

[**SOC Roles & Responsibilities 8**](#_1m2wsneppdn3)

[Roles & Responsibilities 8](#_u7uf6gcdaztl)

[Director – Security Operations 8](#_4r8rrz5qz7wq)

[Manager – Security Operations Center (SOC) 8](#_psldv18z5lyb)

[SOC Level 1 Analyst 9](#_n7czoqjk9u0y)

[SOC Level 2 Analyst 10](#_g4dnebotxajd)

[SOC Level 3 Analyst 10](#_ry70rhgmsg7l)

[Cyber Intelligence Analyst 11](#_hcg2g11haekt)

[Manager – Incident Response 11](#_lvmoosdfdzob)

[Incident Response Analyst 12](#_ixrmstnhrwnm)

[Forensic Analyst / Investigator 12](#_wbpndp3eiq82)

[SIEM Engineer/Content Developer 13](#_tb9z0kapvhgr)

[Cybersecurity Data Scientist 14](#_1zdc95eo7ygd)

[Responsibility Chart 14](#_62rrqwh0ff3b)

[RACI Matrix 14](#_ctkyocidajvh)

[**Incident Response Framework 15**](#_8c0cd2qr1n7x)

[Incident Response Framework: Security Operations Center 15](#_ua4vfasz79w1)

[Description 15](#_1rnnspa7c3vj)

[**SOC Incident Response Procedures 16**](#_pi1zkve81685)

[Summary 16](#_ihf51nea4xuj)

[Purpose 17](#_b2y9gzfpjbwz)

[Incident Response Decision Matrix 17](#_qrwj0vxq98r8)

[Scope 19](#_glp62wvxqyvf)

[Definitions 19](#_97scql4t290l)

[Severity Definitions 20](#_q5m0nbo538km)

[Incident Response Methodology 22](#_ofg4sw2lmm5v)

[Incident Preparation 22](#_cs13kyptaqgb)

[Watch / Monitor Phase (Detection) 23](#_sj8v3shz6nj2)

[Investigation Phase 23](#_wm8xz5mu5eyy)

[Initiate Action 24](#_rm0zls6e53wn)

[Incident Information 25](#_4jjrqixg2b0z)

[Continue to Monitor Activity 26](#_dh709jxk21e6)

[Document Activity in the Shift Log 26](#_xs2icpu86bsv)

[Follow Up on Activity 26](#_1uhaf539zvx8)

[Service Level Objectives (SLOs) 26](#_xe7wfuj73wy3)

[General goals: 26](#_dgeilxlgc63j)

[Incident management goals: 26](#_xg9gkclcitn3)

[Remediation SLOs 27](#_lpc9wutiil6r)

[Notification SLOs 27](#_f2j0y57410zr)

[Dependencies within the Organization 28](#_gqgansorvooc)

[Additional IR Phases 28](#_awhpd6hmdn4f)

[Mobilize 28](#_5pihwyj7wbmz)

[Assessment and Containment 29](#_jqj50bt3gr1z)

[Technical Root Cause Analysis 30](#_49emsv52qd2d)

[Remediation & Recovery 31](#_83yc2y6tcn30)

[Remediation Scenarios/Options: 31](#_tsrk59ep6pra)

[General Recovery Guidance: 32](#_4jscwwfpaaeb)

[Post Mortem (Lessons Learned) 32](#_umaodrmzl813)

[Recommendations 33](#_jgatr1ofj81j)

[**SOC Analytical Processes & Procedures 33**](#_632nqpp2dhpt)

[Intrusion Analysis Process 34](#_i4dy9owj6czy)

[Incident Triage Workflow & Narrative 35](#_re3m5sc3xfwj)

[Incident Analysis Procedures 39](#_q8850cja53to)

[Information Fusion Procedures 43](#_tpp5naha66x3)

[Focused Monitoring Procedures 44](#_ku5jb11lo64r)

[SOC Use Cases 46](#_pmpvsrxt4h5s)

[Host Analysis Process 51](#_tcqb31ld9sjy)

[Subtle Event Process 55](#_nkcqo8lr8l4a)

[Data Exploration Procedures 56](#_bqvoroppy490)

[**SOC Business Process & Procedures 58**](#_p9xp7lu3qrz6)

[SOC Efficiency Metrics 59](#_v1tlrq9bjknz)

[SOC Analytics Efficiency Metrics 61](#_hfr5f6x6bfwa)

[Process Improvement 62](#_r6q2p6vzmkj7)

[Process Maturity 64](#_6wjn1kpkdpek)

[Agile Methodology 67](#_5oce4f3n6iju)

[Documentation Standard Procedures 68](#_motqppf9w406)

[Compliance Process 70](#_qw3bfgs4gex7)

[Compliance Support 72](#_xhqpugsh9iub)

[Business Continuity & Disaster Recovery Process 77](#_2r56qczeoxds)

[Business Continuity & Disaster Recovery Plans 79](#_pnd1tai5ovgr)

[**SOC Operational Processes & Procedures 79**](#_s3huh66jb77l)

[Incident Triage 80](#_porqqr1totrw)

[Callout / Escalation 85](#_w7nlzhq2s4h8)

[Incident Management Procedure 86](#_w1gwa2qpgbbo)

[Crisis Response 91](#_5htr9q89no71)

[Shift Log Management 95](#_tkvmvps162i6)

[Phone Bridge Details 97](#_b2e6o6cha328)

[Vulnerability Scanning Schedule 98](#_48jpm8wlzxie)

[IP & Domain Blocklisting 100](#_v409bboe6zel)

[Daily Operations Process 109](#_2zbs17x8u6w4)

[Daily Ops Meeting 110](#_bn7lzht0b2rb)

[Problem Tickets and Change Controls 111](#_kn414reciep)

[Shift Staffing Schedule 112](#_7v2l3i2jmzbx)

[Shift Turnover 113](#_jrkiaqlco1s8)

[Weekly Operational Process 114](#_gex5x3d4e85w)

[Weekly Threat Intelligence Report 114](#_ibtkkcxdity4)

[Reporting Process 116](#_zb8vmznitam2)

[Periodic Reports 117](#_vkwridw0kwvh)

[**SOC Technology Processes & Procedures 118**](#_jwi78m5b0h83)

[Design Process 118](#_q1h7ganlatpw)

[Architecture 120](#_xz905e3k1f9g)

[Data Retention Standard 120](#_1tnhn1pqlyw5)

[Network Diagrams 122](#_1aydkegjhsl0)

[Content Development Design 122](#_yinsixd921p3)

[Azure Infrastructure Monitoring 134](#_koehtje7aogq)

[Engineering Incident Management 135](#_ldtzgu68506x)

[User Access Control Design 137](#_4zu1bs7y81cr)

[**SOC Tools and Resources 139**](#_it04f3x60byf)

[Technical Resources 139](#_frcqznr4jbhs)

[Threat intelligence Sources 141](#_23gsw2p3t9vj)

[**SOC Incident Actions 142**](#_r56scjy195f4)

[Suspicious PowerShell Command Line 142](#_84fbz1agvy1z)

[**SOC Training 150**](#_k1foljvnn26x)

[Leverage Microsoft Learn for Role-Based Training for Information Security Professionals in Azure 150](#_4kpios8m6a6a)

# 

# SOC Main

The mission of the Security Operations Center is to:

* Identify and alert on all cyber threats and compliance exceptions
* Assist in minimizing the impact of adverse events that do occur
* Achieve rapid situational awareness of current threats and compliance statutes
* Automate manual reporting processes
* Expedite remediation and incident response times
* Continually measure and improve the effectiveness of security and compliance processes
* Automate monitoring and enforcement of security controls

## Process & Procedures by Category

| Process & Procedures by Category | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| SOC Analytical Processes & Procedures | SOC Operational Processes & Procedures | SOC Technology Processes & Procedures | SOC Business Processes & Procedures | SOC Incident Actions | SOC Tools & Resources | SOC Training |

Every SOC Analyst is responsible for reading and understanding all processes and procedures documented in this knowledge base. After each new analyst reads a process or procedure page, he/she will sign that page in the section labeled Analyst Signatures acknowledging their understanding and acceptance. SOC analysts will automatically receive nightly notifications of all changes made to these processes and procedures.

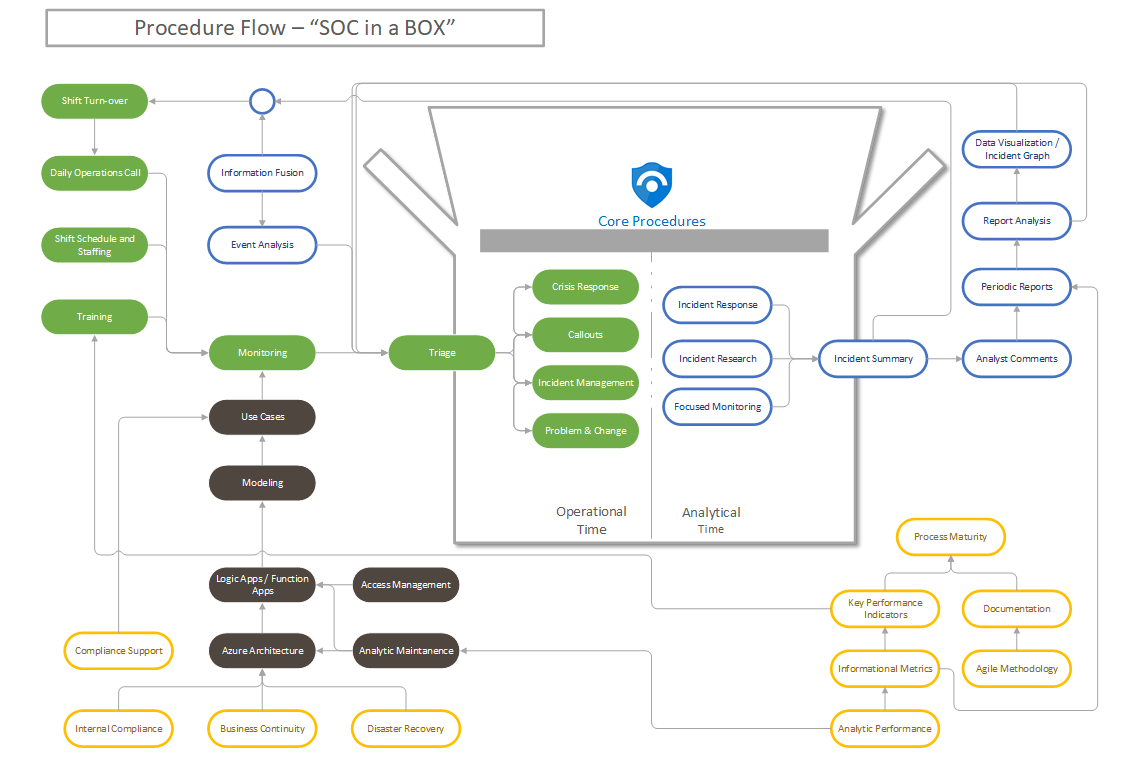
## Additional Categories

| Additional Categories | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Process Hierarchy | Procedure Flow | SOC Roles and Responsibilities | SOC Contacts & Procedures | SOC Incident Actions | SOC Tools & Resources | SOC Training |

## Procedure Flow

This is a visual representation of the procedures that drive Analytics and Operations within the SOC.

For example, business functions and compliance requirements drive use cases. SOC Operations and shift changes impact how incidents are triaged. This is a cycle that is fed by the [CUSTOMERS] SOC Analytic, Business, and Operational processes, Compliance Frameworks, and staffing practices.



# 

# 

# 

# 

# SOC Contacts

## SOC Contacts

| SOC Team Contacts | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Name | Title | Primary Phone | Secondary Phone | Office Line | User ID | Location | Knowledge Base Pages |

## 

## SOC Workstations

| SOC Workstations | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| User | Location | Internal Line | Workstation Name | IP Address | Mac Address | Serial Number |

## 

## Pager Contact Information for Security

| Pager Contact Information for Security | | | |
| --- | --- | --- | --- |
| Team Name | Pager Info. for Outlook | Phone Number | Manager |

## 

## General IT & Emergency Contacts

| General IT & Emergency Contacts | | |
| --- | --- | --- |
| Team Name | Phone Number | Description |

## 

## Departmental Contacts

| Departmental Contacts | | | | | |
| --- | --- | --- | --- | --- | --- |
| Department | Manager | Individual(s) | Items Responsible | Manager Phone | AD Group |

## 

## Email Distribution Lists

| Email Distribution Lists | | |
| --- | --- | --- |
| Team Name | Email | Description |

## 

## External Contacts

| External Contacts | | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
| Vendor | Contact Name | Position | Area of Expertise | Email | Phone | Alt Phone |

## 

## Internal Contacts

| Internal Contacts | | | | | |  |
| --- | --- | --- | --- | --- | --- | --- |
| Vendor | Contact Name | Position | Area of Expertise | Email | Phone | Alt Phone |

# 

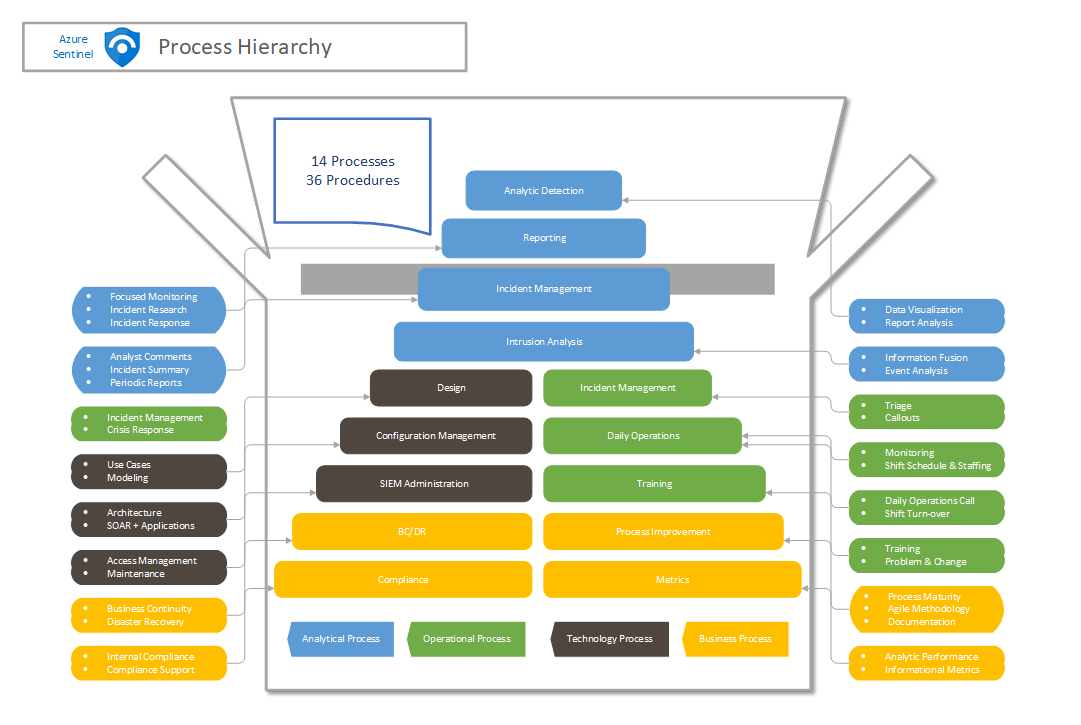
# SOC Process Hierarchy

## Purpose

This diagram shows how each Process & Procedure is mapped and outlined.

## Description

**Business processes are the foundation of the Process and Procedure Pyramid that drives Technology and Operational processes. At the top are customized Analytic use cases, that result in Detection and Remediation.**

****

# 

# SOC Roles & Responsibilities

## Roles & Responsibilities

This section provides a high level overview of the needed roles and responsibilities for successfully operating and maintaining a Security Operations Solution to satisfy the business requirements defined.

## Director – Security Operations

The Director – Security Operations is responsible for setting the tone and direction of the Security Operations Center (SOC), defining its mission and communicating with senior management and other teams to accomplish its tasks.

The Director manages the overall relationships with:

* First Line Senior Management
* Second Line
* Compliance
* Audit

## Manager – Security Operations Center (SOC)

The Manager – Security Analysis is responsible for leading the day to day operations of the SOC analyst staff. The role coordinates and works with the SOC Analysts to make sure that the analysts processes and technology are meeting the SOC security monitoring, analysis, and escalation objectives, organization service level agreements, objectives, and metrics.

In addition, the Manager of SOC Security Analysts will:

* Ensure daily operational processes effectively support SOC operations objectives.
* Execute continuous process improvement.
* Interface with other SOC and outside teams.
* Manage the process improvement program for SOC processes.
* Ensure that all SOC personnel issues are being addressed.
* Ensure senior management is aware of any issues or incidents.
* Ensure all SOC staff receive development guidance in accordance with the practices and standards of the SOC.
* Manage shift scheduling. Manage regular, holiday, illness, vacation and emergency scheduling
* Conducts shift turnovers and briefings.
* Own the successful completion of all daily operational processes and procedures.
* Ensure analysts follow existing procedures and all procedures are documented in accordance with local guidelines.
* Track tactical issues in execution of all SOC responsibilities.
* Document and track analyst training requirements.

## SOC Level 1 Analyst

A Level 1 SOC Analyst executes daily operations procedures as a matter of daily responsibility. The role of an SOC Analyst is the detailed and repeatable execution of all operational tasks as documented in processes and subordinate procedures. Specifically, the SOC Analyst will be responsible for monitoring the Azure Sentinel Incident Blade for security events/alerts/incidents and closing or escalating those as necessary. SOC Analysts maintain the group email address and distribution lists, answer SOC main phone lines, and update all relevant documentation such as shift logs and tickets.

Specifically, the SOC Level 1 Analyst(s) will:

* Rapidly identify, categorize, prioritize and Triage Incidents as the initial step for the enterprise using all available CUSTOMER's log and intelligence sources to include but not limited to:
* Firewalls
* Systems and Network Devices
* Web Proxies
* Intrusion Detection/Prevention Systems
* Data Loss Prevention
* Antivirus Systems
* OneNote Framework

1. Monitor incoming event queues for potential security incidents using Azure Sentinel per operational procedures.
2. Perform initial investigation and triage of potential incidents, and escalate or close Incidents as applicable.
3. Use available SOC tools for historical analysis purposes as necessary for detected Alerts/Incidents; for example, historical searches using Azure Sentinel Log Analytics.
4. Monitor SOC e-mail queue for potential event reporting from outside entities and individual users.
5. Maintain SOC shift logs with relevant activity from analyst shift.
6. Document investigation results, ensuring relevant details are passed to the Secondary Analysts for final event analysis.

* Update/reference SOC collaboration tool (Wiki, OneNote) as necessary for changes to SOC processes and procedures, and ingest of SOC daily intelligence reports and previous shift logs.
* Conduct research and document Alerts/Events of interest within the scope of IT Security

Additionally, Level 1 Analysts who have tenure in security monitoring of more than one year will:

* Track tactical issues in execution of SOC responsibilities
* Mentor junior analysts to improve detection/analytical capabilities within the SOC.
* Manage SOC event and information intake to include gathering intelligence reports, monitoring ticket queues, investigating reported incidents, and interacting with other security and network groups as necessary.
* Coordinate with SIEM Engineers to tune Events and Alerts.
* Serve as shift subject matter experts on incident detection and analysis techniques providing guidance to junior analysts and making recommendations to organizational managers.

## SOC Level 2 Analyst

The Level 2 Analyst ensures incidents are detected and tracked in a timely manner. The Level 2 Analyst owns the successful adherence to all procedures executed during their presence in the SOC including documentation and measurement of all subordinate procedures as well as the continual improvements to them. As the senior analysts on a shift, SOC Level 2 Analysts have final decision authority for escalation of Incidents inside the SOC and will serve as senior mentor to SOC Level 1 staff.

Additionally, the SOC Level 2 Analyst(s) will:

* Track tactical issues in execution of SOC responsibilities
* Monitor Level 1 Analyst performance investigating incoming Incidents using SOC-available tools.
* Ensure SOC Triage Tagged Incidents are addressed in a timely manner using available reporting and metrics.
* Investigate Level 1 escalated Incidents.
* Mentor Level 1 Analysts to improve detection/analytical capabilities within the SOC.
* Manage SOC event and information intake to include gathering intelligence reports, monitoring ticket queues, investigating reported incidents, and interacting with other security and network groups as necessary.
* Coordinate with SIEM Engineers to tune Alerts and Events.
* Serve as shift subject matter experts on incident detection and analysis techniques providing guidance to junior analysts and making recommendations to organizational managers.
* Drive and monitor shift-related metrics processes ensuring applicable reporting is gathered and disseminated per SOC requirements.

Finally, the Information Fusion Procedure, where various data inputs are fed to both operations and engineering is primarily driven by the assigned Level 2 Analysts. These senior analysts will gather information, organize it into an accessible format and ensure its full dissemination.

## SOC Level 3 Analyst

A Level 3 Analyst is a subject matter expert responsible for managing threats, disseminating information, and handling, responding to, and investigating all incident escalations from the CUSTOMER Security Operations Center. Level 3 team members are responsible for coordinating with the CUSTOMER CSIRT process when necessary, and managing incidents throughout the event life-cycle. Level 3 team members will further an investigation and ensure root cause and resolution for metrics, tracking, lessons learned are compiled, documented and disseminated in conjunction with the CIRT process.

They will provide insight and expertise to examine malicious code (malware), attack vectors, network communication methods, analyze threats against target systems and networks, determine target network capabilities and vulnerabilities, support development and maintenance of new tools and techniques to exploit specific targets, and produce technical after-action reports in support of the SOC. Level 3 members will be the focal point for critical security Alert, Events and Incidents and will serve as subject matter experts in providing recommendations to the SOC Incident Manager and other members of Information Security and IT management for escalation and remediation. Level 3 Analysts are also responsible for training and mentoring their Level 2 peers in order to improve SOC Analyst capability. Finally, Level 3 members will work with the SIEM Engineers to develop and refine use cases within Azure Sentinel focusing on emerging threats.

## Cyber Intelligence Analyst

The Cyber Intelligence Analyst role is responsible for intelligence collection, analysis, and dissemination for use in development of specific cyber monitoring capabilities. The Intelligence Analyst conducts research and develops/delivers timely recommendations to the SOC Analysts, incident responders, and SIEM engineers. The analyst will research adversary tactics, techniques, and procedures to determine patterns in network or system activity and associated malware. They will coordinate closely with security engineers and Second Line Intelligence peers to make changes to security tools to detect the latest threats.

The Cyber Intelligence Analyst will also:

* Maintain relationships with the CUSTOMER Corporate Information Security intelligence peers, Industry peers, and law enforcement community to be able to leverage information sharing networks
* Perform proactive research to identify and characterize new emerging threats, vulnerabilities, and risks
* Brief executive management on current threat landscape in written or oral communication
* Develop actionable intelligence to drive countermeasure development
* Share operational threat intelligence with SOC Analyst peers
* Work closely with security analysts to get direct feedback about new, unknown suspicious behavior, and indicators
* Research, analyze, and synthesize large amounts of data and information.
* Work closely with content & policy engineers to provide information on detection pattern for new upcoming threats.
* Participate in an on-call rotation

## Manager – Incident Response

The Manager – Incident Response is responsible for leading the IR effort of the SOC. This role engages with other First Line and Second Line teams to define incident response processes

In addition, the Manager – Incident Response will:

* Ensure security incidents are tracked and documented.
* Interface with other SOC and outside teams.
* Execute continuous process improvement.
* Manage the process improvement program for SOC IR processes.
* Ensure senior management is aware of any issues or incidents.
* Lead root cause analysis and post-mortem dialogue after significant Incidents to capture lessons learned and define process or technology improvements

## Incident Response Analyst

An Incident Response Analyst is a subject matter expert responsible for managing threats, disseminating information, and handling, responding to, and investigating all incident escalations from the CUSTOMER SOC. Incident Response Analysts are responsible for coordinating with the CUSTOMER Corporate Information Security (CIS) process when necessary, and managing incidents throughout the event life-cycle. Incident Response Analysts will further an investigation and ensure root cause and resolution for metrics, tracking, and lessons learned are compiled, documented and disseminated in conjunction with the CIS process.

They will provide insight and expertise to examine malicious code (malware) alerts, attack vectors, network communication methods, analyze threats against target systems and networks, determine target network capabilities and vulnerabilities, support development and maintenance of new tools and techniques to exploit specific targets, and produce technical after-action reports in support of the SOC. Incident Response Analysts will be the focal point for critical security Alerts, Events and Incidents and will serve as subject matter experts in providing recommendations to the SOC Incident Manager and other members of Information Security and IT management for escalation and remediation.

Incident Response Analysts are also responsible for training and mentoring their Security Analyst peers in order to improve SOC analyst capability. Finally, Incident Response Analysts will work with the SIEM Engineers to develop and refine use cases within Azure Sentinel focusing on emerging threats.

## Forensic Analyst / Investigator

The Forensic Analyst is responsible for the development and maturity of the forensic and investigations program within the CUSTOMER organization. The Forensics Analyst performs a variety of highly technical analyses and procedures dealing with the collection, processing, preservation, analysis, and presentation of computer related evidence. They will examine malicious code (malware), attack vectors, and network communication methods, and analyze against target systems and networks, determine target network capabilities and vulnerabilities, support development and maintenance of new tools and techniques to exploit specific targets, and produce technical, after-action reports in support of the CUSTOMER.

Additional responsibilities include:

* The Forensic Analyst/Investigator will conduct forensics analysis on systems and ensure root cause and resolution for metrics, tracking and lessons learned are compiled, documented and disseminated.
* Use of forensic tools and investigative methods to find specific electronic data, including internet use history, processing documents, images, and other files.
* The Forensic Analyst is responsible for disseminating and reporting cyber-related activities, conducting vulnerability analyses, conducting risk management of computer systems and recovering information from computers and data storage devices.
* Analyze and review escalated cases until closure; this includes investigating and recommending appropriate corrective actions for data security incidents which includes communicating with the implementation staff responsible.
* Perform post mortem analysis on logs, traffic flows, and other activities to identify malicious activity.
* Research, develop, and keep abreast of testing tools, techniques, and process improvements in support of security event detection and incident response.
* Reverse engineer and analyze binaries, files, and other malicious attack artifacts.
* Establish, maintain and ensure complete chain of custody of forensic evidence.
* Recovers and examines data from computers and other electronic storage devices in order to use the data as evidence in criminal prosecutions.
* When equipment is damaged, the forensic analyst must dismantle and rebuild the system in order to recover lost data.
* Analyst writes up technical reports detailing how the computer evidence was discovered and all of the steps taken during the retrieval process.
* The Analyst also gives testimony in court regarding the evidence he or she collected. The Analyst keeps current on new methodologies and forensic technology, and trains law enforcement officers on proper procedure with regard to computer evidence.
* The Forensic Analyst will contribute to the design and development of innovative research projects and attend and participate in professional conferences to stay abreast of new trends and innovations in the field of information systems and/or cyber security.
* This expert is not only proficient in the latest forensic response and reverse engineering skills, but is astute in the latest exploit methodologies.
* He/she will provide significant input into the design and development of the organizations working information security systems operations and maintain strategy and methodology to comply with the organization’s cyber security standards and mission.

## SIEM Engineer/Content Developer

The SIEM Engineer is primarily responsible for the administration, apps & infrastructure, playbooks,azure functions, i.e. architecture, configuration and analytic (KQL) performance within Azure Sentinel. The engineer performs all administration, development, management, configuration, and testing tasks related to Azure Sentinel. SIEM Engineers will be responsible for content development including reports, dashboards, analytic (KQL) rules, filters, and metrics. The SIEM Engineer also develops, implements, and executes standard procedures for the "front-end" operation within Azure Sentinel. The SIEM engineer will also communicate with the SOC Manager and Analysts to optimize the KQL (analytics) performance to better meet the needs of the SOC.

Other duties include:

1. Developing, implementing, and executing standard procedures for the administration, backup, disaster recovery, and operation of Azure Sentinel including:

* Operating system security hardening (vms, azure monitor connectors)
* Backup management (azure storage, Azure Data Explorer, other)
* Capacity planning (Long-term/Short-term storage)
* Change management (Analytic(Detections)/Workbooks/Playbooks/Notebooks versioning)
* Version/patch management (vms for azure monitor connectors)
* Lifecycle upgrade management

1. Tune Azure Sentinel KQL performance and event data quality to maximize Azure Sentinel efficiency and assists with Data Source correlation using Azure Sentinel. Additionally, the SIEM Engineer is responsible to ensure all Azure Sentinel components perform as expected meeting established service level objectives for optimal system uptime.

## Cybersecurity Data Scientist

The Cybersecurity Data Scientist role is responsible for design, development, and support of advanced security analytics within the CUSTOMER environment using big data technology solutions. This role interfaces directly with the intelligence, forensics, and analysis teams. This role will involve working directly with security leaders throughout the CUSTOMER organization to develop solutions to complex predictive analytic problems involving diverse input data sources including real-time data. This role works alongside a team of Hadoop engineers to develop theories using security data, analyze the requirements of our stakeholders and provide expertise in a complex technical environment. The role provides expertise in exploratory data analysis, pattern discovery and advanced analytical techniques to anticipate or detect undiscovered threats as well as aid in historical search for forensic response situations. The role uses LogAnalytics/Azure ML and other Big Data tools to accomplish the applicable tasks.

## Responsibility Chart

RACI is an acronym for the four major headings in a responsibility chart:

| **Role** | **Individual** |
| --- | --- |
| Responsible | Individual or group actively working to achieve the task. This group reports to the individual Accountable for the completion of the task to verify scope and successful completion. |
| Accountable | Individual or group responsible for the completion of a given phase/task. |
| Consulted | Individuals who provide consulting input into the phase/task. The opportunity for the two way communication is provided to the consulted group. |
| Informed | Individuals who are informed of the progress of the phase/task. One way communication is provided to individuals in the informed group. |

## RACI Matrix

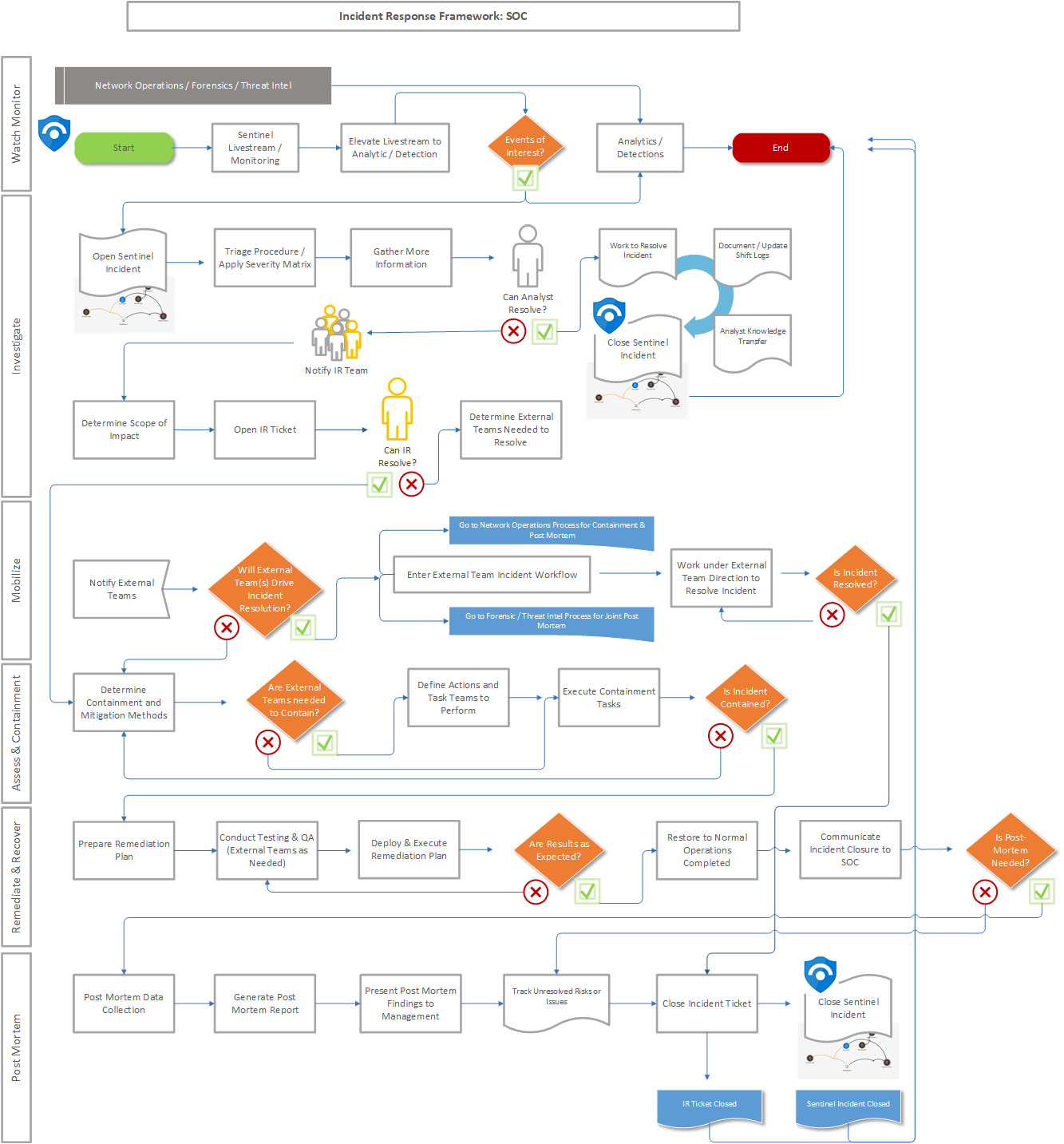
| **Phase/Role** | **Director - Security Operations** | **Manager - Security Analysis** | **Level 1 & Level 2 Analyst** | **Level 3 Analyst** | **Cyber Intelligence Analyst** | **Manager - IR** | **IR Analyst** | **Cybersecurity Data Scientist** | **Forensic Analyst/Investigator** | **Business Unit Management Teams** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Watch/  Monitor | A | A | R | I | I/C | I | - | - | - | - |
| Investigation | A | A | R | R | I/C | C | A/C | - | C/R | I |
| Assess & Contain | A | A | I | R | I/C | C | A/C | - | C/R | I/A |
| Remediate & Recover | A/C | A/C | I | I | I/C | A/C | A/C | C | C/R | I/A |
| Post Mortem | A/C | A/C | I | I | I/C | A/C | A/C | C | C/R | I/A |

# Incident Response Framework

## Incident Response Framework: Security Operations Center

## Description

This diagram describes how Sentinel is used from the initial monitoring of data sources through the Incident Response process to incident remediation, recovery and post mortem.



# SOC Incident Response Procedures

## Summary

**What is an Incident?** An incident is defined as a series of events that may compromise the integrity of a large number of systems, multiple organizational zones or networks resulting in catastrophic data loss, prolonged organizational downtime, or major financial impact. The CUSTOMER Security Operations Center organization will continuously work throughout the Incident Response process as a core component of conducting security monitoring and analysis.

The IR process describes the activities conducted throughout each response phase. The IR process enables the SOC to transition from each phase in an operationally sound manner, involving analysis, triage, case management, and escalation and ultimately engaging the CUSTOMER Incident Response Team (CUSTOMER -IRT) upon critical/urgent incidents which may impact the business and operations of the Organization, or Business Areas/Units.

## Purpose

The purpose of this process is to provide the SOC Analysts with detailed procedures for the handling of all events or incidents that occur within the CUSTOMER Enterprise. Incidents can be categorized as one of the following:

* Any malicious event (hack, leak, breach, compromise, etc.) to IP, PII, confidential data, digital assets, or any element of the network or the digital assets that can be accessed by it.
* Any violation of security or corporate policy by anyone granted legitimate access including vendors, partners, full-time employee (FTE), contingent staffing groups (CSG), guests, interns, contractors, etc.
* Any malicious event resulting in loss or compromise to any IP, PII, confidential data, digital assets or the network (or anything connected to it) caused by anyone granted access to that asset, or who gained access to it through a malicious act (virus, malware, hack, breach, worm, etc.). The daily process and procedures executed by the SOC with this IR process demonstrates how the organization addresses and manages security incidents.

## Incident Response Decision Matrix

## 

| **IR Decision Matrix** | | | |  |
| --- | --- | --- | --- | --- |
| Category | Description | Single Workstation | Multiple Workstations / Single HVT / Single HRT | Multiple HVTs / Multiple HRTs |
| Reconnaissance | This category involves the initial communications from a source (external or internal) to a target host. Common example of this traffic is scanning activity. | SEV-3 | SEV-3 | SEV-3 |
| Attack/Delivery | This category involves the delivery/transmission of malware. For example Phishing, USB Drives, websites hosting malicious content, etc. | SEV-3 | SEV-2 | SEV-1 |
| Host Exploitation | This category involves the possibility or probability that an attempt to deliver malware was successful. For example AV, IDS, or other security tools events. | SEV-3 | SEV-2 | SEV-1 |
| Binary Installation | This involves advanced attack vectors not monitored by conventional security tools. For example, additional registry settings, increasing or unidentified windows processes, security tools services terminated, and etc. | SEV-3 | SEV-3 | SEV-2 |
| C2 | This category involves an internal device possibly beaconing out to a control server. For example firewall logs indicating attempts from internal devices to IP’s identified as currently or at some point in the past, identified with malware. | SEV-3 | SEV-2 | SEV-1 |
| Local Compromise | This category involves the creation of local accounts, privilege escalation, compromise of existing local accounts, unapproved changes made to group policies, unapproved permission changes for file and folder access, and the use of common command line tools in Windows and Unix. | SEV-2 | SEV-2 | SEV-1 |
| Internal Recon | This category involves a compromised host profiling the network for other vulnerable targets which may suggest the use of active security tools such as netcat or is possibly a vulnerability scanner. | SEV-2 | SEV-2 | SEV-1 |
| Lateral Movement | This category involves the movement from the compromised host to other hosts. Examples in this area look for such events like net login, remote registry, remote WMI communications, remote group policy editor and remote session communications such as file share access, RDP, SSH, HTTP. | SEV-2 | SEV-2 | SEV-1 |
| Established Persistence | This category includes any activity that attackers may use to maintain their presence on a compromised network. Examples of this behavior are newly spawned communication services between internal hosts, such as HTTPS, between servers that should not provide this service; common unknown processes being found on multiple hosts; and new binaries being added to the compromised host. | SEV-2 | SEV-2 | SEV-1 |
| Stage & Exfiltration | This category involves an attacker taking active steps to steal and exfiltrate data. Examples of this activity are spikes in normal network traffic, or any other anomalous traffic that deviates from expected network traffic. | SEV-2 | SEV-2 | SEV-1 |
| Business Process | This category involves health events, testing, misconfigured devices, normal business ops. etc. | SEV-4 | SEV-4 | SEV-4 |
| Policy Violation | This category involves user behaviors associated with Policy Violations. | SEV-4 | SEV-4 | SEV-4 |

## 

## Scope

This process applies to all incidents that are presented to all SOC Analysts and also applies to the CUSTOMER's Incident Response Team tasked with monitoring, response and escalation.

## Definitions

* A **Security Event** is a change in the everyday operations of an asset/device (i.e. workstation, or server), network or information technology service, indicating that a security policy may have been violated or a security safeguard may have failed.
* A **Security Alert** is a correlation of Security Events together that identify a Security Risk.
* A **Security Incident** is defined as a series of events that may compromise the integrity of a large number of systems, multiple organizational zones or networks resulting in catastrophic data loss, prolonged organizational downtime, or major financial impact.
* A **High-Value Target (HVT)** is a person or asset that an attacker/intruder is attempting to exploit for person gain.

1. Assets which may contain Personally Identifiable Information (PII), Protected Critical Infrastructure Information (PCII), Intellectual Property (IP), Application and/or Development Source Code/Builds, or Electronic Transactions such as Credit Cards, or Stock trades.
2. Persons who may have business/company plans such as future acquisitions, new or emerging products/services, competitive product or service pricing and licensing. The objective of the SOC is to prioritize events where the High Value Assets are either the target or the source of the alert to conduct further analysis and investigation.

* **Personal Identifiable Information (PII)** is defined as any information that can be used to distinguish or trace an individual‘s identity,such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII data can be sensitive or non-sensitive.
* **Payment Card Industry (PCI)** PCI can be described as a set of security standards that were developed to protect card information during and after a financial transaction.
* **Sarbanes-Oxley (SOX)** compliance is best defined as legislation that was passed by the U.S. Congress to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise, as well as improve the accuracy of corporate disclosures.

## Severity Definitions

| **Severity 1 (Critical)** |  |
| --- | --- |
|  | **Critical Compromise, Major Service disruption or publicly displayed attack** |
|  | - Mission critical systems that support multiple businesses (systems defined as mission critical per Ops/Tech) OR sectors of the critical infrastructure (systems defined as Tier 0 for BCP/DR purposes)  - CUSTOMER has experienced a substantial loss of service and/or revenue  - Prevents CUSTOMER from making sales, or meeting legal or contractual obligations  - Potential regulatory fines or penalties  - Critical business impact to the company; competitive edge, reputational, data-privacy breach  - All or a substantial portion of CUSTOMER's mission critical data is at a significant risk of loss or corruption  - CUSTOMER business operations have been severely disrupted  - Potential large financial risk or legal liability  - Multiple systems (HVT), significant number of workstations, groups and users affected; high probability of propagation  - Mission critical system (e.g., payroll system) to a single business  - Significant and immediate threat to human safety  - Complete system compromise and possible full data-privacy breach  - Law Enforcement assistance is required  - Severity 2 events that are not resolved within the established Service-Level Agreements (SLAs) |
|  | **Examples:** |
|  | - Unauthorized access to sensitive systems (HR, Payroll, Finance, etc)  - Distributed Denial of Service Attacks or DoS Attacks  - Theft of computer systems and/or media containing sensitive/confidential information  - Malware causing destructive outbreak to a large number of workstations or servers (Zero day attacks)  - Defacement of CUSTOMER Web Sites  - Vulnerability on an CUSTOMER transactional server or subnet |

## 

| **Severity 2 (Major)** |  |
| --- | --- |
|  | **Serious Impact or Compromise, Incident/Attack affects multiple organizations/customers** |
|  | - Operations can continue in a restricted fashion, although long-term productivity might be adversely affected  - Organization has lost the ability to provide a critical service to a subset of system users  - Single High Value Targets affected or potentially compromised  - Impact to company confidential data  - Major or business-critical applications are affected  - Multiple systems that contain PII or PCI and/or users affected  - Critical impact to the organization (reputational)  - Severity 3 events that are not resolved within the established Service-Level Agreements (SLAs) |
|  | **Examples:** |
|  | - Improper usage of high-level accounts such as root or administrator  - Phishing threats to compromise internal, sensitive data  - Vulnerability on a CUSTOMER non-transactional server or subnet  - Multiple users/workstations infected by malware  - Unauthorized disclosure of CUSTOMER internal or confidential information (i.e. email, blogs, news groups)  - Spear-phishing attempts targeting CUSTOMER executives  - Internal web site was compromised without authorization |

## 

| **Severity 3 (Moderate)** |  |
| --- | --- |
|  | **Intermittent security alerts, moderate security impact** |
|  | - Non-critical systems (e.g., associate workstations), OR Non-critical infrastructure; internal impact is less than 5%  - Medium Severity, typically issues such as policy violations, single system infections and/or whereas the malicious code is known and contained  - Escalation directly to the respective Business Unit for remediation  - Severity 4 events that are not resolved within the established Service-Level Agreements (SLAs) |
|  | **Examples:** |
|  | - Isolated reconnaissance activities (network) by potential attackers  - Password policy violation by an employee  - Virus/Malware infection isolated to an individual user  - Single report of suspicion that someone has gained unauthorized access to his/her/their account  - Phishing/spear-phishing threat to compromise customer data  - Detection and removal of viruses by a server before it enters the network  - Repeated port scanning from same external source |

## 

| **Severity 4 (Minor)** |  |
| --- | --- |
|  | **Informational, some security impact** |
|  | - Non-critical systems (e.g., associate workstations), OR Non-critical infrastructure  - No effect to the organization’s ability to provide all services to all users  - No breach of data / information was exfiltrated, changed, deleted, or otherwise compromised  - Single systems and/or users affected that contains PII or PCI  - Minimal recovery required  - Escalation directly to the respective Business Unit for remediation |
|  | **Examples:** |
|  | - Receipt of e-mail expressing “low-level” threat  - Discovery of a Phishing event without report of compromise |

## Incident Response Methodology

## Incident Preparation

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. The SOC should have preparatory measures to ensure that they can respond effectively to security events/incidents. All documentation should be updated/maintained in the SOC Knowledge Base (Wiki, OneNote).

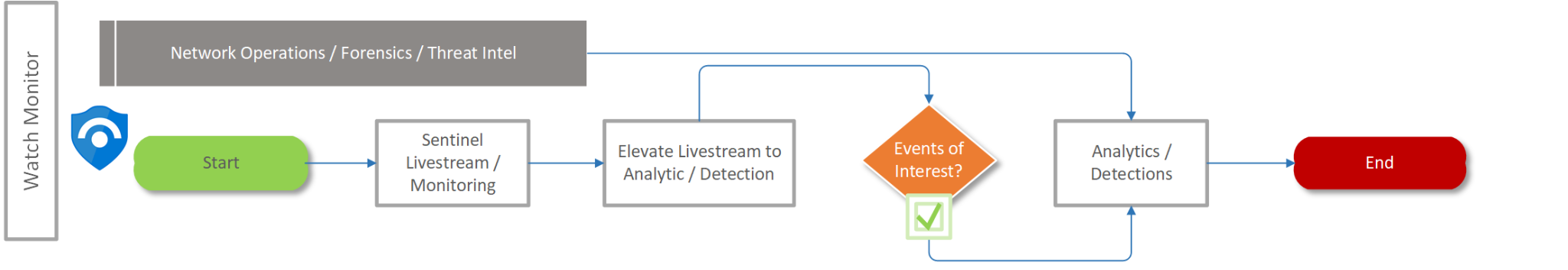
Recommended actions include:

* Maintain Contact information for team members and others within and outside the organization (primary and backup contacts)
* Maintain escalation procedures (phone numbers & email addresses)
* Assist with maintaining IRT documentation
* Have a War Room available

## Watch / Monitor Phase (Detection)

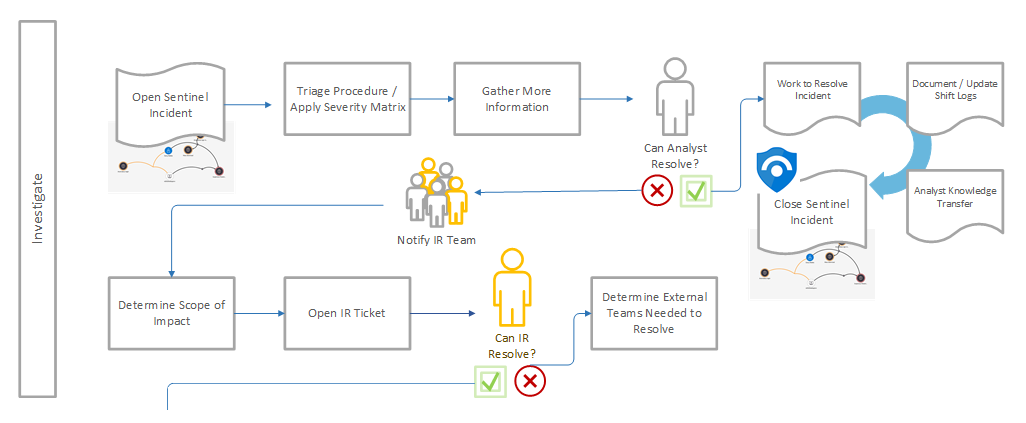
The SOC group should strive to detect and validate security events and incidents rapidly because infections can spread through an organization within a matter of minutes. Early detection can help an organization minimize the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organization sustains.

START --> Create / Monitor Azure Sentinel Livestream --> Elevate Livestream to Analytic/Detection --> Fires Alert and Creates an Incident



## Investigation Phase

A SOC Analyst needs to determine what action to take based on Incidents observed within Azure Sentinel. Triage is the process of evaluating multiple events to determine which are the most critical and prioritizing your response based on this analysis. This procedure will result in one of the listed response actions.



Determine Category Type & Action Needed

The SOC Analyst should apply the decision matrix below using the Category Type and asset priority. This is used in conjunction with the SOC Response Procedures for the rule triggered. The severities defined below are based on adaptations from the CUSTOMER Company Threat Matrix.

Analysts also need to note the following:

* If there is a fast spreading new worm or virus do an immediate callout and include SOC management
* If any security device (FW, IDS/IPS sensor, Web Proxy) fails, notify engineers via Remedy for instructions.
* If traffic appears to be part of a vulnerability scan or penetration test, check the Vulnerability Scan Scheduling page for verification.

## Initiate Action

The Analysts should initiate appropriate response action based on the outcome of the decision matrix above. If any particular Alert/Incident is dismissed, Analysts should follow Azure Sentinel's Incident Procedures.

* **SEV-1** = Annotate the Incident/Alert and initiate the Critical Call out Procedures with a response time requirement of 15 minutes.
* **SEV-2** = Annotate the Incident/Alert and initiate the Urgent Call out Procedures with a response time requirement of 30 minutes.
* **SEV-3** = Annotate Incident/Alert. Work Incident internally, if a callout is needed promote case to a SEV-2. Azure Sentinel Incidents created will be under the Incident schema
* **SEV-4** = Annotate Incident/Alert. Low priority, work internally, if callout is necessary, promote case to a SEV-2.

Once the SOC Analysts suspects a security event or an incident is occurring or has occurred and has been deemed actionable, it is important to immediately begin documentation of all facts related to that event. Every task completed from initial identification of an event until final resolution, should be documented in detail and time-stamped.

The SOC will open an Azure Sentinel Incident in the Azure Sentinel Incident Blade. At a minimum, the following should be documented in this case:

* Current Status of the Alert/Events or the incident
* Type of Alerts/Events or Incident (e.g., disruption of service, malicious code, unauthorized access, inappropriate usage)
* Full name of the Analyst (will retain case ownership)
* Summary of the event or incident
* Contact information for all involved parties (e.g., system owners, system administrators)
* List of all pertinent logs and technical information gathered
* Cause of the event / incident (e.g., misconfigured application, unpatched host)
* Business impact of the event
* Actions Taken by all SOC Analyst(s) or Incident Response Team
* Contact Information for Other Teams Involved
* Notes/Comments from other Incident Handlers
* Next Steps/Actions to be Taken (e.g., Waiting for system to be re-imaged, waiting for system patch to be applied to vulnerable system)

## Incident Information

It has been identified that a standard set of incident related data fields need to be collected for each incident. This will not only facilitate more effective and consistent incident handling, but also assist the organization in meeting applicable incident reporting requirements. The list below provides information to be collected for all incidents. These are not intended to be comprehensive, and more/less information will be collected based on the specific context of the incident.

Incident Details

* Log of actions taken by all handlers
* Date/time (including time zone) when the incident was discovered
* Estimated date/time (including time zone) when the incident started
* Type of incident (e.g., denial of service, malicious code, unauthorized access, inappropriate usage)
* Physical location of the incident (if known)
* Source/cause of the incident (if known), including hostnames and IP addresses
* Description of the incident (e.g., how it was detected, what occurred)
* Operating system, version, patch level and installed software
* Documentation of all gaps identified during the incident handling. For instance, missing asset information, delivery time of supportive departments, etc.
* Endpoint Threat Protection installed, enabled, and up-to-date (yes/no)
* Description of affected resources (e.g., networks, hosts, applications, data), including systems’ hostnames, IP addresses, and business function
* Estimated technical impact of the incident (e.g., data deleted, system crashed, application unavailable)
* Response actions performed (e.g., shut off host, disconnect host from network)
* Other organizations contacted (e.g., software vendor)
* If any PII was compromised during the incident, what type of PII was it?
* Do the affected systems contain any sensitive data (i.e. PII, PCI or SOX)?

Signs of an incident that can be categorized as indicators and precursors.

* Precursors are signs that an incident may occur in the future.
* A threat from a hacktivist group stating the group will attack CUSTOMER or CUSTOMER’s customers
* An announcement of a new exploit that targets vulnerable CUSTOMER's servers
* Web server log entries revealing unauthorized Web vulnerability scanning
* Upcoming termination of a CUSTOMER's employee or contingent worker
* Indicators are signs that an incident may have occurred or is actively occurring.
* Network IDS/IPS sensor alerts when a buffer overflow attempt occurs against a CUSTOMER server
* Endpoint Threat Protection software alerts after detecting malware on a host
* Web Server crashes
* User complaints regarding poor network connectivity
* System Administrator identifies suspicious executable on a CUSTOMER server
* Business Criticality: This analysis will consider potential financial, brand, customer and service impact as the primary criteria for incident prioritization.
* Considerations:
* What is the business purpose of each of the systems that are involved in the incident, attacker and target?
* Do these systems host a business critical application or are they in the same network zone with systems that are business critical?
* Do the involved systems store or transmit PCI or PII data?

## Continue to Monitor Activity

If necessary, initiate the Focused Monitoring procedures in support of other teams. Using the Focus Monitoring Procedure to initiate a LiveStream to watch for ongoing Alerts or Events as they occur.

## Document Activity in the Shift Log

Document all activity (including false positives) in the Shift Log using the Shift Log Management guidelines.

## Follow Up on Activity

Ensure that the appropriate response action is fully executed and the ticketing and closure procedures are completed.

## Service Level Objectives (SLOs)

Within the SOC, several metrics are reported weekly to management. As part of this process service level objectives must be defined, measured and reported. A service level objective (SLO) is a key element of a service level agreement (SLA) between a service provider and a customer. While incidents may vary in the length of time needed to resolve, there are several metrics that can be defined.

## General goals:

Event annotation – All SOC Analysts will review every Incident in the Incident Blade within Azure Sentinel within 15 minutes of the Alert/Incident receipt time during normal business hours. All events from off hours will be analyzed within 4 hours of an analyst coming on duty.

## Incident management goals:

Incident Triage – All Incidents in "Open or Active" in the Incidents blade of Azure Sentinel will be triaged within 15 minutes of them being created and moved into the Secondary Analyst structure.

Investigations will be started on all Incidents within the following times based off of their priority: (All times are assuming business hours)

* **Severity 1: Immediately**
* **Severity 2: Within 10 minutes of triage**
* **Severity 3: Within 60 minutes of triage**
* **Severity 4: Within 24 hours of triage**

## Remediation SLOs

| **Incident Severity Table** |  |  |
| --- | --- | --- |
| Description | Scope | System Criticality |
| Severity 1 – Critical | Pervasive | Critical |
| Severity 2 - Major | Wide | High |
| Severity 3 – Moderate | Significant | Medium |
| Severity 4 – Minor | Narrow | Low |

* Severity 1 (SEV-1) – A Severity 1 Incident is worked as the matter of highest Severity until completely resolved. These cases are often handled with a war room response and can require a round the clock response.
* Severity 2 (SEV-2) – A Severity 2 Incident is worked as a matter of high Severity until completely resolved. These are handled at any time of the day or night as they are detected or reported, but after initial triage may be delayed until business hours if appropriate.
* Severity 3 (SEV-3) – A Severity 3 Incident is worked urgently during business hours until resolved.
* Severity 4 (SEV-4) – A Severity 4 Incident is worked best effort on business days until resolved.

## 

## Notification SLOs

| **Severity** | **Who** | **When** | **How** |
| --- | --- | --- | --- |
| Sev-1 | - ALL SOC Analysts  - IR Team  - SOC Manager  - Director of IT Security  - CISO | **First Notification:** Immediately  **Subsequent notifications:** 15 minutes or as announced | Teams  Teams / Phone & Encrypt Email  Teams / Phone & Encrypt Email  Encrypted Email  Teams WarRoom / Phone |
| Sev-2 | - ALL SOC Analysts  - IR Team  - SOC Manager | **First Notification:** 10 Minutes  **Subsequent notifications:** 30 minutes or as announced | Teams  Teams  Teams |
| Sev-3 | - ALL SOC Analysts  - SOC Manager | **First Notification:** 60 minutes  **Subsequent notifications:** Daily or as announced | Teams  Teams |
| Sev-4 | - ALL SOC Analysts | **First Notification:** 24 Hrs  **Subsequent notifications:** Daily or as announced | Teams |

## Dependencies within the Organization

It is important to identify other groups within this organization that may be needed to participate in incident handling so that their cooperation can be solicited before it is needed. Every incident response team relies on the expertise, judgment, and abilities of others, including:

* Management: Management invariably plays a pivotal role in incident response. In the most fundamental sense, management establishes incident response policy, budget, and staffing. Ultimately, management is held responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting. Without management support, an incident response team is unlikely to be successful.
* Cyber Security: Members of the information security team are often the first to recognize that an incident has occurred or is occurring and may perform the initial analysis of incidents. In addition, information security staff members may be needed during other stages of incident handling—for example, altering network security controls (e.g., firewall rules) to contain an incident.
* IT Support: IT technical experts (e.g., system administrators, network administrators, and software developers) not only have the needed technical skills to assist during an incident but also usually have the best understanding of the technology with which they deal on a daily basis. This understanding can facilitate decisions such as whether to disconnect an attacked system from the network.

## Additional IR Phases

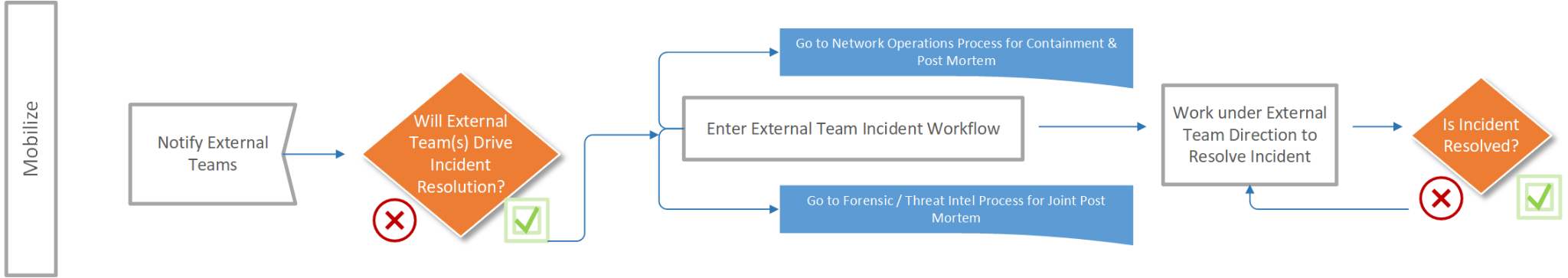
## Mobilize

During the Mobilize phase, the CUSTOMER Security Operations Center will engage the SOC Manager, the Incident Manager and members of the Incident Response Team (Level 3) if a critical incident or any event has been escalated from all SOC Analysts that has occurred. Additionally, they will provide all of the pertinent information that was gained from the previous phases.

The SOC-IM will reassess the severity/criticality of the incident prior to mobilization of the IRT. The SOC-IM will own and manage the incident moving forward. First, the SOC-IM will prepare an incident summary to inform the IRT and the senior management team that an incident has occurred and that the IR plan has been enacted.

Next, the SOC-IM will determine whether additional information or coordination with external teams is required. If all information gathered confirms the occurrence of a high severity incident, then the SOC-IM will notify the IRT and open a communications line to coordinate efforts.

An incident response team is typically composed of the SOC-IM and IRT; IT operations, network operations, business stakeholders, and executive management. In some instances, legal and public relations (PR) organizations will also collaborate as necessary.

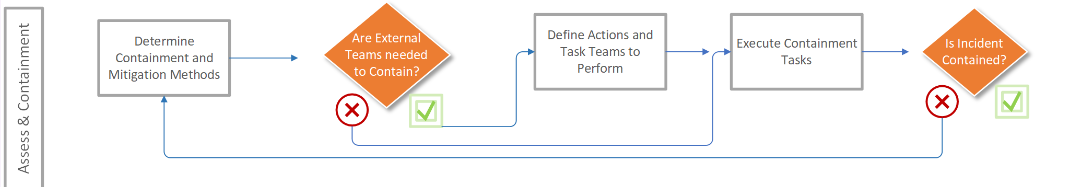


## Assessment and Containment

An incident may need to be contained and/or quarantined to keep it from spreading and to prevent further damage or loss from occurring. During this phase, efforts should be taken to keep potential evidence intact, while balancing the needs of the system owner and the incident investigator. In some cases, it may be necessary to either remove the system from the attacker’s ability to access it, or to contain it in some way that is not detectable. Failure in this regard can result in serious damage to the system and related infrastructure as the attacker recognizes the actions you are taking. It is important to consider that some attacks may cause additional damage when contained and/or quarantined, so the SOC should not assume that because a host has been removed from the network, further damage to the host has been prevented.

* Containment Considerations:

1. Is the incident currently on-going?
2. What is the business impact?
3. Is stolen information stored on the compromised system? If so this system may be monitored by the attacker and there may be automated routines to delete evidence which would likely destroy the system.
4. What is the production impact if you pull the network cable or remove the system from production status?
5. Does the containment strategy affect our ability to preserve evidence?
6. What effect does the strategy have on service availability (e.g., network connectivity, services provided to external parties)?
7. What amount of time and resources are needed to implement the strategy?
8. What is the effectiveness of the strategy (e.g., partial containment, full containment)?
9. What is the duration of the solution (e.g., emergency workaround, temporary workaround, permanent solution)?



## Technical Root Cause Analysis

Purpose:

The purpose of the technical root cause analysis is to determine the mechanism of attack, the modus operandi (M.O.) of the attacker and the extent of the compromise within the CUSTOMER Enterprise.

* Task 1 - Gather all technical information needed to research the details of the incident.

1. Potential Technical Information to Review:

1.1 Operating system logs (Windows/\*NIX)

1.2 Firewall logs

1.3 Router logs

1.4 Application logs

1.5 Proxy logs

1.6 IDS/IPS logs

1.7 Endpoint Threat Protection logs

1.8 DLP logs

1.9 The image of any virtual servers

1.10 Network packet captures

1.11 Any other information as discovered in the course of the investigation.

1. Obtain digital evidence from Windows Systems
2. Obtain digital evidence from Unix/Linux Systems

* Task 2 - Conduct a thorough technical review of collected technical information to determine the mechanism of the attack.

1. Analyzing Unknown Binaries with Bit9 and/or Carbon Black
2. Conducting Basic Static/Dynamic Malware Analysis with a known good Sandbox

* Task 3 - Review of the sequence and context of the attack to understand the Modus Operandi of the attacker.
* Task 4 - Review peer and similar systems to identify if more systems are involved in the incident.
* Task 5 - Identify and document any systemic weaknesses observed within the CUSTOMER Enterprise network.

## Remediation & Recovery

Once an incident has been contained and/or quarantined, it is necessary to eliminate components that allowed the incident to occur, as well as identify and mitigate all vulnerabilities that were exploited. During this phase, it is crucial to identify all affected hosts within the CUSTOMER Enterprise network, so that they can be remediated appropriately.

* Task 1 - Complete a peer review of incident details and proposed remediation to ensure consensus on the recommended approach and the details of the attack as documented in the security case.
* Task 2 - Conduct a remediation conference call (if needed), to disseminate and discuss recommended and required actions to remediate the incident.
* Task 3 - Add all IP addresses and/or host names involved in the incident to the Azure Sentinel compromised and/or hostile WatchList(s) to increase Incident Severity on any subsequent events/alerts detected. This connects directly to the focused monitoring procedures from the SOC team.
* Task 4 - Confirm remediation actions have been completed and conduct a final vulnerability assessment of the redeployed system, to prevent reinfection.

During the remediation and recovery phase, systems must be restored to normal operation. Depending on the nature of a particular incident, corrective actions could be related to technology, policies and procedures, and/or personnel.

Due to the nature of Advanced Persistent Threats (APTs), multiple attack vectors and the sophisticated nature of cyber-attacks, attackers may leave behind undetected malware, or legitimate executable(s) which may contain a vulnerability or a backdoor on the compromised systems. To combat this threat, the SOC may require the impacted systems to be flattened, formatted,and reinstalled (FFR/wipe and reinstate) to restore the systems trust.



## Remediation Scenarios/Options:

* Simple changing of all passwords or removal of infected files.
* Minor modification to applicable applications and/or operating system reconfiguration.
* System restore from a clean backup.
* Completely rebuilding a system/asset; flattened, formatted, and reinstalled (FFR).

## General Recovery Guidance:

* Data should be restored from a trusted source and validated.
* The operating system and all applications should be updated wherever possible, patched, and all unnecessary services disabled.
* For purpose-built devices (i.e., routers, switches, and security appliances) consult the vendor for information on security conscious configurations.
* All system passwords should be changed and hosts with which the compromised system shared a trust relation examined for possible signs of compromise.
* If the root cause for the compromise has been determined, appropriate steps should be implemented to mitigate the risks.
* Focused Monitoring should be increased following an intrusion. Post compromise monitoring of a network will often reveal additional probes and may help identify additional compromised resources.

Note: Remediation & Recovery should be conducted in a phased approach so that remediation steps are prioritized appropriately. During the early phases, the intent should be to increase the security posture with quick, high value changes to prevent future incidents and further outbreaks. The later phases should be focused on long term changes (i.e., infrastructure changes) and ongoing efforts to keep the CUSTOMER Enterprise network as secure as possible.

## Post Mortem (Lessons Learned)

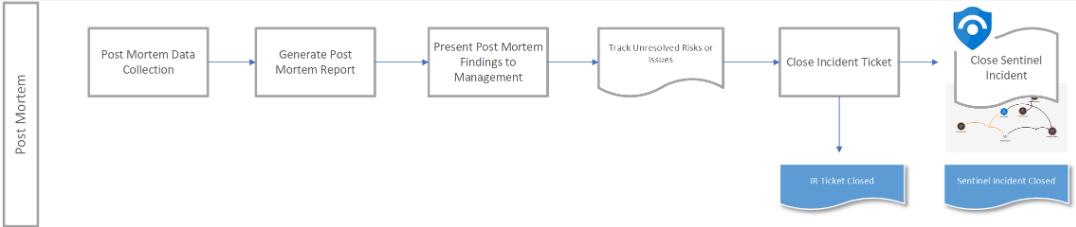
Purpose:

One of the most important parts of the incident management process is also the most often omitted: learning and improving. The CUSTOMER SOC will conduct a “lessons learned” meeting with all involved parties after a major incident, and periodically after lesser incidents. Doing so is extremely helpful in improving security measures and the incident handling process itself. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred,what was done to intervene, and how well intervention worked.

Questions to be answered in the lessons learned meeting include:

* Exactly what happened, and at what times?
* How well did the staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
* What information was needed sooner?
* Were any steps or actions taken that might have inhibited the recovery?
* What would the staff and management do differently the next time a similar incident occurs?
* What corrective actions can prevent similar incidents in the future?
* What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

In addition, the SOC will compile a Post Mortem Report. The report shall describe the incident, investigation methods, general conclusion, recommendations to avoid future related incidents and, if appropriate, lessons learned from the investigation.



## Recommendations

* Small incidents need limited post incident analysis, with the exception of incidents performed through new attack methods that are of widespread concern and interest.
* Updating incident response policies and procedures is another important part of the lessons learned process. Postmortem analysis of the way an incident was handled will often reveal a missing step or an inaccuracy in a procedure, providing motivation for change.
* The response to an incident that has been resolved can be analyzed to determine how effective it was. The following are examples of performing an objective assessment of an incident:

1. Reviewing logs, forms, reports, and other incident documentation for adherence to established incident response policies and procedures
2. Identifying which precursors and indications of the incident were recorded to determine how effectively the incident was logged
3. Determining if the incident caused damage before it was detected
4. Determining if the actual cause of the incident was identified

# SOC Analytical Processes & Procedures

| **Process Name** | **Procedures** | **Description/Comments** |
| --- | --- | --- |
| Intrusion Analysis Process |  |  |
|  | Incident Triage Workflow & Narrative | Procedures for the SOC Analyst as Incidents enter the Azure Sentinel Incidents Blade |
|  | Incident Analysis | How analysts should utilize internal and external resources to perform security threat research |
|  | Information Fusion | How analysts should look at Incidents that are presented to them within the Azure Sentinel Incidents Blade |
|  | Focused Monitoring | How analysts should focus on specific Events/fields in order to broaden the search to find out more about what an IP, host, user, etc. is doing |
|  | SOC Use Cases | Use Cases designed, built and deployed for the SOC |
| Host Analysis Process |  |  |
| Subtle Event Process |  |  |
|  | Data Exploration | Procedures for using Azure Sentinel or other tools to visually review security events for abnormalities |

## Intrusion Analysis Process

**Purpose**

The purpose of this process is to support the SOC Analysts with a structured approach to the discipline of intrusion analysis and operational event management.

**Scope**

This process applies to all Incidents that are presented with the tag Triage, as this is the accountable tag for SOC operations. This also applies to all SOC Analysts tasked with monitoring, recognition and escalation.

**Process Summary**

All SOC Analysts will monitor the Azure Sentinel Incident Blade for Security Alerts turned Incident. They will evaluate and investigate these Incidents to determine if they represent significant security concerns.

An information security device detects some form of traffic that conforms to a suspicious pattern and then generates an event which is normalized, annotated, aggregated, correlated and displayed on the Azure Sentinel Incident Blade. The on-duty analyst(s) must then decide if this Incident warrants further analysis or some level of response. The process of analyzing this Incident is the subject of the procedures subordinate to this process. Once an Incident or series of Incident(s) has been analyzed and a decision made as to its validity, threat, and criticality, the Incident Triage Procedures provides a decision matrix to determine the appropriate level of response.

The Information Fusion Procedures spell out the detailed steps taken to ensure that all analysts have a comprehensive view of the current state of information security threats and vulnerabilities across the globe as well as within the CUSTOMER enterprise. This procedure will spell out the steps involved in the collection, analysis and dissemination of analytical security information. This procedure will result in a well-informed community of intrusion analysts. All SOC Analysts are primarily responsible for the execution of this procedure.

The Incident Analysis Procedures documents the step-by-step approach to analyzing the signature, context, appropriateness, and specifics of a given information security event displayed in the Azure Sentinel Incidents Blade. The procedure will result in the appropriate escalation of significant Incidents, Alerts, and Events, as well as the effective handling of less critical Incidents, Alerts, and Events. This procedure is primarily the responsibility for all SOC Analysts.

## Incident Triage Workflow & Narrative

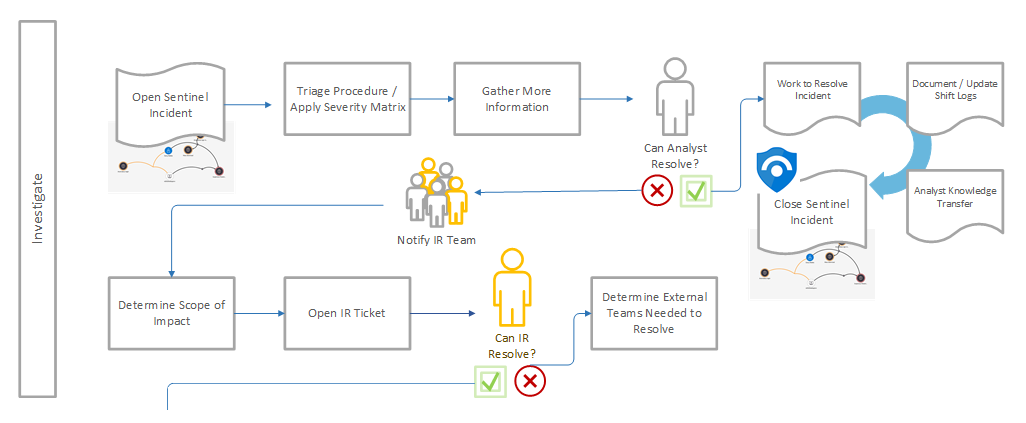
**Incident Annotation Stages**

The various steps that make up a collaborative workflow for annotations are called Stages. Individual Incidents can be assigned to the various stages by an analyst investigating Incidents. Stages are assigned to individual Incidents using tagged annotations. You can assign stages or tags to an Incident by clicking on an Incident and clicking the "+" under Tags to add your annotation/tag.

The SOC will report on Incidents and the resulting Azure Sentinel Incidents generated from the analysis they conduct. It is very important to tag/annotate Incidents properly in order to ensure that SOC activity reporting is correct.

These Incident annotation stages that can be used by the SOC Analyst within the Azure Sentinel Logs view are listed below with a description for each.

**Workflow Diagram:**

****

| **Incident Annotation Stages by Tags** | **DESCRIPTION** |
| --- | --- |
| Queued | Azure Sentinel Incidents by default are queued by Creation date and contain all Alerts/Events that come into Azure Sentinel. |
| Triage | The first custom stage of the SOC workflow, Triage will be used by all SOC Analysts to move Incidents/Alerts/Events of interest from the Queued stage to a separate queue for further investigation. This helps to provide a lower false positive rate. |
| Update Incident | This stage is used to update existing Azure Sentinel Incidents that have been previously Opened and Triaged by SOC Analysts. |
| Incident Previously Created | This stage is used to denote that we have a duplicate Incident/Alert which is already being worked. This allows analysts to identify Incidents/Alerts/Events which are not necessarily false positives, but do not need to have new Incidents created or do not need to be added to the existing Incident because the Alerts/Events are repeat Alerts/Events. |
| Under Investigation | This stage will be used by SOC Analysts to conduct additional analysis on Incidents/Alerts/Events that were moved out of the Triage Stage. |
| False Positive / No Further Action | This stage can be used at any point in the workflow to close an Incident with corresponding Alerts/Events that are either false positives or have completed their lifecycle. |

**Azure Sentinel Incident Stage Management**

All of the Incident stages should be reviewed periodically. The priority of the Incidents will dictate which needs to be addressed first, so the order listed in this narrative is just for functional purposes.

**Azure Sentinel Incident Triage Stages**

| **Incident Triage Stages by Tags** | **DESCRIPTION** |
| --- | --- |
| Open | If determination is made that an Incident is considered to be actionable, this stage will be used. This stage will be used for tracking of incidents throughout the Incident lifecycle. NOTE: SOC Incidents might want be tied into an external ticketing systems (i.e. Archer) when engaging other teams for escalation and/or remediation. For example, the Archer ticket should be entered into the SOC case so someone can tie the two together in an audit or review. |
| Open/Escalated - Awaiting Information | Incidents that have been escalated to an External Team by way of the Incident Response Team. This will allow another set of eyes on a particular Incident or group of Incidents to assist with the investigations process. |
| Closed - False Positive | This stage is to be used when an Incident has been deemed a false positive and no further action is required. |
| Closed - Remediated | Incidents that have been fully examined and the Analyst has provided remediation. |
| Closed - Insufficient Data | Incidents that were closed as a result of insufficient data to support the investigation. These Incidents need further review to understand what data is needed to further support the investigation of these Incidents. |
| Closed - No Risk | Incidents that have been identified where there was no risk to the Enterprise. (i.e. misconfigured device, authorized scanning) |
| Closed - Other | Incidents that have been closed that don’t match the previously identified closure codes (i.e. FP, Remediated, Insufficient data, etc). |

**Incident Triage Process (Primary Analyst)**

1. An Alert/Incident fires into the Incidents Blade within Azure Sentinel. If there is more than one SOC Primary Analyst triaging, they will select the Incidents they wish to investigate and then change the Incident annotation stage to **“Under Investigation”**. The Incident should then be assigned to the Analyst. The Primary Analyst has 5 - 15 minutes to examine the Incident and determines if the Incident is an ‘Incident of interest’. If the Incident is NOT of interest, then it has been determined to be a false positive. The Analyst shall change the Incident Annotation stage to **"False Positive/No Further Action"**. The Incident is then closed and updates the Daily Shift Log. If content can be created and/or modified to eliminate the false positive that information needs to be submitted to the SIEM engineers as a Content Change Request. If the Azure Sentinel content doesn’t need to be modified, a SOC Analyst will note the reason for the false positive (i.e. passwords expire, system misconfiguration, etc.) in the daily shift logs.
2. If an Incident has been deemed **“actionable”**, the Primary Analyst will conduct additional analysis and compile more information about the Incident. The Primary Analyst then checks to see if a new Azure Sentinel Incident or if an existing Incident needs to be updated. If a new Incident is needed, the Analyst gathers the necessary details, opens an Incident and adds all relevant event(s)/bookmark(s) to the Incident. The Analyst changes the Incident stage to **“Open”**. An Incident should only be opened if the analyst is fairly confident that the event(s) is not a false positive. The Primary Analyst notifies a Secondary Analyst (“off-channel”) via email or Teams or another method that there is an Incident opened and tags that Incident with **“Open”**.
3. If the event(s) triaged/hunted and bookmarked are part of an existing Azure Sentinel Incident, the Analyst updates the details of that Incident and adds all event(s)/bookmark(s) to the existing Incident. The Incident is then tagged with the **“Add to Incident”** stage. The Primary Analyst notifies a Secondary Analyst (“off-channel”) via email that there is an Incident opened and also tags that Incident **“Open”**.
4. Once an Incident is opened, it is the responsibility of the Incident owner/creator to manage the Incident to closure, unless it is escalated to the Secondary Analysts or the Incident Response Team.

**Secondary Analyst - Investigation Process**

1. The Secondary Analysts need to routinely filter within the Incidents blade of Azure Sentinel for the Incidents Tagged **"Open"** to identify any Incidents that need to be further investigated. Escalations from the Primary Analysts will be sent via Teams to the Secondary Analysts. The Analyst that would be responsible for “Incident ownership” will move the Incident Taggs from **“Open”** to **"Under Investigation"** and assign the Incident to themselves.
2. In the event that their investigation leads to a False Positive, the Analyst needs to document within the Incident the conclusion and change the Incident stage to **“Closed – False Positive”**. The Analyst then closes the Incident and transfers the knowledge of their findings to the Primary Analysts. The Secondary Analysts will also update the Shift log(s) with those findings. If content can be created and/or modified to eliminate the false positive that information needs to be submitted to the SIEM engineers as a Content change.
3. If the Incident has been determined to be valid and no escalation is required, the Analyst will conduct further analysis and continue resolving the Incident. Once the issue has been remediated the Analysis will update the Incident details and then change the Incident to **“Closed – Remediated”.**
4. The Analyst then documents within the Incident the conclusion and changes the Incident tagged stage to **“Closed – Remediated”** (with other appropriate closure notes). The Analyst then closes the Incident and transfers the knowledge of their findings to the Primary Analysts. The Secondary Analysts will also update the Shift log(s) with their findings.
5. If the incident requires escalation, the Analyst proceeds with moving the Incident to the **“Escalated to IR”** by tagging the Incident. A SOC Analyst notifies a member of the Incident Response Team via Teams or Email.

**Incident Response Team - Triage Process**

1. The Incident Response Team needs to routinely check the Incidents tagged with “Escalated to IR” within the Azure Sentinel Incidents Blade to identify any Incidents that need to be further investigated. Escalations from the Secondary Analysts will be sent via Teams or an email to the Incident Response Team.
2. In the event that their investigation leads to a False Positive, the Analyst needs to document within the Incident the conclusion and change the Tagged stage to **“Closed – False Positive”**. The Analyst then closes the Incident and transfers the knowledge of their findings to the Primary & Secondary Analysts and updates the Shift Log(s). If content can be created and/or modified to eliminate the false positive that information needs to be submitted to the SIEM engineers as a Content change.
3. If the Incident has been determined to be valid, the Incident Responder determines if External Teams are needed to assist with the investigation. If no other team is needed, then IR proceeds with following the predefined Incident Response plan. The IR Team member that is responsible for investigating the incident will declare **“Incident ownership”** and assign the Incident to themselves.
4. Once the issue has been remediated, the Analyst then documents within the Incident the conclusion and changes the Incident Tagged stage to **“Closed – Remediated”** (with other appropriate closure notes). The Analyst then closes the Incident and provides a knowledge transfer with their findings to the Primary & Secondary Analysts. The IR Team will also update the Shift log(s) with their findings.
5. If an Incident has been determined to be valid and there is an External Team needed to assist with the investigation, a member of the IR Team re-tags the Case to **“Open - Awaiting Information”**. The IR Team member that is responsible for the investigation will declare “Incident ownership” and assign the Incident to themselves.

The IR Team also identifies which external team the incident needs to be escalated to. After escalation has been established, the necessary team will continue to resolve the incident. Once the issue has been remediated, the Analyst then documents within the Incident the conclusion and re-tags the Incident with the tagged stage of **“Closed – Remediated”** (with other appropriate closure notes). The Analyst then Closes the Incident and provides a knowledge transfer with their findings with the Primary & Secondary Analysts. The IR Team will also update the Shift log(s) with their findings.

**Incident Closure Workflow**

1. Once an Incident is closed, review the details of the Incident, the indicators of compromise, the attack vector and the root cause.
2. With the information above, determine if an update is needed to the knowledgebase and update as needed.
3. Update the Final Incident, review details with informative knowledge and make sure the Incident has been tagged/annotated closed.
4. With the information above, determine if content needs to be updated or new content created.

## Incident Analysis Procedures

**Description**

The Incident Analysis procedure is the basic analytical process a SOC Analyst must use to determine if a series of Azure Sentinel Incidents are critical, warrant some level of callout, or are insignificant and warrant no action. A Primary Analyst will monitor the Azure Sentinel Incident Blade for Incidents tagged with "Triage". The Primary Analyst will monitor for a period of 2 or 4 hours according to the Monitoring Schedule.

* A Primary Analyst has 5 - 15 minutes from the time an Incident populates the Azure Sentinel Incidents Blade to triage and tag Incidents of interest with the "Triage" tag, in accordance with the SOC SLA. SLA tracking is monitored by SOC Leadership. A Secondary Analyst will monitor the Azure Sentinel Incidents tagged with "Triage". The Secondary Analyst will monitor for a period of 2 or 4 hours according to the Console Monitoring Schedule.
* The Secondary Analyst has an 8-hour SLA to resolve these Incidents. This is so the analyst has sufficient time to review and triage Incidents that merit more in-depth analysis.

It may be necessary to monitor the Incidents blade for additional tags based on new requirements such as virus outbreaks, new 0-days, etc. This notification will be provided to the Primary SOC Analysts by the SOC Leadership as necessary.

**Step 1: Group Events for Analysis**

The Primary Analyst will review all Incidents and tag and triage them as necessary for review or close them. If analysis on any of the Incidents is expected to take longer than 5 - 15 minutes, the Primary Analyst will escalate the Incident(s) with the "Triage" tag for review by the Secondary Analyst.

**Step 2: Understanding the Attack**

The Primary Analyst should gather and understand the full context of the cyber-event. Use a tool like notepad to record the following information (this will be transferred to the event annotation notes):

**Identify Source IP / Destination IP Addresses**

* Use Nslookup (Windows DNS), Search

**Identify Host/Asset Type**

* Workstation or Server
* Type - Enterprise, Production or Development

**Identify Accounts**

* If a service account? Who is the owner of the service account?
* What is the SID of the account that was locked?
* Which Domain does this account belong to?
* What permissions / privileges have been assigned to this account? Were permissions elevated

**Identify if the Host is Internal or External**

**What is the MAC Address? DHCP enabled?**

* If external, use the following tools:

1. Use Threat Analytics Search to make a quick assessment of the reputation
2. www.Centralops.net
3. www.Tcpiputils.com
4. Other (public) Threat intel sources

* Identify Source / Destination Hostname(s)
* Identify Target Hostname(s)
* Identify affected Source / Destination Port(s)
* Identify Operating System and affected services

**Identify the attack vector**

* Email, Instant Messaging, IRC, etc
* Malicious websites/browser redirects
* OS, Application, or Browser vulnerabilities (or feature/functionality)
* Host configuration; services, shares, accounts/passwords, etc

**Research the Context of the attack**

* Research the detected malware type(s)
* What does it do? How does it infect a host? Name of malware?
* Does is disable services? (i.e FW, AV/AS, HIPS)
* Does it drop files? if so where?
* What’s the propagation method?

1. Email delivery? (is the actual email in the logs?)
2. Web delivery (can you identify the domain?)

* Is there a System level or share-level infection?
* What’s the probability of other infections?
* What is the file path & name? This can indicate the infection vector (e.g. filename.msg may infer it was via email, C:\Users\jdoe\AppData\Local\Microsoft\Windows\Temporary Internet Files\ may infer it was via web browser.
* Are there mitigation steps required? Did AV successfully "clean" the infection?
* Detailed Indicators of Compromise (IoC's) associated with the security event(s)

**Identify if any <Customer's> devices are attempting communications with "malicious IP's"**

* Did the host call back to a known bad command and control site?
* Identify Network protection (Firewalls, IDS/IPS, Endpoint Threat Protection, Sink Hole, Proxy)
* Identify all known vulnerabilities (CVE, AV DAT version, recent exploits, etc.)
* All activity with similar Source or Destination address in last 5-30 days
* Detailed definitions of relevant signatures
* Any correlating information from external sources (immediately known Intel)
* Run a KQL to search for both the offending IP/domain and for the specific indicator to see if any other hosts are making similar connection attempts.

**Step 3: Analyze and Assess the Impact of the Attack**

The Analysts should investigate any Attack by using any/all internal and external tools and resources.

**Additionally, all Analysts should be prepared to answer the following:**

* Was the attempt successful?
* How many hosts are involved?
* Was the IP blocked by the FW or Proxy?
* Were any Customers impacted?

**What was the origin and/or details about the attacker IP?**

* WhoIs, Domain tools
* Spoofed IP (pcap analysis is required)
* Skill of attacker (automated scripts vs. obfuscation attempts)
* Country, ISP, Business (what is the net block)

**What was attacked?**

* DMZ
* Corporate systems
* Database(s)
* [CUSTOMER's] Application(s) - Web?

**What did they do (or try to do)?**

* Identify names of IDS signatures or alarms, as well as definitions of the various signatures.
* What broad categories do all the events fit in? (Web, OS, Application, SQL, etc...)

**When did they do it?**

* Identify all date-time-groups (DTG), attack timeline (fast/slow), time of day in source IP time zone.
* Identify a series of subtle events or rash of attacks (fast/slow)
* Same time of day vs. various times

**Where did they attack from?**

* Identify the IP address of attacked system(s), external/internal/DMZ, applications, open ports, vulnerabilities, and usernames (if any).

**Why did they do it?**

* Identify the purpose of the attack. Targeted or random?
* Web Defacement
* Admin access
* Reconnaissance
* Dos/DDoS or other outage

**How did they go about it?**

* Identify the tool used (vulnerability scanner, port scanner), hand crafted, type of attack (buffer overflow, SQL injection, format string), protocol used, flags set, or other details.

**Step 4: Determine What Action is Needed**

Depending on the severity of the Incident, an analyst may need to report the Incident in several manners. The outcome of the analysis should prompt the analyst to perform one or more of the following actions. Once one of the below actions are taken, the Incident(s) should be tagged using the appropriate tags as detailed in the Incident Triage Workflow Procedures.

**Close Incidents**

* If the Incident(s) are either false positives or do not warrant further attention, the Incident(s) should be closed.
* This may be the case when traffic is blocked by a proxy device or firewall or if the traffic is normal traffic that is triggering false positives.
* If an Incident is concluded to be a false positive, a filter request should be completed in the Shift Logs section.

**Report Incidents in Shift Logs**

* If the Incidents should be noted for future analysis or operational meetings, the Incident should be reported in the Shift Logs section.
* A shift log entry should be created using the Shift Log Management Procedures.

**Escalating Incidents**

* If the Incidents should be escalated for further analysis by other teams or internal SOC analysts, the Incidents should be escalated per the Incident Triage Procedures.

**Creating Incidents**

* The SOC Analyst has determined that an Alert or series of Alerts/Events appear to be related and warrant further investigation.
* Refer to these procedures in order to open an Incident.

## Information Fusion Procedures

**Description**

The Information Fusion Procedure is important in that it assures that all SOC Analysts are properly informed of the latest global security threats.

**SOC Analyst Procedures**

All SOC Analysts should perform the following tasks:

* Read current Intelligence Reports.
* The Daily Intelligence Report will cover the latest threats, external news and operational news.
* Query Azure Sentinel for internal events that may correlate with news provided by Intelligence Reports.
* Review all news and messages sent via email.
* Relay all news of significant events and messages provided by other [Customer]'s Teams via email and update the shift log report.

**Sr. SOC Analyst Procedures**

All Senior SOC Analysts will create the Daily Intelligence Report, Weekly Intelligence Reports and other reports as defined in the Roles and Responsibilities. These reports will provide necessary information to all analysts within the SOC. Senior SOC Analysts own the following reports and processes:

| **Report** | **Description** |
| --- | --- |
| Daily Intelligence Report | The Daily Intelligence Report is produced to inform Analysts of Threats, External News and Operational News. |
| Weekly Threat Report | The Weekly Threat Report is produced to inform analysts of key issues and other significant metrics for each week. |

## Focused Monitoring Procedures

**Description**

Once an Incident has been created, the Focused Monitoring procedure is initiated. This procedure is designed to ensure that the SOC is closely monitoring a previously recognized situation for further expansion of its scope or character.

* Ensure all Source IPs are added to an Azure Sentinel Livestream for continued monitoring. (Example below)
* Ensure all Destination IPs are added to an Azure Sentinel Livestream for continued monitoring.
* Gather all relevant historical information from any Entities listed from within the Incident and add history to the Incident comments.
* Any Incident-relevant events/alerts triggered by the same source should be noted in the Incident comments.
* Any events/alerts originating from internal Source IPs, which were previously Destination IPs in the original attack, should be added to the Incident comments.

Focused Monitoring is leveraged during an incident and/or monitoring of a series of alerts or events for business impact analysis; network, operations, service levels, productivity and to monitor for further propagation or to monitor to determine if the incident/issue is increasing or decreasing in scope.

**Procedure**

* Create an Azure Sentinel Livestream based upon varying details or perspectives;

1. Example using Entity type Source/Destination IPs:

1.1 Ensure all Source IPs are added to an Azure Sentinel Livestream for continued monitoring.

1.2 Ensure all Destination IPs are added to an Azure Sentinel Livestream for continued monitoring.

1.3 Ensure that the Incident gets updated and that the appropriate team members are appraised

1. Gather all relevant historical information from any Entities listed from within the Incident and add history to the Incident comments.
2. Any Incident-relevant events/alerts triggered by the same source should be noted in the Incident comments.
3. Additional, you must update the applicable Incident documentation sections; i.e. Follow-up, Analyst Comments, etc
4. Any events/alerts originating from internal Source IPs, which were previously Destination IPs in the original attack, should be added to the Incident comments.

* Update the SOC Shift Logs.

**An Example**

Below is an example for creating an Azure Sentinel Livestream.

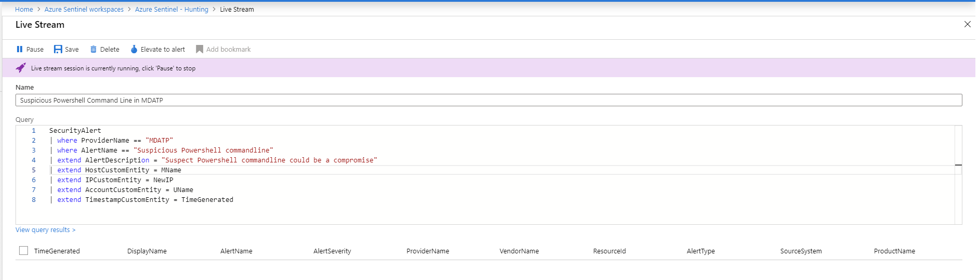
**To create a livestream session from scratch:**

1. Select the Livestream tab
2. Click + New livestream.
3. On the Livestream pane:

* If you started livestream from a query, review the query and make any changes you want to make.
* If you started livestream from scratch, create your query.

1. Select Play from the command bar.

* The status bar under the command bar indicates whether your livestream session is running or paused. In the following example, the session is running:

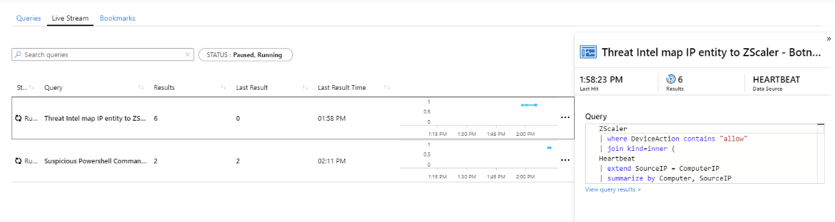


Select Save from the command bar.

* Unless you select Pause, the session continues to run until you are signed out from the Azure portal.

**To View your livestream sessions:**

1. In the Azure portal, navigate to Sentinel > Threat management > Hunting > Livestream tab.
2. Select the livestream session you want to view or edit. For example:



Your selected livestream session opens for you to play, pause, edit, and so on.

**To receive notifications when new events occur:**

1. Because livestream notifications for new events use Azure portal notifications, you see these notifications whenever you use the Azure portal. For example:



## SOC Use Cases

**Description**

The [CUSTOMER] Security Operations Center (SOC) is leveraging the SANS: Critical Controls for Effective Cyber Defense Framework & MITRE ATT&CK Framework to provide both a roadmap for future capabilities as well as establishing a reporting standard to drive security awareness and risk management. The Use Case library below contains the SANS CC aligned to the specific SOC Use Cases outlined within each respective MITRE ATT&CK Tactic.

While partial or not all of the Critical Controls are within scope, the Security Operations Center in coordination with cross functional organizations and resources will continue to on-board additional devices/technologies, recommend additional security controls and/or capabilities of new or existing technologies to improve and mature the security posture, and continuously develop and refine use cases for both detection and reporting purposes.

Utilize the Use Case Documentation Template to properly document all use cases.

**AZURE SENTINEL FUSION USE-CASES**

These scenarios combine two of the fundamental logs used by security analysts:

* Firewall logs from Palo Alto Networks and end-point detection logs from Microsoft Defender ATP. In all of the scenarios listed below, a suspicious activity is detected in the end point that involves an external IP address, then, this is followed by anomalous traffic from the external IP address back into the firewall. In Palo Alto logs, Azure Sentinel focuses on threat logs, and traffic is considered suspicious when threats are allowed (suspicious data, files, floods, packets, scans, spyware, URLs, viruses, vulnerabilities, wildfire-viruses, wildfires).

1. Network request to TOR anonymization service followed by anomalous traffic flagged by Palo Alto Networks firewall. <https://docs.microsoft.com/azure/sentinel/fusion#network-request-to-tor-anonymization-service-followed-by-anomalous-traffic-flagged-by-palo-alto-networks-firewall>
2. PowerShell made a suspicious network connection followed by anomalous traffic flagged by Palo Alto Networks firewall. <https://docs.microsoft.com/azure/sentinel/fusion#powershell-made-a-suspicious-network-connection-followed-by-anomalous-traffic-flagged-by-palo-alto-networks-firewall>
3. Outbound connection to IP with a history of unauthorized access attempts followed by anomalous traffic flagged by Palo Alto Networks firewall. <https://docs.microsoft.com/azure/sentinel/fusion#outbound-connection-to-ip-with-a-history-of-unauthorized-access-attempts-followed-by-anomalous-traffic-flagged-by-palo-alto-networks-firewall>

* Using advanced multistage attack detection, Azure Sentinel supports the following scenarios that combine anomaly events from Azure Active Directory Identity Protection and Microsoft Cloud App Security:

1. Impossible travel to a typical location followed by anomalous Office 365 activity. <https://docs.microsoft.com/azure/sentinel/fusion#impossible-travel-to-atypical-location-followed-by-anomalous-office-365-activity>
2. Sign-in activity for unfamiliar locations followed by anomalous Office 365 activity. <https://docs.microsoft.com/azure/sentinel/fusion#sign-in-activity-for-unfamiliar-location-followed-by-anomalous-office-365-activity>
3. Sign-in activity from infected devices followed by anomalous Office 365 activity. <https://docs.microsoft.com/azure/sentinel/fusion#sign-in-activity-from-infected-device-followed-by-anomalous-office-365-activity>
4. Sign-in activity from anonymous IP address followed by anomalous Office 365 activity. <https://docs.microsoft.com/azure/sentinel/fusion#sign-in-activity-from-anonymous-ip-address-followed-by-anomalous-office-365-activity>
5. Sign-in activity from users with leaked credentials followed by anomalous Office 365 activity. <https://docs.microsoft.com/azure/sentinel/fusion#sign-in-activity-from-user-with-leaked-credentials-followed-by-anomalous-office-365-activity>

**On-Board Anlytics Key**

| **Status** | **Use case is…** |
| --- | --- |
| **Hold** | On hold. For example the event data source is not in Azure Sentinel, an end system configuration or policy change is required or the use case is causing too many false positives and cannot be tuned sufficiently at this time. |
| **Dev** | In development by a content author. No Incident stage annotation or annotated as 'Development'. No SOC action. |
| **Test** | Being soak tested. Alerts/Events annotated/tagged for "Testing". Allows confirmation that Analytic use case is not overly noisy, Use Case and IR procedure are to be updated within the SocRA Watchlist. Ops Lead / Senior Analyst can review Alerts/Events. |
| **Approved** | Currently in test but approved for production and awaiting the move to be Incident Enabled. |
| **Prod** | In production. Alerts/Events added to Incident and annotated/tagged for "Triage". Subject to metrics. SOC Analysts are to respond to Incidents. |

**AZURE SENTINEL Analytics/Detection(s) On-board Tracking Table**

This is the Use-case/Detection Matrix that lists out all of our Out-Of-The-Box detections, mapping them back to Corresponding Data Sources as well as to MITRE ATT&CK Tactics:

| NAME | RULE TYPE | DATA SOURCES | MITRE TACTICS |
| --- | --- | --- | --- |
| Advanced Multistage Attack Detection | Fusion | Persistence, Lateral Movement, Exfiltration, Command and Control |  |
| Create incidents based on Microsoft Defender Advanced Threat Protection alerts | Microsoft Security | Microsoft Defender Advanced Threat Protection​ (Preview) |  |
| Create incidents based on Microsoft Cloud App Security alerts | Microsoft Security | Microsoft Defender Advanced Threat Protection​ (Preview) |  |
| Create incidents based on Azure Security Center for IoT alerts | Microsoft Security | Azure Security Center for IoT |  |
| Create incidents based on Azure Security Center alerts | Microsoft Security | Azure Security Center |  |
| Create incidents based on Azure Advanced Threat Protection alerts | Microsoft Security | Azure Advanced Threat Protection |  |
| Create incidents based on Azure Active Directory Identity Protection alerts | Microsoft Security | Azure Active Directory Identity Protection |  |
| (Preview) Anomalous SSH Login Detection | ML Behavior Analytics | Syslog | Initial Access |
| User account created and deleted within 10 mins | Scheduled | Security Events | Persistence, Privilege Escalation |
| User account added to built-in domain local or global group | Scheduled | Security Events | Persistence, Privilege Escalation |
| Time series anomaly for data size transferred to public internet | Scheduled | Cisco ASA +2 | Exfiltration |
| Time series anomaly detection for total volume of traffic | Scheduled | Barracuda Web Application Firewall +6 | Exfiltration |
| THALLIUM domains included in DCU takedown | Scheduled | DNS (Preview) +3 | Command and Control, Credential Access |
| Suspicious Resource deployment | Scheduled | Azure Activity | Impact |
| Suspicious number of resource creation or deployment activities | Scheduled | Azure Activity | Impact |
| Suspicious granting of permissions to an account | Scheduled | Azure Activity | Persistence, Privilege Escalation |
| Successful login from IP and failure from a different IP | Scheduled | Azure Active Directory | Credential Access, Initial Access |
| SSH Potential Brute Force | Scheduled | Syslog | Credential Access |
| SSH newly internet-exposed endpoints | Scheduled | Syslog | Initial Access |
| Squid proxy events related to mining pools | Scheduled | Syslog | Execution, Impact |
| Squid proxy events for ToR proxies | Scheduled | Syslog | Command and Control |
| Sign-ins from IPs that attempt sign-ins to disabled accounts | Scheduled | Azure Active Directory | Initial Access, Persistence |
| SharePointFileOperation via previously unseen IPs | Scheduled | Office 365 | Exfiltration |
| SharePointFileOperation via devices with previously unseen user agents | Scheduled | Office 365 | Exfiltration |
| Sensitive Azure Key Vault operations | Scheduled | Microsoft web application firewall (WAF) | Impact |
| Security Event log cleared | Scheduled | Security Events | Defense Evasion |
| RDP Nesting | Scheduled | Security Events | Lateral Movement |
| Rare subscription-level operations in Azure | Scheduled | Azure Activity | Credential Access, Persistence |
| Rare RDP Connections | Scheduled | Security Events | Lateral Movement |
| Rare high reverse DNS count | Scheduled | DNS | Discovery |
| Rare high NXDomain count | Scheduled | DNS | Command and Control |
| Rare application consent | Scheduled | Azure Active Directory | Persistence, Lateral Movement, Collection |
| Rare and potentially high-risk Office operations | Scheduled | Office 365 | Persistence, Collection |
| Process execution frequency anomaly | Scheduled | Security Events | Execution |
| Process executed from binary hidden in Base64 encoded file | Scheduled | Security Events | Execution, Defense Evasion |
| Powershell Empire cmdlets seen in command line | Scheduled | Security Events | Execution, Persistence |
| Potential Kerberoasting | Scheduled | Security Events | Credential Access |
| Palo Alto - potential beaconing detected | Scheduled | Palo Alto Networks | Command and Control |
| Palo Alto - possible internal to external port scanning | Scheduled | Palo Alto Networks | Discovery |
| Office policy tampering | Scheduled | Office 365 | Persistence, Defense Evasion |

**Process Owner**

SOC Manager

## Host Analysis Process

**Summary**

Host Analysis is a vital and cautious part of the Security Operations Center response processes. This process extends into the research and analysis for malicious code, social engineering and/or unauthorized system modification down to the endpoint. Particular caution must be taken in this process as not to violate privacy laws either domestic or international. Additionally, the analyst's objective is to not render forensic evidence inadmissible in the event of legal litigation.

The intent of this document is to provide consistent, repeatable, and objective guidance in performing host investigation to include information gathering, anomaly analysis, triage and escalation for a potentially compromised Business Unit asset.

**Scope**

The process and procedures defined in this document must be conducted on the [Customer] and it's subsidiaries assets;

* To confirm validity and severity of a detection via Azure Sentinel with Defender for Endpoints (via use cases or raw analysis).
* To confirm validity and severity of symptoms and behavior reported by an [Customer] team member.
* To confirm the validity of abuse complaints.
* Determine the points of entry and type of compromise. Identification of areas for further investigation and issues for attention.

**Inappropriate Content**

If suspicious or malicious Content is discovered during the course of the host investigation, the analyst is to immediately disengage from the host investigation and follow the escalation procedure for engaging the SOC Manager and/or IR Team. HR. The escalation to SOC Manager must also include the Incident information relative to the investigation for potential system compromise; logic which triggered alert, Incident notes, steps taken thus far, directories accessed, tools used, and a summary of the current state of the system.

* Do not take screenshots of said content
* Do not modify the file/folder of said content
* Do not copy, modify or delete the files and/or folders in which said content is located.
* Do not engage a [Customer] Team Member nor their respective manager

**International Privacy Concerns**

Please be aware of differing international requirements and restrictions which are potentially applicable in regards to responding and investigating a host for potential compromise. For the purpose of this section we will focus on the following countries related to EU privacy law; France, Germany, & Sweden. Other countries may be applicable; however, as a rule of thumb, when in doubt refer to the SOC Manager and respectively your legal representatives.

* Do not access folder(s) that are labeled as private; or confidential located in the team member's user profile.
* Do not access folders that contain user's personal information.
* If there is definitive cause and justification to access the restricted folder; you must escalate to the Office of Legal Compliance.

1. For example, malicious code may reside in the users\appdata\local\temp or rogue COM files may have been placed into Temporary Internet Settings.

**Malicious Content**

Malicious content must always be stored in password protected, encrypted ZIP files. The password applied to the Zip container must be determined by your SOC Manager.

**Pre-Requisites**

* Investigate entities on devices using Defender for Endpoints "live response"
* Before you can initiate a session on a device, make sure you fulfill the following requirements:

1. Verify that you're running a supported version of Windows.
2. Devices must be running one of the following versions of Windows

Windows 10

1.1 Version 1909 or later

1.2 Version 1903 with <https://support.microsoft.com/help/4515384/windows-10-update-kb4515384>

1.3 Version 1809 (RS 5) with <https://support.microsoft.com/help/4537818/windows-10-update-kb4537818>

1.4 Version 1803 (RS 4) with <https://support.microsoft.com/help/4537795/windows-10-update-kb4537795>

1.5 Version 1709 (RS 3) with <https://support.microsoft.com/help/4537816/windows-10-update-kb4537816>

Windows Server 2019 - Only applicable for Public Preview

2.1 Version 1903 or with <https://support.microsoft.com/help/4515384/windows-10-update-kb4515384> or later

2.2 Version 1809 with <https://support.microsoft.com/help/4537818/windows-10-update-kb4537818>

1. Enable Live Response from the Advanced Setting Page.

You will need to enable the Live Response capability in the (Advanced Features Settings) <https://docs.microsoft.com/microsoft-365/security/defender-endpoint/advanced-features?view=o365-worldwide> page.

NOTE: Only users with Manage Security or Global Admin roles can edit these settings.

1. Ensure that the device has an Automation Remediation level assigned to it.

You'll need to enable, at least, the minimum Remediation Level for a given Device Group. Otherwise you won't be able to establish a Live Response session to a member of that group.

1. Ensure that you have the appropriate permissions.

Only users who have been provisioned with the appropriate permissions can initiate a session. For more information on role assignments, see (Create and manage roles) <https://docs.microsoft.com/microsoft-365/security/defender-endpoint/user-roles?view=o365-worldwide>.

Depending on the role that's been granted to you, you can run basic or advanced live response commands. Users' permissions are controlled by RBAC custom roles.

**Initiate a Live Response Session on a Device**

1. Sign in to Microsoft Defender Security Center.
2. Navigate to the devices list page and select a device to investigate. The devices page opens.
3. Launch the live response session by selecting Initiate live response session. A command console is displayed. Wait while the session connects to the device.
4. Use the built-in commands to do investigative work. For more information, see Live Response Commands listed below.
5. After completing your investigation, select Disconnect session, then select Confirm.

NOTE: (Basic Live Response Commands) <https://docs.microsoft.com/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide#live-response-commands>

NOTE: (Advanced Live Response Commands) <https://docs.microsoft.com/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide#advanced-commands>

**Download a file in the Background**

To enable your security operations team to continue investigating an impacted device, files can now be downloaded in the background.

* To download a file in the background, in the live response command console, type download
* If you are waiting for a file to be downloaded, you can move it to the background by using Ctrl + Z.
* To bring a file download to the foreground, in the live response command console, type fg

Here are some examples:

DOWNLOAD A FILE IN THE BACKGROUND

| **Command** | **What it Does** |
| --- | --- |
| Download "C:\windows\some\_file.exe" & | Starts downloading a file named some\_file.exe in the background. |
| fg 1234 | Returns a download with command ID 1234 to the foreground. |

**Put a file in the library**

Live response has a library where you can put files into. The library stores files (such as scripts) that can be run in a live response session at the tenant level. Live response allows PowerShell scripts to run, however you must first put the files into the library before you can run them. You can have a collection of PowerShell scripts that can run on devices that you initiate live response sessions with.

**To upload a file in the library**

1. Click the Upload file to the library.
2. Click Browse and select the file.
3. Provide a brief description.
4. Specify if you'd like to overwrite a file with the same name.
5. If you'd like to be, know what parameters are needed for the script, select the script parameters check box. In the text field, enter an example and a description.
6. Click Confirm.
7. (Optional) To verify that the file was uploaded to the library, run the library command.

**Additional Commands & Running Scripts see the URL**

<https://docs.microsoft.com/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide>

**Roles & Responsibilities**

* **SOC Analysts**: to conduct host investigation within the parameters of the defined procedure, providing a detailed account of their investigation and findings.
* **SOC Manager**: is responsible for the successful execution of process and procedures of his/her respective team members.

## Subtle Event Process

**Purpose**

The purpose of this process is to describe the procedures SOC Analysts will use to detect subtle events.

**Scope**

Subtle events are those security events that are difficult to detect during operational monitoring due to extended time or other tactics used to disguise attacks. This process applies to all Incidents/Alerts/Events that are presented within the Azure Sentinel Incidents Blade.

**Process Summary**

All SOC Analysts are responsible for detecting significant intrusions and attempts that are missed in standard operational monitoring. A subtle event is an attack that is intentionally crafted to be difficult to detect. These include; unknown signatures, low & slow, IDS evasion, and other attack patterns that are difficult to detect in operational time (5-15 minutes). Operational time is the time frame from the first appearance of an Incident/Alert/Event in the Azure Sentinel Incidents Blade until the SOC Analyst clears it, either by tagging it for review or by closing it out. Highly skilled attackers will often conduct attacks that happen over much larger time windows than any individual Incident/Alert/Event will remain through monitoring, thus once operational time is exhausted there exists a set of analytical disciplines that are meant to discover these attacks by looking at larger sets of data. The primary purpose of this process is to discover highly skilled attackers and to recognize patterns of attack that are not widely recognized.

All SOC Analysts are responsible for conducting weekly analysis using Azure Sentinel's Hunting Blade.

The Data Exploration procedure defines the analytical methodologies for SOC Analysts to look at larger security datasets and to conduct exploratory data analysis. This procedure will leverage the Hunting Blade and Hunting KQL Queries provided within Azure Sentinel. This procedure documents the mechanics of interacting with large datasets but cannot fully capture the complete analysis process as that is guided by the ingenuity of the individual analyst.

**Roles & Responsibilities**

* SOC Manager owns the successful completion of all daily operational processes and procedures. The SOC manager is also responsible for ensuring these daily operational processes effectively support SOC operations and for continuous process improvement.
* SOC Analysts executes daily operations procedures as a matter of daily responsibility and owns the successful completion of all procedures executed during his/her presence in the SOC. SOC Analysts own the documentation and measurement of all subordinate procedures as well as the continual improvements to them. The role of a SOC Analyst is the detailed and repeatable execution of all operational tasks as documented in this process and its subordinate procedures.

**Additional Processes**

* Subordinate Procedures

1. Data Exploration

* Related Process & Procedures

1. Reporting Process
2. Intrusion Analysis Process

**Process Owner's Names**

SOC Manager

## Data Exploration Procedures

**Description**

This topic describes the procedures for using Azure Sentinel's Hunting Blade to review security events for abnormalities. Data Exploration is concerned with the identification of IOCs that were previously unknown or hidden within data sets. These IOCs can then be addressed or operationalized for situational awareness. If you're an investigator who wants to be proactive about looking for security threats, Azure Sentinel has powerful hunting search and query tools to hunt for security threats across your organization's data sources. But your systems and security appliances generate mountains of data that can be difficult to parse and filter into meaningful events. To help security analysts look proactively for new anomalies that weren't detected by your security apps, Azure Sentinel' built-in hunting queries guide you into asking the right questions to find issues in the data you already have on your network.

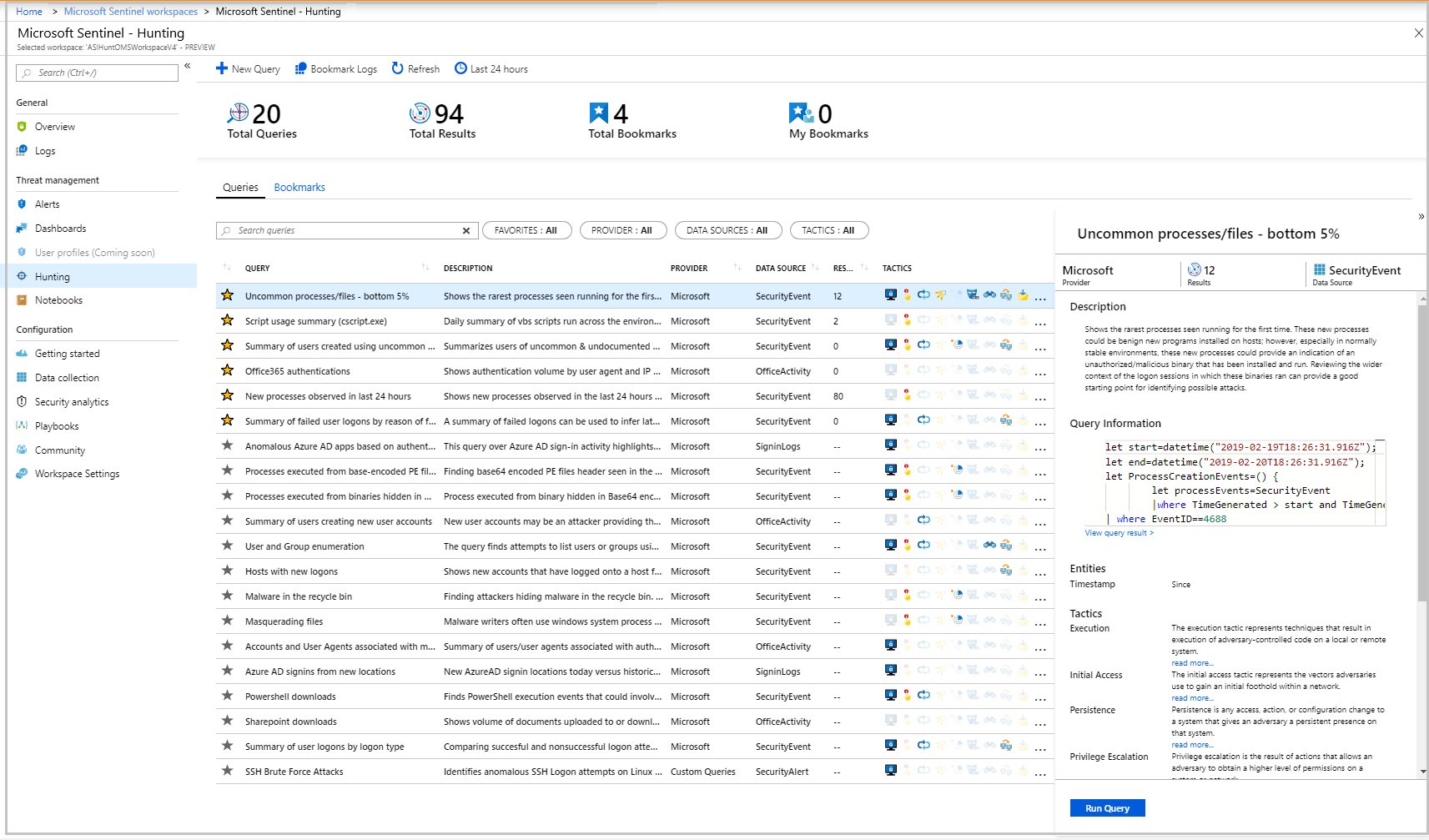
**Hunt for threats**

With Azure Sentinel hunting, you can take advantage of the following capabilities:

* Built-in queries: To get you started, a starting page provides preloaded query examples designed to get you started and get you familiar with the tables and the query language. These built-in hunting queries are developed by Microsoft security researchers on a continuous basis, adding new queries, and fine-tuning existing queries to provide you with an entry point to look for new detections and figure out where to start hunting for the beginnings of new attacks.
* Powerful query language with IntelliSense: Built on top of a query language that gives you the flexibility you need to take hunting to the next level.
* Create your own bookmarks: During the hunting process, you may come across matches or findings, dashboards, or activities that look unusual or suspicious. In order to mark those items so you can come back to them in the future, use the bookmark functionality. Bookmarks let you save items for later, to be used to create an incident for investigation. For more information about bookmarks, see Use bookmarks in hunting.
* Use notebooks to automate investigation: Notebooks are like step-by-step playbooks that you can build to walk through the steps of an investigation and hunt. Notebooks encapsulate all the hunting steps in a reusable playbook that can be shared with others in your organization.
* Query the stored data: The data is accessible in tables for you to query. For example, you can query process creation, DNS events, and many other event types.
* Links to community: Leverage the power of the greater community to find additional queries and data sources.

**Start Hunting**

1. In the Azure Sentinel portal, click Hunting.



1. When you open the Hunting page, all the hunting queries are displayed in a single table. The table lists all the queries written by Microsoft's team of security analysts as well as any additional query you created or modified. Each query provides a description of what it hunts for, and what kind of data it runs on. These templates are grouped by their various tactics - the icons on the right categorize the type of threat, such as initial access, persistence, and exfiltration. You can filter these hunting query templates using any of the fields. You can save any query to your favorites. By saving a query to your favorites, the query automatically runs each time the Hunting page is accessed. You can create your own hunting query or clone and customize an existing hunting query template.
2. Click Run query in the hunting query details page to run any query without leaving the hunting page. The number of matches is displayed within the table. Review the list of hunting queries and their matches. Check out which stage in the kill chain the match is associated with.
3. Perform a quick review of the underlying query in the query details pane or click View query result to open the query in Log Analytics. At the bottom, review the matches for the query.
4. Click on the row and select Add bookmark to add the rows to be investigated - you can do this for anything that looks suspicious.
5. Then, go back to the main Hunting page and click the Bookmarks tab to see all the suspicious activities.
6. Select a bookmark and then click Investigate to open the investigation experience. You can filter the bookmarks. For example, if you're investigating a campaign, you can create a tag for the campaign and then filter all the bookmarks based on the campaign.
7. After you discover which hunting query provides high value insights into possible attacks, you can also create custom detection rules based on your query and surface those insights as alerts to your security incident responders.

**Additional Context can be found here**

<https://docs.microsoft.com/azure/sentinel/hunting>

**Process Owner's Names**

SOC Manager

# SOC Business Process & Procedures

| **Processes Name** | **Procedures** | **References** |
| --- | --- | --- |
| Business Measurement Process (Metrics) |  |  |
|  | SOC Efficiency Metrics | Primarily intended to monitor SOC key performance indicators. Used to manage the efficiency and effectiveness of the Incident/Alert Triage Processes |
|  | SOC Analytics Metrics | Primarily intended to monitor tactical SOC activity. Daily view into events to identify any suspicious activity, active threats, or system health issues |
| Process Improvement |  |  |
|  | Process Maturity | Processes detailing the steps involved in improving the maturity of the SOC |
|  | Agile Methodology | Procedures for improving Agile Methodologies |
|  | Documentation Standards | Outlining the standards for documentation |
| Compliance Process |  |  |
|  | Compliance Support | Procedures that provide methods for the SOC in order to adhere to IT security policies & Requirements for the compliance teams to attain the required audit/logging and event notification controls |
| Business Continuity Process |  |  |
|  | Business Continuity & Disaster Recovery Plans | Official documentation for business continuity and disaster recovery |

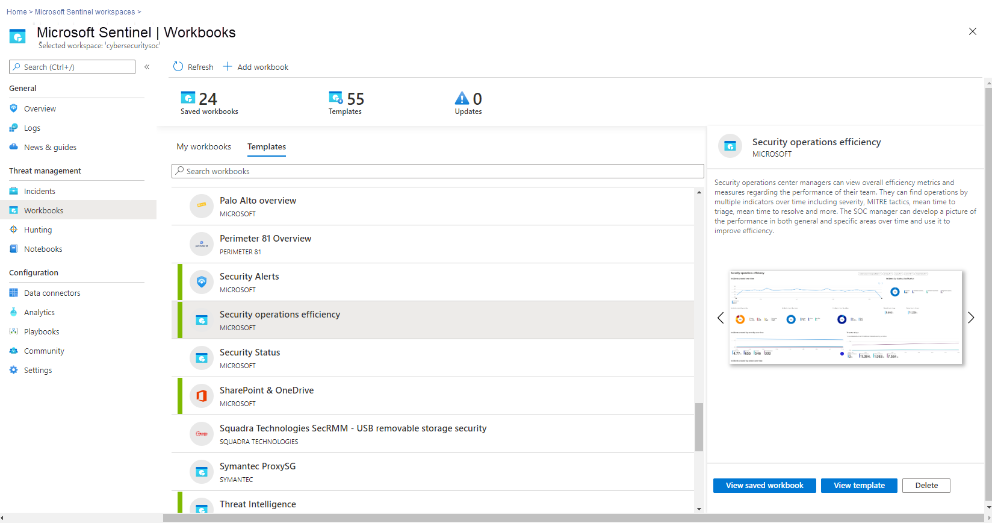
## SOC Efficiency Metrics

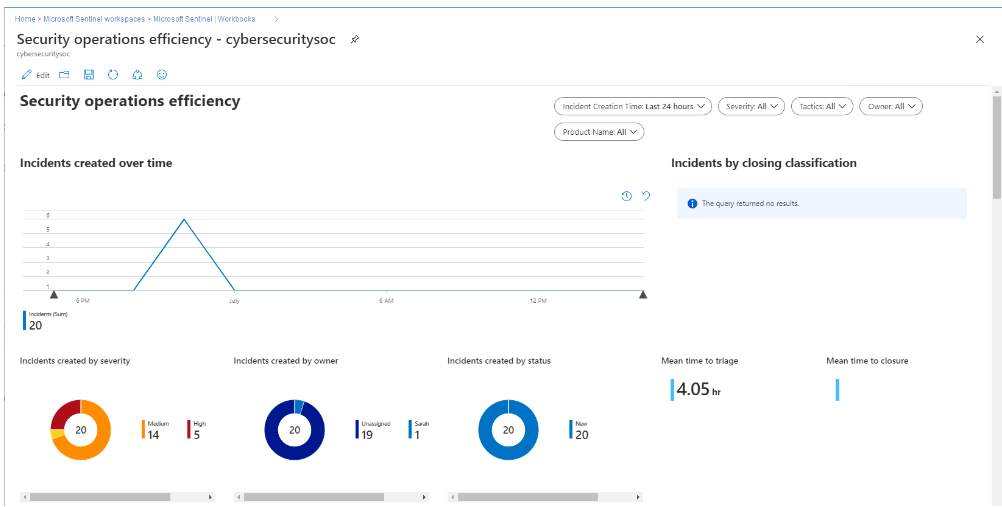
**Security operations efficiency workbook**

To complement the SecurityIncidents table, we’ve provided you with an out-of-the-box security operations efficiency workbook template that you can use to monitor your SOC operations. The workbook contains the following metrics:

* Incident created over time
* Incidents created by closing classification, severity, owner, and status
* Mean time to triage
* Mean time to closure
* Incidents created by severity, owner, status, product, and tactics over time
* Time to triage percentiles
* Time to closure percentiles
* Mean time to triage per owner
* Recent activities
* Recent closing classifications

You can find this new workbook template by choosing Workbooks from the Azure Sentinel navigation menu and selecting the Templates tab. Choose Security operations efficiency from the gallery and click one of the View saved workbook and View template buttons.





Every time you create or update an incident, a new log entry will be added to the table. This allows you to track the changes made to incidents, and allows for even more powerful SOC metrics, but you need to be mindful of this when constructing queries for this table as you may need to remove duplicate entries for an incident (dependent on the exact query you are running).

## SOC Analytics Efficiency Metrics

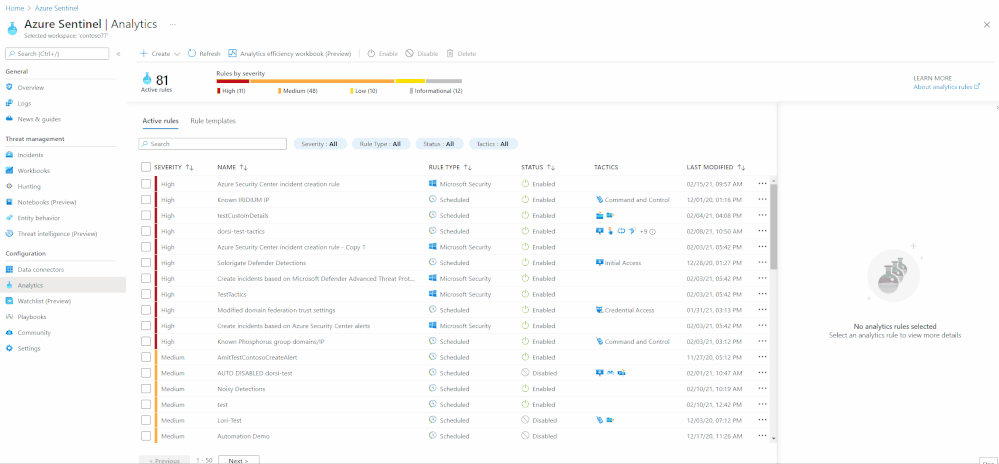
Description

The modern SOC handles multiple data sources and needs to detect threats and provide insights to the analyst. Since SOC resources are limited, a delicate balance must be struck between maximizing the detection of threats and minimizing the occurrence of false positives.

In the Analytics Efficiency Workbook, we try to provide different perspectives on detections.

* Alert rules - a holistic view of our detections provides us with insights into the detections' overall coverage. In this section, we can see our MITRE ATT&CK framework coverage, overall rules status, rules that require attention, and a view of the detection suite.
* Alerts - in this view, we will look at the alerts created from our detections. Since not all rules will create incidents, we can monitor the noisiness of the detections and see which ones require tuning. In the alerts insights section, we provide insights into detections that are not firing and might require attention and track the load from different providers.
* Incidents - The load on the SOC is determined by the number of incidents we create. Here we can monitor which detections created incidents and the reasons incidents are closed. When looking at the incident load and the closing reason, we can deduce which detections require attention and tuning.

Iterating on all 3 views in a repetitive process will improve our detection efficiency, SOC performance, and, ideally, the organization’s detection suite. This continuous process should adapt our detections to the ever-changing security threat landscape.



There are two ways to access this workbook –

1. The workbooks gallery - You can find this new workbook template by choosing Workbooks from the Azure Sentinel navigation menu and selecting the Templates tab. Choose Detection efficiency from the gallery and click one of the View saved workbook and View template buttons.
2. The Analytics pane - You can find the new workbook in the Alert rules action panel at the top of the pane. If a saved workbook were created from the workbook template, the button would lead to the saved workbook. If not, it will lead to the workbook template. More details can be found in the documentation.

## Process Improvement

**Purpose**

The purpose of this document is to provide the framework for the [CUSTOMER] Security Operations Center (SOC) Process Improvement program. This process will include a list of procedures associated with the continuous process improvement program; these will leverage the Carnegie Mellon Software Engineering Institute Capability Maturity Model for Integration (CMMI). The business goal is to enable the on-going assessment of SOC operations and provide feedback to improve service capability over time.

**Scope**

This process applies to all processes and procedures implemented in the [CUSTOMER] SOC. This process supports the assessment of the current state, suggests improvement areas and specific actions to improve service capabilities. The scope of this process is strictly limited to the [CUSTOMER] SOC.

**Process Summary**

The SOC Manager and the SOC Operations Lead evaluate the maturity and effectiveness of SOC process and procedure on a biannual basis. They use this information to improve SOC service delivery effectiveness. A continuous improvement process will enable the SOC's service delivery to be consistent, predictable, and on a path of continuous improvement. This is important in the field of security operations to guarantee a standardized, repeatable and high quality-of-service in recognizing and responding to critical information security events.

The Process Maturity Procedures will document the detailed steps for continuous process improvements. Given the rapid rate of change in the field of information security, this process will also be supported by an Agile Methodology Procedures to ensure that the SOC can effectively respond to new and emerging information security attacks with iterative and rapidly evolving process and procedures. The Agility procedure will also allow the SOC to become operationally effective much faster than traditional waterfall development methodologies. The Documentation Procedures will establish the methodology for drafting and maintaining appropriate documentation to support maturity and agility objectives.

* Perform initial assessment
* Score assessment, report maturity level and findings
* Identify service maturity goals
* Create action plans to achieve goals
* Execute service improvements

The [CUSTOMER] SOC will measure process maturity by using the Carnegie Mellon Software Engineering Institute's Capability Maturity Model for Integration. The CMMI is defined to contain the following levels:

| **CMMI LEVEL** |  |
| --- | --- |
| Level 1 | Ad hoc (Chaotic) |
| Level 2 | Repeatable |
| Level 3 | Defined |
| Level 4 | Managed |
| Level 5 | Optimized |

The targeted maturity level for the [CUSTOMER] SOC is Level-3 (Defined): It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

**Metrics**

* Process Maturity Assessment Results (CMMI)

**Roles & Responsibilities**

* SOC Manager is responsible for the overall success of this process. The SOC manager ensures that the emphasis, technology, training, and budget are available to support the continuous improvement goals. The SOC Manager sets the maturity objectives.
* SOC Operations Lead is responsible to work with the SOC Manager to define action plans, prioritize action plans, track progress, review, and evaluate action plan effectiveness.
* SOC Analyst is responsible to execute action plans to support continuous improvement.

**Process Linkages**

* Subordinate Procedures

1. Process Maturity
2. Agile Methodology
3. Documentation Standards

* Related Process & Procedures

1. Business Measurement Process (Metrics)

**Process Owner**

SOC Manager

## Process Maturity

**Description**

The purpose of this procedure is to detail the steps necessary for process maturity as outlined in Process Improvement Process. The goal of this procedure is to provide the [CUSTOMER] Security Operations Center (SOC) with a continuous process improvement program that adheres to the Carnegie Mellon, Software Engineering Institute, Capability Maturity Model (SEI/CMM) Level-3. This procedure should be performed periodically (as needed) and all processes should be reviewed every 180 days. The next scheduled appraisal is planned for: MMM DD, YYYY.

**Step 1 - Perform Assessments**

**Score Maturity**

The SOC Appraisals will use the Standard CMMI Appraisal Method for Process Improvement (SCAMPI). Method C will be used for internal appraisals, the SOC leadership team will organize the assessment and an employee external to the SOC [CUSTOMER] will conduct the on-site portions of the assessment.

**Appraisal Method**

**Planning Phase**

The purpose of the planning phase is to review the appraisal methodology (this document) as well as to prepare the logistical aspects for the on-site phase of the appraisal.

* Scope Appraisal - While the scope of appraisals will not change from one appraisal to the next, (scope encompasses the entire SOC), a review of any specific goals, specific deadlines, or results reporting changes should be discussed during this step. Any additional decisions to be made by the SOC sponsors and SOC leadership should be made during this phase as to not impact the appraisal process.
* Plan Appraisal - Plan appraisal involves development of the appraisal plan, establishing the availability of planned interviewees during the on-site period, planning the logistic requirements of the appraisal (meeting rooms, support staff availability, etc.), establishing the roles of appraisal team members, and verifying the appraisal schedule with all affected parties. It also involves verifying who will receive data upon appraisal conclusion.

**Preparation Phase**

The purpose of the preparation phase is to prepare the appraisal team for the on-site activities and conduct a preliminary gathering and analysis of data through the Appraisal Record Matrix (ARM).

* Prepare - Prepare appraisal team involves reviewing the details of the appraisal with the team. The facilitator reviews with the team the SEI-CMMI and appraisal method, appraisal plan, schedule, information regarding the SOC, wiki evidence, goals for the organization, and any additional parameters. Specific responsibilities for each team member are assigned.
* Analyze Evidence - The appraisal team analyzes the data gathered in the Appraisal Record Matrix (ARM) and determines areas for practice validation, identifies potential discrepancies in responses, and performs a gap analysis against the SEI-CMMI. This process element results in a set of exploratory questions and anticipated responses for use during the project lead interviews (conducted by an assessor external to the SOC). Anticipated responses will be derived from the ARM and used to correlate the interview responses with OneNote procedures and documentation during the onsite phase.

**Onsite Phase**

The purpose of the onsite phase is to explore the results of the preliminary data analysis, and provide an opportunity for practitioners at the appraised entity to participate in the data gathering and validation process.

* Interview Practitioners - The interview portion of the appraisal begins with an introductory session with the appraisal participants to review the appraisal process and affirm SOC commitment to the appraisal. Next, the session facilitator introduces the team, explains the purpose of the session, and asks each practitioner the exploratory questions. All referenced documents should be contained on the framework. There is a separate session for each practitioner. This interview typically provides corroborating and clarifying data in relation to the evidence collected (recorded in the Appraisal Record Matrix (ARM)).
* Analyze Data Tracking Sheet & Develop Preliminary Findings - The appraisal team analyzes the evidence and consolidates the data tracking sheet. The voting members systematically analyze the data from all sources to generate a list of preliminary findings related to the process areas and capability levels under investigation. Finally, this data consolidation step allows the appraisal team to determine any needed changes in the schedule or outstanding elements of the data gathering process.
* Compile Findings - Develop final findings involves analyzing the preliminary findings and ARM in light of the contents of the capability levels, determining the estimated process capability for each process area investigated, and consolidating the preliminary findings for presentation to the sponsor.

**Reporting Phase**

The reporting phase is the concluding phase of the appraisal process in which the team performs its final analysis of all data gathered during the previous three phases and presents its findings to the sponsor.

* Finalize Scoring & Report Outcomes - Finalize scoring involves synthesizing the Appraisal Record Matrix (ARM) into a rating profile. The team reviews notes and achieves consensus on the capability level for each process area. The findings developed during the onsite phase and analysis of the SOC, are presented and explained to the sponsor by the appraisal team.
* Manage Appraisal Records - Managing appraisal records involves the proper disposal of all materials gathered and created during the appraisal. Most intermediate work products and inputs will be destroyed while the final ARM, findings, and final report are sent to the sponsor.
* Review Results & Report Lessons - Report lessons learned involves synthesizing information about what did and did not work during the appraisal and suggestions for improvement. This step will also incorporate a review of the appraisal results to determine faults in process and potential areas of improvement.

**Business Process Metrics**

* Business Measurement Process (Metrics) - Defines the maturity and process performance measurements.

**Appraisal Timeline**

* The following is the Appraisal Timeline:

**Step 2 - Create Action Plan**

Within two weeks of the appraisal, an action plan will be created to address the results of the appraisal. The steps below can be used to create this action plan:

* Determine steps needed to address the appraisal results

1. Interview and observe analysts to validate the as-is conditions.
2. Brainstorm ideas for improvement, including SOC Analysts and management.
3. Document improvement plan (evidence of maturity)
4. Knowledge Base revisions to document the changes implemented for the improvement process.

**Step 3 - Execute Improvements**

On the timeline defined by the action plan, improvements will be made to address the results of the appraisal.

* Update process documentation in knowledge base

1. Document changes in the appropriate knowledge base page utilizing the Documentation Procedures.
2. Communicate changes to stakeholders (SOC Analysts and Management)
3. Nightly automated knowledge base change e-mails will notify all shifts of the change.
4. SOC Analyst verbal communication is to be used to reinforce the process changes made in the knowledge base.
5. Track progress of change implementation, update knowledge base as necessary.
6. Ensure successful completion by process and procedure review.

## Agile Methodology

**Summary**

The term Agility is used to describe a business process that is characterized by rapid and iterative execution. The ability to rapidly complete required tasks is critical to the rapid development of the [CUSTOMER] SOC. These practices are well understood and documented in the agile methodology processes (<http://martinfowler.com/articles/newMethodology.html>).

**Agile SOC Operations**

Agility within Security Operations is not simply the continuous improvement of processes and procedures; this extends also to technology and people. A success organization (or team) continuously refines their operations to obtain better performance across all services. Whether responding to a zero-day exploit, deployment of new technology systems or use cases our objective is to maximize the effectiveness of our operations (People, Process and Technology) to enable the business through security risk management.

**Awareness: Monitoring and responding**

* Organizational Strategy occurs in the first loop. Activities which occur within this loop are central to the success of the organization.
* The organizational strategy must be reflected within the organizations mission and vision statement

**Balance: Improving existing processes**

* Operational Efficiency occurs in the second loop; constant adjustment and fine tuning of standard operating procedures to achieve the best overall performance.
* Detect, identify and errors, gaps and/or areas of improvement-efficiency

**Agility: Creating new operations (processes, procedures, or capabilities)**

* Operational Effectiveness occurs when persons build new capabilities and systems to address new issues, threats or opportunities.
* Occurs when a new issue, threat or opportunity is detected and/or required.

**Agile procedures**

* Rapidly document a first draft of any needed process or procedure.
* Leverage the initial draft process and procedures in daily operations.
* Subject the draft to continuous process improvement (performed by SOC Analysts and management during daily use).

1. Any analyst that identifies a process improvement or change immediately documents the change in the knowledge base process, i.e. Azure Sentinel Workbook "SOC Process Framework".
2. A full revision history is kept to track and maintain changes.
3. A nightly e-mail is sent to the SOC analysts and management with all process changes listed.

* Periodic process/procedure reviews are used to maximize Process Maturity and effectiveness.

1. Use monthly KPI metrics to make improvements / adjustments.

## Documentation Standard Procedures

**Description**

This procedure illustrates the process for creating or updating process and procedure documentation on the SOC Knowledge Base. All SOC procedures are maintained within the Knowledge Base; procedure modifications and version control are also handled through the Knowledge Base. The Knowledge Base contains links to other Knowledge Base sections that house Main, Analytical, Operational, Technology, SOC Shift Logs, Tools and Resources, and other SOC related information.

**Documentation Procedures**

The following procedure describes how to make updates and changes to the SOC Process Framwork Workbook within Azure Sentinel. A flowchart illustration of this process is also available below.

1. Login to Azure Sentinel through the Azure Portal. <https://portal.azure.com/>
2. Navigate to the SOC Process Framework Workbook and click "View Saved Workbook"
3. Click "Edit" to open the workbook in Edit Mode

1.1 Does the desired topic exist?

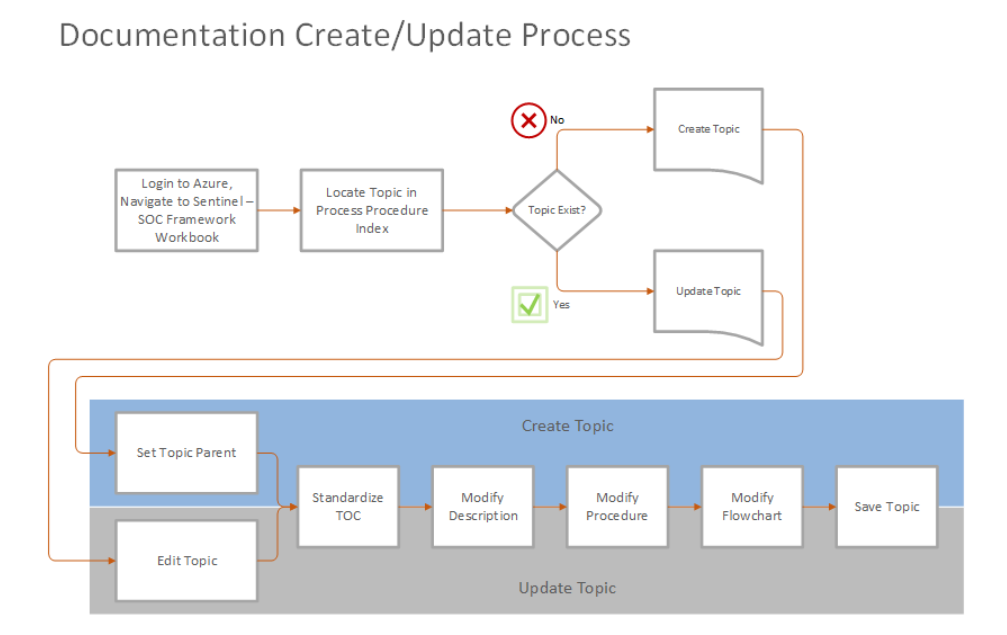
* If NO,
* Create a New Procedure Page using the +Add to add a new Text Page.
* Use an appropriate and descriptive Title Header as the Topic Name.
* Set Topic Parent to appropriate Topic Parent - This is a link or Tab on the Main Topic Menue.
* Skip to Update procedure documentation step

1.2 Select Procedure

1.3 Update procedure documentation

* Standardize TOC (Table of Contents)
* Modify Description
* Include brief overview of the procedure and the purpose of the procedure.
* Modify Procedure
* Include descriptive procedure steps
* Add references as necessary
* Match procedure steps to flowchart items
* Modify Flowchart
* Update Visio flowchart
* Save as .jpg file
* Save .jpg file as an attachment in the Knowledge Base Topic and embed in the procedure document.

1. Click "Save"



## Compliance Process

**Purpose**

The purpose of this document is to provide the process framework for the [CUSTOMER] SOC to comply with internal [CUSTOMER] IT & security policies, and to describe how the [CUSTOMER] SOC supports the broader corporate regulatory requirements. This process includes a list of procedures associated with applicable regulatory compliance and internal standards.

**Scope**

This process applies to all procedures implemented in the [CUSTOMER] SOC for regulatory compliance and compliance related activities. The scope of this process includes Azure Sentinel application and its defined regulatory Use Cases (see also Compliance Support). The primary regulations that are supported by the SOC are PCI, SOX, HIPAA, and general privacy best practices (PII/Personally Identifiable Information).

**Process Summary**

The SOC Manager and Lead Engineer will ensure that all systems in use by the [CUSTOMER] SOC are compliant with [CUSTOMER] Policies. The Lead Engineer will design and deploy appropriate Azure Sentinel content to satisfy the regulatory compliance use cases.

This process will contain one primary subordinate procedure; Compliance Support Procedures will document how the SOC meets [CUSTOMER]'s internal IT and security policies, corporate regulatory requirements, and will specify, down to individual use cases, how each regulatory requirement (as specified by the compliance owner) is to be met. These procedures will leverage foundational Azure Sentinel and underlying SaaS/PaaS capabilities such as M365 Compliance Manager and Azure Security Center.

Regulatory Drivers

1. Cybersecurity Maturity Model Certification (CMMC): [Cybersecurity Maturity Model Certification (CMMC) (osd.mil)](http://osd.mil)
2. PCI: <http://www.pcisecuritystandards.org>
3. Sarbanes-Oxley Act (SOX): <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ204.107>
4. Health Insurance Portability and Accountability Act (HIPAA): <http://aspe.hhs.gov/admnsimp/pl104191.htm> General privacy best practices (PII): <http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>

**Compliance Process (High-Level)**

1. Develop appropriate Use Case documentation to support the solution to be implemented in Azure Sentinel.
2. Leverage Azure Sentinel Workbooks/Reports built-in (Templates)
3. Refer to the Use Cases Procedures in Design Process
4. Determine priority for implementation
5. Identify specific content to be generated through Azure Sentinel
6. Design and implement Azure Sentinel Use Case components
7. Validate output and reporting mechanisms
8. Have compliance owner validate output
9. Update components and reporting as requirements change

**Metrics**

* Reports defined - Contract Progress
* Use cases defined & completed - Contract Progress

**Roles & Responsibilities**

* SOC Manager is responsible for the overall success of this process. The SOC manager ensures that the technology, training and budget is available to support SOC compliance.
* Lead Engineer will devise all content as defined in the appropriate use cases and will administer the content within Azure Sentinel in accordance with internal security policies.
* Security Compliance Team is responsible to provide policy and standards; provide reporting requirements; provide SOC related change/problem management of policies and standards; and receive compliance reports.

**Additional Processes**

* Subordinate Procedures

1. Compliance Support Procedures

* Related Process & Procedures

1. Business Measurement Process (Metrics)
2. Process Improvement
3. Daily Operations Process
4. Reporting Process
5. SOC Use Cases

**Process Owner**

SOC Manager

## Compliance Support

**Summary**

The Compliance Procedure is designed to provide the SOC with a standardized method to ensure that [CUSTOMER] IT & security policies are adhered to during daily operations. Small and mid-size organizations may centralize compliance responsibilities into the SOC while larger organizations may have separate risk and compliance organizations with which the SOC will interoperate and collaborate. Organizations of all size significantly increase efficiency and transparency by mapping internal processes to specific external regulatory standards that are in scope for the organization (e.g. CMMC, PCI, HIPAA). Mapping and reporting against a defined international/external standard enables the SOC to dedicate focus on operations and not repeated administrative reporting tasking.

As part of [CUSTOMER]'s Information Systems Division, the SOC is expected to adhere to and assist with enforcement of all applicable [CUSTOMER]'s Policies. The requisite policies are listed below.

**Scope**

All SOC Procedures and Personnel are subject to and required to adhere to the [CUSTOMER] IT & security policies. In addition, where applicable, these policies are to be enforced through system and reporting/alerting design.

**Procedure Description**

The compliance procedure described below is intended to describe the compliance procedures in place within the SOC to adhere to all [CUSTOMER]'s Policies and applicable legal regulations.

1. An initial review of the [CUSTOMER] Corporate Policies is to be completed and the Applicable Policies & Standards included in the Applicable Policies & Standards listing below.
2. The listing of Applicable Policies & Standards below will be periodically reviewed and updated as defined in the Process Maturity Procedures.

* If new policies are released, existing policies are expanded, or the Procedures of the SOC are updated, the listing of applicable policies should also be updated.
* In addition, if any applicable legal regulations are added or expanded to include the standard operations of the SOC, those should also be listed below.

1. As SOC Content is developed, the Applicable Policies & Standards listing below is to be consulted and the content developed in accordance with the relevant policies.
2. During SOC operations (normal and abnormal), SOC personnel are expected to adhere to and assist with enforcement of all applicable policies.
3. All Regulatory Compliance procedures are to be included in the Compliance Support topic.

**Applicable Policies & Standards (Adherence & Enforcement)**

The following internal policies are examples and may include information applicable to the SOC or SOC Operational Procedures:

1. Cybersecurity Maturity Model Certification (CMMC): [Cybersecurity Maturity Model Certification (CMMC) (osd.mil)](http://osd.mil)
2. FedRAMP/NIST 800-53: SP 800-53 Rev. 5
3. PCI: <http://www.pcisecuritystandards.org>
4. Sarbanes-Oxley Act (SOX): <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ204.107>
5. Health Insurance Portability and Accountability Act (HIPAA): <http://aspe.hhs.gov/admnsimp/pl104191.htm>
6. General privacy best practices (PII): <http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>

**Process Procedures**

1. Subordinate Procedures

1.1 Validation of O365 Configuration against required compliance framework

* SOC managers shall leverage O365 Compliance Manager capability to validate both Microsoft and [CUSTOMER] responsible controls
* Assign appropriate user/admin access for Compliance Manager
* Select appropriate Compliance Manager Template (ISO 27001, CMMC Level 3, etc.)
* Review recommended improvement actions and assign as appropriate for completion
* Those responsible for completion shall document implementation and test results in Compliance Manager for customer-responsible controls
* Leverage reporting capabilities of Compliance Manager to report both Microsoft and [CUSTOMER] actions for internal and external requests

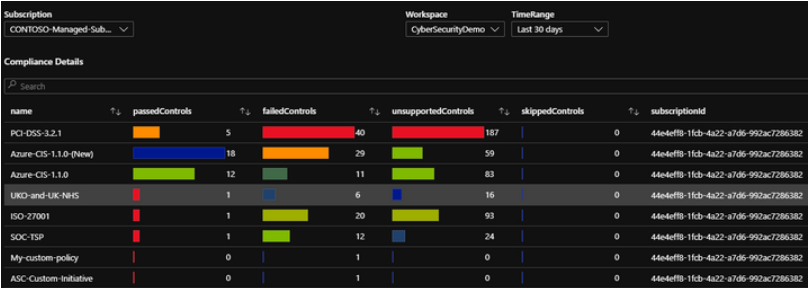
1.2 Validation of Azure Configuration against required compliance framework

* Use of Azure Security Center.
* Azure Security Center helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard.
* Security Center continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in the standards applied to your subscriptions. The dashboard reflects the status of your compliance with these standards.
* When you enable Security Center on an Azure subscription, the Azure Security Benchmark is automatically assigned to that subscription. This widely respected benchmark builds on the controls from the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) with a focus on cloud-centric security.
* The regulatory compliance dashboard shows the status of all the assessments within your environment for your chosen standards and regulations. As you act on the recommendations and reduce risk factors in your environment, your compliance posture improves.

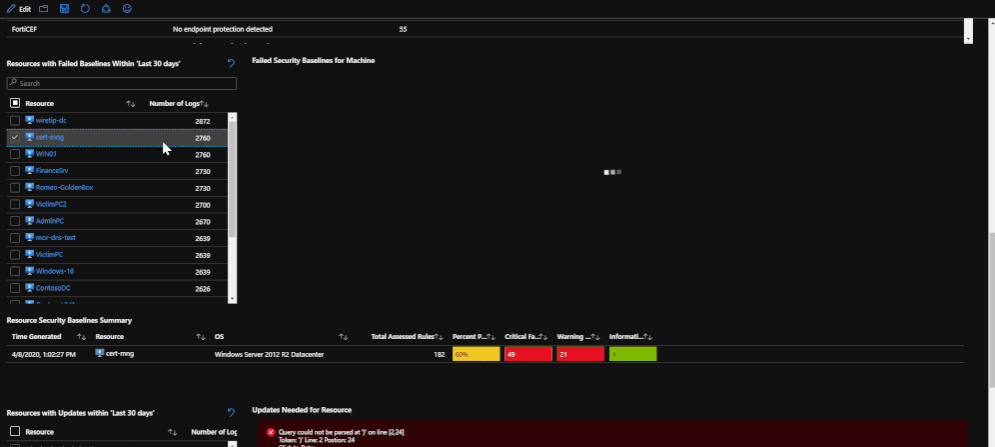
1. Related Processes & Procedures

2.1 Event Management Process

1. See also Azure Sentinel's Workbook: **ASC Compliance and Protection**







**Detailed Compliance Support Steps**

**Step 1: Receive Compliance Requirements**

The first step involves the compliance team providing the SOC with a set of logging and reporting requirements.

1. Compliance team provides logging & reporting requirements.
2. Determine which needs can be met by the SOC Operational Processes.

**Step 2: Identify Data Sources**

The second step will also need to be completed with assistance of the data/business owners.

1. Develop listing of data sources necessary to meet requirements collected in Step 1.
2. Identify system owners that maintain data required to meet the logging/reporting requirements (i.e. platform admins, application admins, DB admins).
3. Provide system owners with steps necessary to provide audit/logging information to Azure Sentinel Connectors.
4. Note: If all requirements cannot currently be met with Azure Sentinel, notify the compliance team and provide alternate recommendations (if available).

**Step 3: Add Data Sources to Sentinel**

The third step requires support from the system owners & administrators to provide the interfaces necessary for Azure Sentinel to collect the required information.

1. Coordinate with system owners to supply logging/audit information to Azure Sentinel.
2. Provide support as necessary (i.e. links to examples or system documentation) if system owners cannot supply the necessary information.
3. Once system logs are transmitted to an Azure Sentinel, verify that the required field and trace information is available and is being properly indexed in Azure Sentinel.

**Step 4: Create Reporting**

1. From the requirements gathered in Step 1, generate the trends, queries, and reports necessary to meet the reporting criteria.
2. Schedule reports as necessary to provide automatic generation and distribution to the compliance teams, SOC, and system owners.
3. Most reports will be generated on a regular basis; however, it may be necessary to generate some on an 'on-demand' schedule. These reports should be prepared, but not scheduled for automatic execution or distribution. Work with compliance teams and system owners to generate meaningful, useful reports that can aid them with the secure operation of their systems and in meeting the compliance objectives of the organization.

**Step 5: Review and Approve Reporting Contents & Schedule with Compliance Team**

1. Once reports have been generated, verify with the compliance team and system owners that the delivered reports are applicable, meaningful, and useful in meeting the organization's compliance objectives.
2. Conduct periodic reviews of compliance reporting (as part of the Process Maturity cycle) to verify that the services and reporting provided to the compliance teams by the SOC are useful.

**Compliance Status Matrix**

|  | **SOX** | **HIPPA - Benefits** | **HIPPA - PHARMA/Optical** | **PCI** | **CMMC** | **Step Description** |
| --- | --- | --- | --- | --- | --- | --- |
| Assigned | Matt E. | Randal C. | Beth B. | Edward H. | Rin U. |  |
| Step 1 Status |  |  |  |  |  | Receive Compliance Requirements |
| Step 2 Status |  |  |  |  |  | Identify Data Sources |
| Step 3 Status |  |  |  |  |  | Add Data Sources to Azure Sentinel |
| Step 4 Status |  |  |  |  |  | Enable/Edit or Create Reporting |
| Step 5 Status |  |  |  |  |  | Review and Approve Reporting |

**Supporting Processes**

1. Related Process & Procedures

* Internal Compliance
* Process Maturity

**Process Owner**

SOC Manager

## Business Continuity & Disaster Recovery Process

**Purpose**

The purpose of this document is to provide the framework for [CUSTOMER]'s Security Operations Center (SOC) Business Continuity and Disaster Recovery plans. This process will include a list of procedures associated with a business continuity plan based on specific scenarios and having detailed disaster recovery plans. The goal is to provide a plan that minimizes impact to service capability in the event of disaster scenario or technology failure.

**Scope**

This process applies to all procedures implemented in the [CUSTOMER] SOC to minimize disruptions to service or capability. The scope of this process is strictly limited to the [CUSTOMER] SOC. This process will be documented within the BC/DR Procedure page.

**Process Summary**

The Lead Engineer will provide the appropriate technology configuration for Disaster Recovery and detailed plans for Business Continuity. A business continuity and disaster recovery plan is essential to ongoing service capability as well as overall business security and health. As part of this effort, the Azure infrastructure may be configured for fail-over on all asset pairs.

**BC/DR Planning Process**

* Identify BC/DR scenarios
* Identify impact per scenario
* Develop detailed recovery plans for each scenario and establish objectives.

1. RTO - Recovery Time Objectives
2. RPO - Recovery Point Objectives

* Test recovery plans on an annual basis
* Evaluate effectiveness of plans
* Review plan on a quarterly basis

**Metrics**

* Process Maturity Assessment Results

**Roles & Responsibilities**

* SOC Manager is responsible for the overall success of this process. The SOC manager ensures that the technology, training and budget is available to support the BC/DR plans.
* Lead Engineer is responsible for maintaining appropriate technical configurations to meet defined recovery time and point objectives.
* SOC Operations Lead is responsible to work with the SOC Manager to define BC/DR scenarios, plans, test, review, and evaluate plan success.
* SOC Analyst is responsible to identify service capability disruptions, execute BC/DR plans, and provide continuous improvement feedback.

**Applicable Policies & Standards**

* http://url - Insert [CUSTOMER]'s Policies Here

**Supporting URLs**

* SLA for Log Analytics | Microsoft Azure
* Service Level Agreements Summary | Microsoft Azure

**Supporting Processes**

* Related Process & Procedures

1. Business Measurement Process (Metrics)
2. Process Improvement
3. Daily Operations Process
4. Reporting Process

**Process Owner**

SOC Manager

## Business Continuity & Disaster Recovery Plans

**Overview**

All BCDR Plans for the [CUSTOMER] and/or SOC are maintained at (insert link here).

Links

* https://url Insert [CUSTOMER]'s BC/DR Plans Here

# SOC Operational Processes & Procedures

| **Process Name** | **Procedures** | **Description/Comments** |
| --- | --- | --- |
| Incident Management Process |  |  |
|  | Incident Triage | Describes how a SOC Analyst determines what action to take based on Alerts fired and Incidents Created within Azure Sentinel |
|  | Callout / Escalation | Instructions for the SOC Analyst for Incident escalation of all severities |
|  | Incident Management Procedure | Documents the step-by-step flow involved in the closed-loop management of Azure Sentinel Incidents |
|  | Crisis Response | Documents the steps a SOC Analyst should take in the event a cyber-crisis situation is recognized |
|  | Shift Log Management | Instructions for the SOC Analyst describing what information should be provided in a shift log entry |
|  | Phone Bridge Details | Instructions on how to start a phone bridge conference |
|  | Vulnerability Scanning Schedule | Scanning schedule for vulnerability assessments & pen testing exercises |
|  | IP & Domain Blocklisting | Tracking all IP and Domain black lists detected by the SOC |
| Daily Operations Process |  |  |
|  | Daily Ops Meeting | Document all aspects of the daily operations call or meeting for the SOC's situational awareness |
|  | Problem Tickets and Change Controls | Procedures that documents how non-emergent processes associated with SOC operations are handled |
|  | Shift Staffing Schedule | Procedures to ensure appropriate staffing and establishes standard shift schedules |
|  | Shift Turnover | Instructions for conducting a standard shift turn-over |
| Weekly Operational Process |  |  |
|  | Weekly Threat Intelligence Report | Instructions for creating the Weekly Threat Intelligence Report |
| Reporting Process |  |  |
|  | Periodic Reports | Procedures for producing daily and weekly reports in the SOC |

## Incident Triage

**Description**

This procedure describes how a SOC Analyst determines what action to take based on Alert(s)/Incident(s) observed within Azure Sentinel. Triage is the process of evaluating multiple Incidents to determine which are the most critical and prioritizing your response based on this analysis. This procedure will result in one of the listed response actions.

**Step 1 - Determine Category Type and Action Needed**

Apply the decision matrix below using the category type and asset priority. This is used in conjunction with the SOC Rule Response Procedures for the rule triggered. The severities defined below are based on adaptations from the [CUSTOMER's] Threat Matrix.

| SEV- 4 | (Minor) - Informational, some security impact |
| --- | --- |
|  | - Non-critical systems (e.g., associate workstations), OR Non-critical infrastructure  - No effect to the organization’s ability to provide all services to all users  - No breach of data / information was exfiltrated, changed, deleted, or otherwise compromised  - Single systems and/or users affected that contains PII or PCI  - Minimal recovery required  - Escalation directly to the respective Business Unit for remediation |
|  | Examples: |
|  | - Receipt of e-mail expressing “low-level” threat  - Discovery of a Phishing event without report of compromise |

| SEV- 3 | (Moderate) - Intermittent security alerts, moderate security impact |
| --- | --- |
|  | - Non-critical systems (e.g., associate workstations), OR Non-critical infrastructure; internal impact is less than 5%  - Medium Severity, typically issues such as policy violations, single system infections and/or whereas the malicious code is known and contained  - Escalation directly to the respective Business Unit for remediation  - Severity 4 events that are not resolved within the established Service-Level Agreements (SLAs) |
|  | Examples: |
|  | - Isolated reconnaissance activities (network) by potential attackers  - Password policy violation by an employee  - Virus/Malware infection isolated to an individual user  - Single report of suspicion that someone has gained unauthorized access to his/her account  - Phishing/spear-phishing threat to compromise customer data  - Detection and removal of viruses by a server before it enters the network  - Repeated port scanning from same external source |

| SEV- 2 | (Major) - Serious Impact or Compromise, Incident/Attack affects multiple customers |
| --- | --- |
|  | - Operations can continue in a restricted fashion, although long-term productivity might be adversely affected  - Organization has lost the ability to provide a critical service to a subset of system users  - Single High Value Targets affected or potentially compromised  - Impact to company confidential data  - Major or business-critical applications are affected  - Multiple systems that contain PII or PCI and/or users affected  - Critical impact to the organization (reputational)  - Severity 3 events that are not resolved within the established Service-Level Agreements (SLAs) |
|  | Examples: |
|  | - Improper usage of high-level accounts such as root or administrator  - Phishing threats to compromise internal, sensitive data  - Vulnerability on a [CUSTOMER]'s non-transactional server or subnet  - Multiple users/workstations infected by malware  - Unauthorized disclosure of [CUSTOMER]'s internal or confidential information (i.e. email, blogs, news groups)  - Spear-phishing attempts targeting [CUSTOMER]’s executives  - Internal web site was compromised without authorization |

| SEV- 1 | (Critical) - Critical Compromise, Major Service disruption or publicly displayed attack |
| --- | --- |
|  | - Mission critical systems that support multiple businesses (systems defined as mission critical per Ops/Tech) OR sectors of the critical infrastructure (systems defined as Tier 0 for BCP/DR purposes)  - [CUSTOMER] has experienced a substantial loss of service and/or revenue  - Prevents [CUSTOMER] from making sales, or meeting legal or contractual obligations  - Potential regulatory fines or penalties  - Critical business impact to the company; competitive edge, reputational, data-privacy breach  - All or a substantial portion of [CUSTOMER]'s mission critical data is at a significant risk of loss or corruption  - [CUSTOMER]'s business operations have been severely disrupted  - Potential large financial risk or legal liability  - Multiple systems (HVT), significant number of workstations, groups and users affected; high probability of propagation  - Mission critical system (e.g., payroll system) to a single business  - Significant and immediate threat to human safety  - Complete system compromise and possible full data-privacy breach  - Law Enforcement assistance is required  - Severity 2 events that are not resolved within the established Service-Level Agreements (SLAs) |
|  | Examples: |
|  | - Unauthorized access to sensitive systems (HR, Payroll, Finance, etc)  - Distributed Denial of Service Attacks or DoS Attacks  - Theft of computer systems and/or media containing sensitive/confidential information  - Malware causing destructive outbreak to a large number of workstations or servers (Zero day attacks)  - Defacement of [CUSTOMER]'s Web Sites  - Vulnerability on an [CUSTOMER]'s transactional server or subnet |

**Step 2 - Initiate Action**

Initiate appropriate response action based on the outcome of the decision matrix above.

| **SEV1** Annotate-Tag the Incident |
| --- |
| A Senior SOC Analyst contacts the SOC manager with notification of potential callout. After review,confirmation, approval. Initiate the Critical Callout /Escalation Procedures with a response time requirement of [10] minutes. |
| Teams or Email contents of potential callout  - Time/Azure Sentinel Incident Number #  - 0730/20140312-007 (S1) Covered information disclosure  - Include your name as well as a phone number in any Teams or Email message |

| **SEV2** Annotate-Tag the Incident |
| --- |
| A Senior SOC Analyst contacts the SOC manager with notification of potential callout. After proper review, confirmation, approval. Initiate the Critical Callout /Escalation Procedures with a response time requirement of [20] minutes. |
| Teams or Email contents of potential callout  - Time/Azure Sentinel Incident Number #  - 1830/20100312-004 (S2) IIS Directory Traversal  - Include your name as well as a phone number in any email |

| **SEV3** Annotate-Tag Incident |
| --- |
| Work Incident internally, if a callout is needed promote case to a SEV-2. Follow appropriate rule response procedures. |

| **SEV4** Annotate-Tag Incident |
| --- |
| Low priority, work internally, if callout is necessary, promote case to a SEV-2. Follow appropriate rule response procedures. |

**Step 3 - Document Activity in the Shift Log**

Document the activity in the Shift Log using the Shift Log Management guidelines.

**Step 4 - Continue to Monitor Activity**

Initiate the Focused Monitoring Procedures in support of other teams.

**Step 5 - Follow Up on Activity**

Ensure that the appropriate response action is fully executed and the Incident, IR Ticketing and/or Closure procedures are completed.

**Process Owner**

SOC Manager

## Callout / Escalation

**Description**

The callout procedure is initiated once the on-duty SOC Analyst has completed the Incident Triage Procedures and determined that a callout is warranted. This procedure defines how the SOC notifies the Incident Response Team (IRT) of the recognized incident. Any SEV1 or SEV2 incident will always be escalated to the IRT as a first point of contact. This procedure falls under the Incident Management Process. After callout has been performed, annotate the Incident and Tag it to the proper stage (Senior Analyst escalation).

**Flash Notification**

* Time/Azure Sentinel Incident Number #
* 1830/20100312-004 (S2) IIS Directory Traversal
* Summary - What happened?
* Risk - Why do we care?
* Actions - Escalations?
* Include your name as well as a phone number in any Teams or Email message

**Steps**

**Critical Callout (SEV-1)**

* Open the Azure Sentinel Incident via Incident Management Procedures.
* Notify the Incident Response Team (IRT) via Teams or the telephone
* Wait 10 minutes for acknowledgement

1. On-Call / On-duty IRT team members are messaged by Teams or emailed upon Incident being Tagged SEV-1.
2. Wait 5 minutes for acknowledgement
3. Call on-duty back up again
4. Wait 5 minutes for acknowledgement

* Call Incident Response Management
* Continue to cycle until acknowledgement received

**Urgent Callout (SEV-2)**

* Notify the Incident Response Team (IRT) via Teams or the telephone

1. Wait 20 minutes for acknowledgement
2. Call on-duty team member
3. Wait 10 minutes for acknowledgement
4. Call on-duty back up
5. Wait 10 minutes for acknowledgement

* Call Incident Response Management
* Continue to cycle until acknowledgement received

**Process Owner**

SOC Manager

## Incident Management Procedure

**Description**

The Incident Management Procedure is initiated once the SOC Analyst has determined that an Incident or series of Incidents appear to be related and warrant further investigation. This page details the steps an Analyst should take in order to create an informed and standardized Incident. Azure Sentinel definition: An Azure Sentinel Incident is a container for information about a specific Alert(s), usually with one or more Entities, Alerts, and Events attached. An Incident is used to track, investigate, and resolve Alert(s) of interest or a series of raw and correlated events that created an Alert that need further investigation. An Incident should be created any time an analyst is looking into events of interest through a KQL Query.

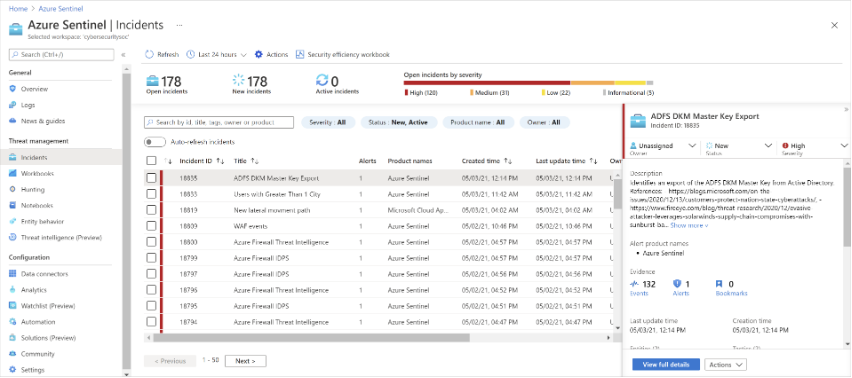
**Azure Sentinel Incidents**

* **SOC Incidents / New:** For newly identified cases before being assigned to the SOC Analysts or the IR team.
* **SOC Incidents / Active - SOC Assigned:** For Incidents analysts are working on internally. Only Incidents that are updated daily by a SOC Tier 1/Tier 2 Analyst.
* **SOC Incidents / Active - IR Assigned & Tagged:** Used by the Incident Response Team investigators to manage their Incidents.
* **SOC Incidents / Active - ExT Assigned & Tagged:** Used by External Team investigators to manage their Incidents.
* **SOC Incidents / Closed:** Categories of CLOSED Incidents.

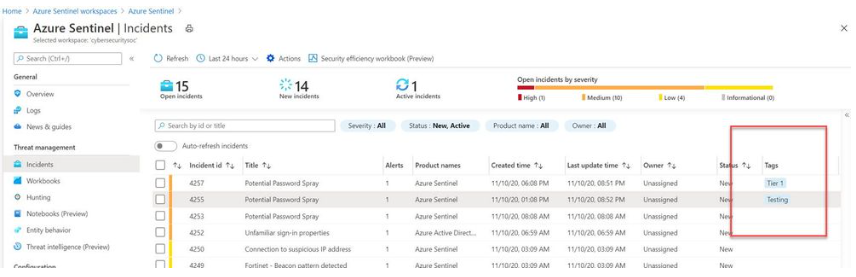
1. **CLOSED - No Risk:** For events that were added to cases and were determined to be of no risk to the [CUSTOMER] Enterprise.
2. **CLOSED - Insufficient Data:** For cases that were unable to determine the root cause. Subcategories might be added for more detailed tracking and measurements.
3. **CLOSED - False Positive:** For cases that were determined to be a false positive.
4. **CLOSED - Remediated:** For cases with a validated conclusion. Subcategories might be added for more detailed tracking and measurements to improve time to resolution.
5. **CLOSED - Other:** Cases that have been closed that don’t match the previously identified closure codes.

**Find an Incident**

From the Azure Sentinel Menu, Select Incidents. The Incidents page lets you know how many incidents you have, how many are open, how many you've set to In progress, and how many are closed.



* You can filter the incidents as needed, for example by tag, status, or severity.

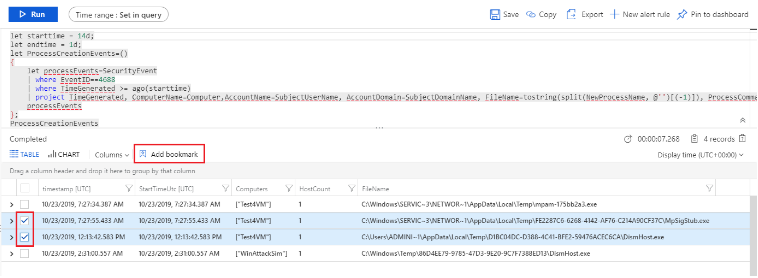


**Procedure**

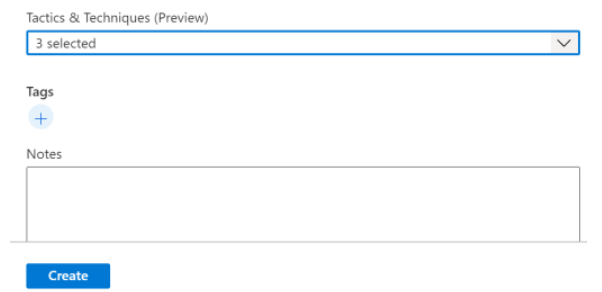
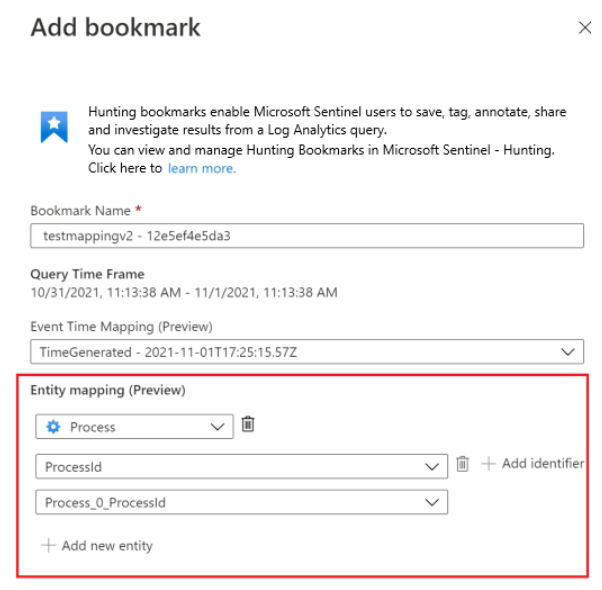
**Open an Incident**

* Determine that an Incident has the appropriate Alerts/Events to investigate (see Incident Triage Procedures)
* Add events of interest to the Incident through Bookmarks and attach them to the Incident.

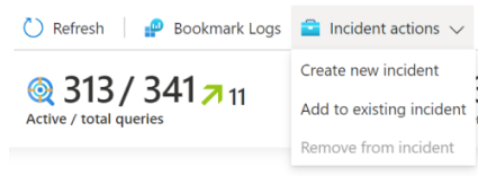
1. Create a Bookmark
2. In the Azure portal, navigate to Sentinel > Logs and execute the desired KQL query.
3. From the log query results list, use the checkboxes to select one or more rows that contain the information you find interesting.
4. Select Add bookmark:



1. On the right, in the Add bookmark pane, optionally, update the bookmark name, add tags, and notes to help you identify what was interesting about the item.
2. In the Query Information section, use the drop-down boxes to extract information from the query results for the Account, Host, and IP address entity types. This action maps the selected entity type to a specific column from the query result. For example:



1. To view the bookmark in the investigation graph (currently in preview), you must map at least one entity type that is either Account, Host, or IP address.
2. Click Save to commit your changes and add the bookmark. All bookmarked data is shared with other investigators, and is a first step toward a collaborative investigation experience.
3. Add bookmarks to a new or existing incident
4. In the Azure portal, navigate to Sentinel > Threat management > Hunting > Bookmarks tab, and select the bookmark or bookmarks you want to add to an incident.
5. Select Incident actions (Preview) from the command bar:



1. Select either Create new incident or Add to existing incident, as required. Then:
2. For a new incident: Optionally update the details for the incident, and then select Create.
3. For adding a bookmark to an existing incident: Select one incident, and then select Add. To view the bookmark within the incident: Navigate to Sentinel > Threat management > Incidents and select the incident with your bookmark. Select View full details, and then select the Bookmarks tab.

**Incident Description**

* Incident Name

1. Use the following Naming convention as follows: yyyy-mm-dd - 001 - Event name and/or details
2. Example: 2021-04-21 - 001 - Local Account Authentication
3. NOTE: This is only for New Incidents created manually.
4. For Incidents created/generated by Security Tools outside of Azure Sentinel, they will already have a Title and Description assigned.

* Incident stage ( Examples: Triaged, Queued, Open, Initial, Follow-up, etc..)
* Incident Severity

1. Assign the Incident severity using the Incident Triage Procedures (i.e. SEV-1, SEV-2, SEV-3, SEV-4)

* Document details and observations (use the following template for information gathering)

1. Attacker Information - Contains Shift log entry and Source IP information including: IP/hostname/port/whoIS/abuse contact/blacklisted/IPAM and Outlook contact info
2. Target Information - Contains Destination IP information including: IP/hostname/port/whoIS/abuse contact/blacklisted/IPAM and Outlook contact info
3. Event Description - IDS/IDP Signature/Firewall Event Analysis/Anti-Virus detail (obtained from filename and website)
4. Analyst Comments - Analyst comments (conclusion) and reference material (previous cases/emails/action items/intel papers)

**Assign the Incident**

* Re-tag the Incident from Open to Under Investigation
* Assign the Incident to yourself or if you are escalating, leave the Incident unassigned and apply the correct annotation-tag described in the
* Perform appropriate notifications (to IR team or SOC Analyst). See the Callout Procedures.

**Updating the Status**

* All SOC Analysts will review the Incident and assign the Incident the appropriate stage. The stage of the Incident will need to be updated as necessary and as defined by the Stage Timing Chart.
* SOC Analysts will update the Incident with the annotation-tag "Follow-up" addressing the following:

1. Actions Taken
2. Follow-up Contact

**Process Owner**

SOC Manager

## Crisis Response

**Description**

A crisis is defined as a series of events that may compromise the integrity of a large number of systems, multiple organizational zones or networks resulting in catastrophic data loss, prolonged organizational downtime, or major financial impact. A SOC Analyst should initiate the Crisis Response procedures for any event that is likely to cause major impact to the organization.

**Step 1 - Gather Information**

The first step a SOC Analyst should do in response to a perceived crisis situation is to gather basic information about the attack. Important information includes:

* Source IP Addresses
* Destination IP Addresses
* Time of Attack
* Context and Depth of Attack
* Estimated Impact

It is very unlikely all information in a Crisis situation will be immediately present, but it is important that the SOC Analyst understands a basic scope of the attack/crisis before engaging another team. **It is critical that all steps taken be documented in the shift log as the steps are being taken.** During a crisis, the Primary Analyst (on-console) will remain on console for the remainder of the shift or until the crisis is remediated. A SOC Analyst that is not on console will be responsible for all communication efforts if a Senior SOC Analyst is not present and would assist the SOC Analyst if present.

**Step 2 - Escalate Events and Notify Teams**

Once an Incident with Alerts/Events or series of Alerts/Events are recognized as a crisis, a Senior Analyst should be contacted immediately. If a Senior Analyst cannot be reached, the SOC Analyst should contact SOC Management.

**SOC Management**

After the situation has been discussed with a Senior Analyst/Manager, a callout to other teams should occur to begin the mitigation process. The SOC should be the central hub of communication during a crisis. **The Incident Responder on-call member should be notified in all crisis situations.**

Here is a sample listing of teams to involve in different crisis situations. Every crisis situation is unique and must be handled in the manner most likely to resolve the crisis.

| **Crisis** | **Teams** |
| --- | --- |
| Virus/Worm Outbreak | Command Center, Helpdesk Team |
| Network Intrusion | Network Team |
| 10+ Server Compromise | Server Team, Network Team |
| Effective DDoS Attack | Command Center, Network Team |
| Outbound Attack on Sensitive Networks (gov, .mil, .cn) | Network Team |
| Serious Impact to Business Processes | Command Center, Network Team, Server Team |

Contact Emails: SOC Contacts Page will contain:

* Brief description of incident
* SOC telephone number

In addition to notifying Security Teams, we should also contact other Ancillary Teams that could monitor or provide assistance during a crisis. **Use appropriate wording. For example instead of "denial of service" you might use "server performance issues" when contacting teams outside of Security.**

Below are distribution lists to reach Field Support managers and team leads for informational emails. These teams should be notified when a crisis is occurring.

| **Distribution List** |  |  |  |
| --- | --- | --- | --- |
| Field Support managers | Emails | Teams | Phone |

Below are manager line numbers for emergency contacts to engage these teams during a crisis.

| Emergency Contacts |  |  |
| --- | --- | --- |
| Team | Description/Actions | Manager's Line |
| Command Center | Initial Crisis Response Point, Information Coordination  Server Team |  |
| Server Team | Analyze and take offline servers |  |
| Network Team | Bring down networked devices |  |
| Applications Team | Application administration |  |
| Field Support (reached via Command Center) | Remote on-site support |  |

**Step 3 - Information Coordination**

Collect additional analytical information about the crisis and coordinate in a manner in which each team receives the same information. It is the Senior Analyst's responsibility to coordinate each team's efforts (if a Senior Analyst/Manager is not available, the task falls to a SOC Analyst that is not on console). This can be done by using one or more of the following communication methods: Conference Call, Phone Bridge, or SOC War Room.

**Conference Call** - If the number of technicians working on the crisis is low (less than 5 people) a conference call can be initiated to coordinate efforts. Note: This is usually only used in the latter stages of crisis resolution when specific technical personnel have been identified to solve the problem. See how to initiate a conference call: Telephone Functions

**Phone Bridge** - Phone Bridges are the standard way of communicating across multiple teams and should be used when more than 5 technicians are on the call. See how to initiate a phone bridge: Phone Bridge Information

Phone bridges will typically include:

* SOC Management
* SOC Support (as needed)

1. Incident Response Team
2. Data Center Operator
3. Event Manager
4. Fix Analyst
5. Fix Manager
6. Ancillary Teams (as needed)
7. Server Team
8. Network Team
9. Applications Team
10. Etc.

NOTE: Teams will identify their Fix Managers, Fix Analysts, and other key players as the Crisis Response requires.

**SOC War Room** - The SOC will likely be the area where multiple teams meet for face-to-face communication. The SOC War Room will be the CCC Conference Room. A Crisis Response situation will supersede any reservations other teams may have for the CCC Conference Room. A Word Document page or a SharePoint OneNote should be created and displayed in the SOC War Room to serve as a whiteboard to capture and manage current response actions.

##Step 4 - Information Management The SOC will provide hourly updates on the crisis to the involved teams as well as Upper Management. A Senior SOC Analyst will provide hourly e-mails and be responsible for keeping each team updated and in sync. Each update should include a timeline of events and current actions taking place by teams. An example is below.

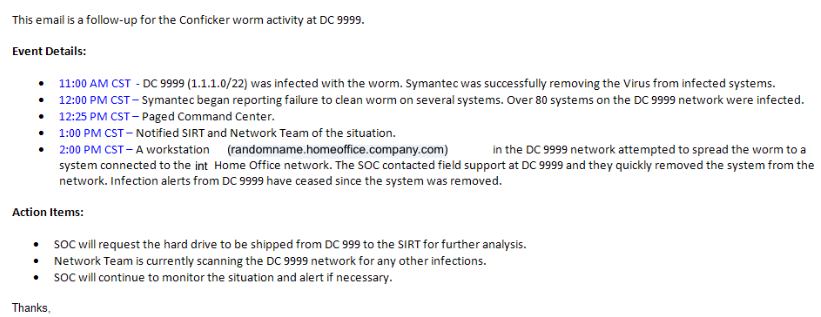
The SOC will generate a final email detailing the events involved in the crisis, steps that were taken to resolve the crisis and further actions that may be necessary to return to status quo once the crisis is deemed over.

**Step 5 - Crisis Remediation**

The final step involves identifying a solution to the crisis and implementing the solution. This step should be carried out by the team that owns the device(s) that will contribute in mitigating the crisis. The SOC can be used to contact internal [CUSTOMER]'s Systems teams and external parties if necessary. Detailed information of a contact to any internal or external person should be documented in the knowledge base ncluding the name, contact information and action of the party.

The SOC should assist in further monitoring of the crisis and coordinating among teams until the resolution is implemented. Long-term incidents involving several teams will require team-member rotation. The SOC will work on a rotating schedule until the crisis is resolved. SOC Analysts will continue to work as scheduled.

**Email Example**



**Process Owner**

SOC Manager

## Shift Log Management

**Description**

This procedure describes how a SOC Analyst should use Shift Logs and what information should be provided in a shift log entry.

**Shift Log Entries**

It is very important for shift log entries to be clear and concise while providing the necessary information. When selecting the appropriate information to enter, an analyst should consider how shift log information is used. We primarily use shift log entries for two purposes: daily operational meetings, historical analysis and event reconstruction.

The following information should be entered in a shift log entry:

* Source IP/hostname and Port (or just multiple if > 5)
* Destination IP/hostname and Port (or just multiple if > 5)
* External vs. Internal
* Base Event name
* Permit vs. Blocked
* Number of related Incidents/Alerts/events
* Basic reasoning behind creating case or closing events

Using the example below, your entry should include roughly the same type of information in the same order.

**Creating Shift Logs**

**Step 1 - Insert New Template Page**

Locate the OneNote Section for the current month and select that Section. Select the Shift Log Template and copy the contents to the new Month/Day Shift page. This page provides the template for the daily shift log pages.

The template page will be located on the Shift Logs section for the selected month.

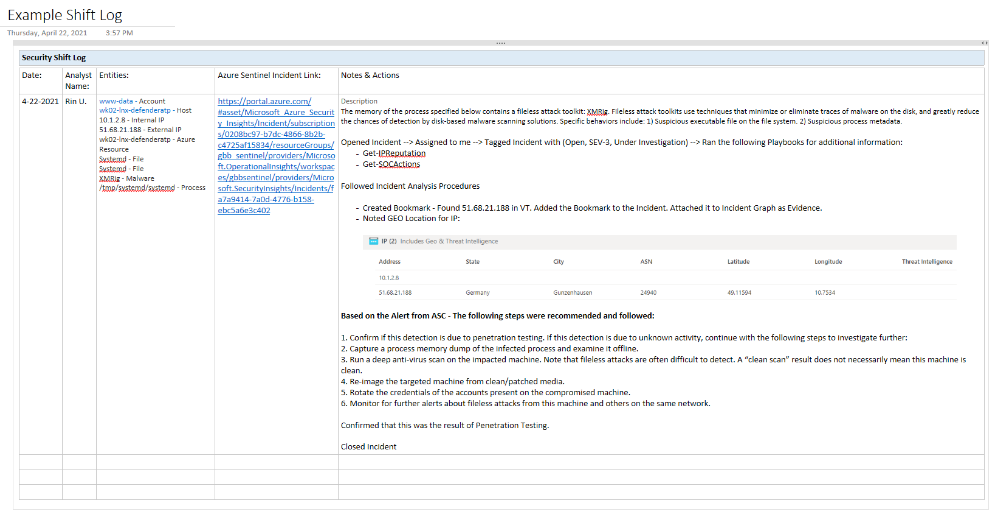
**Step 2 - Enter Date and Analyst Name**

For this example, on the monthly Example Shift Log OneNote Section for the current month we will add the date and Analyst Name to a new page. Each Analyst will have their own page as shown below.



**Step 3 - Make Changes as Needed**

Make the necessary changes to the date and time fields as well as any other links that should be changed. The instructions and proper format for these changes can be found directly Example Shift Log Entry as shown below.



**Process Owner**

SOC Manager

## Phone Bridge Details

**Description**

This process details the steps an Analyst takes to join a Conference Bridge. Please update the information below with current numbers and participation codes.

| Meeting Place dial in numbers: |  |
| --- | --- |
| Internal | 888-677-8000 |
| Local + International | 877-624-8000 |
| Toll Free | 855-446-6338 |

Note: To dial outside of the Company, use +8

**Security Bridge**

425-495-4000 x4953

**Other Bridge Details (changes monthly)**

To start a phone bridge, use the following dial-in code: [253]

**Steps to joining a Conference:**

1. You must use a touch-tone phone to participate in an Instant Meeting Conference.
2. Dial the appropriate access number: a. Participants: Enter numeric passcode followed by a "#" b. Leaders: Enter your numeric leader passcode followed by a # sign.

**Inviting other teams to join a bridge:**

If you need to invite other people onto the SOC bridge please send them the following blurb in email or a meeting invite: "Please join the [CUSTOMER] Security Operations Center on the following phone bridge: Toll Free: [1-866-555-5555], Participant Code: 123456789#"

**Process Owner**

SOC Manager

## Vulnerability Scanning Schedule

**Description**

The [CUSTOMER] Enterprise undergoes frequent scheduled vulnerability scans and penetration testing. The SOC must be aware of the approved scans and their time frame to carry out the scanning/penetration testing. This page serves to provide dates on any approved scans and penetration tests. Additionally, the procedure to verify a suspected scan not listed on this page is also provided.

If a scan or penetration test has been detected and it is not listed on this page, use the Scan Verification Procedure to verify that the scan has been authorized. Any unlisted scans that cannot be verified by the Scan Identification Procedure must be treated as an incident with the appropriate Incident Triage Procedures.

**Vulnerability Scan Scheduling**

Listed below are scheduled vulnerability scans which have been identified as automatic scans:

**[CUSTOMER] Scanner IP Addresses**

| **SCANNERS** |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Server Name | Operating System | Location | IP Addresses | Server Role | SAN |
| VulSERV01 | Server 2019 | East US |  | Console | 500 GB |
| VulSERV02 | Server 2019 | West US |  | Console | 500 GB |

**Port Scan Scheduling**

Listed below is the Port Scanning guidebooks used by [CUSTOMER]:

* Qualys Scanner VLAN Scanning
* Qualys Consultant Scanner Personal Edition User Guide
* Qualys Cloud Agent Getting Started Guide
* Qualys Cloud Platform Evaluator’s Guide

**Manual Scan Scheduling**

Listed in the chart below are approved scheduled scans which have been reported to the SOC.

| **Manual Scan Schedule** |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scan Title | Scan Range | Business Unit | Contact Person | Date/Time of Scan |

**Pen Testing Activity**

The following scan schedules are defined per Web Inspect

| **Penetration Test Activity** |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Business Group | Type of Pen Test | Contact | Source & Destination Information | Pen Tester | Date/Time |

**External IP Addresses for [CUSTOMER]**

These IP's are used by the [CUSTOMER]'s Pen Testers in order to exploit vulnerabilities throughout the [CUSTOMER] environment. There may be other Pen Tester IP's the SOC is not aware of.

* List IP ranges here:

**Process Owner**

SOC Manager

## IP & Domain Blocklisting

**Description**

There are times when the SOC is notified of malicious IP addresses performing scans or exploit attempts. These pieces of information should be tracked within Azure Sentinel so we can automatically be notified if/when the [CUSTOMER] is being attacked by one of these addresses. There are other times when a particular domain name is considered especially malicious and the SOC wants to be notified when someone attempts to or successfully connects to one of these domains. To facilitate this we have created several Blacklists which can be modified by the analyst as new information comes available.

When a malicious IP or domain is identified and added to a blacklist, a search for any previous connection attempts within the past 24 hours must be run in as a KQL query within Azure Sentinel.

Azure Sentinel watchlists enable the collection of data from external data sources for correlation with the events in your Azure Sentinel environment. Once created, you can use watchlists in your search, detection rules, threat hunting, and response playbooks. Watchlists are stored in your Azure Sentinel workspace as name-value pairs and are cached for optimal query performance and low latency.

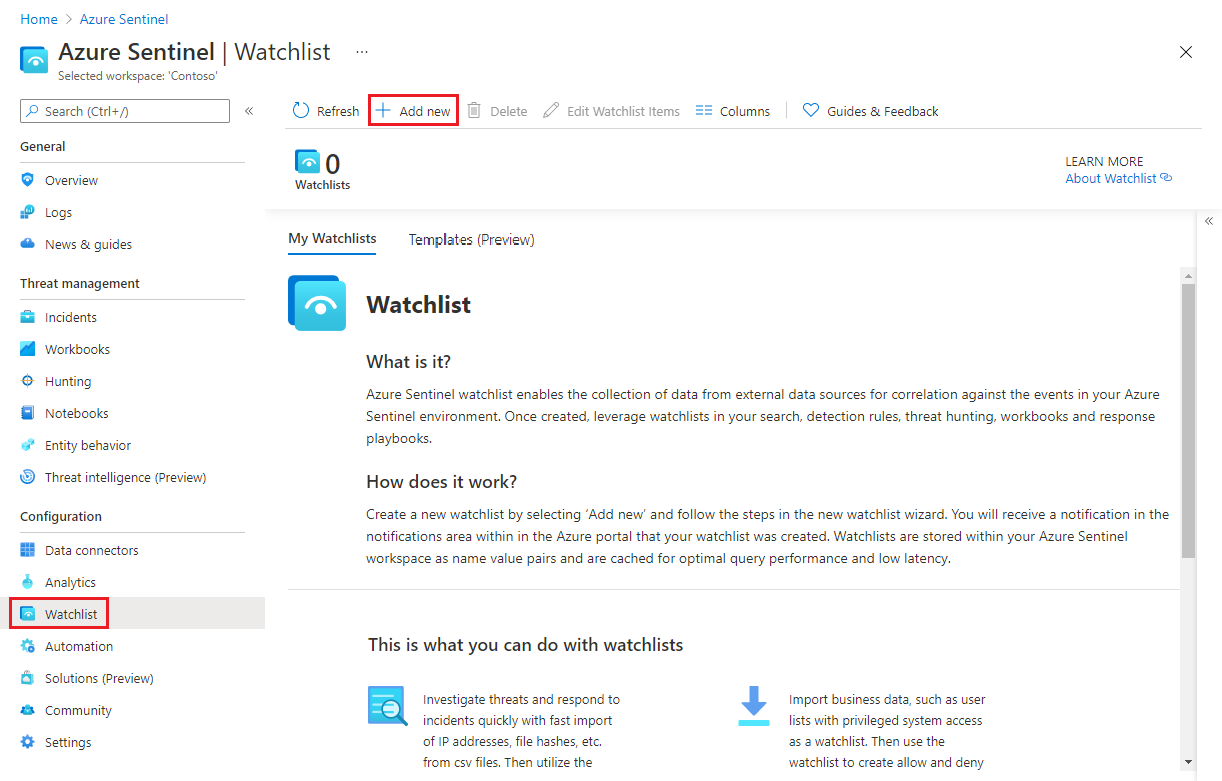
**Common scenarios for using watchlists include:**

Investigating threats and responding to incidents quickly with the rapid import of IP addresses, file hashes, and other data from CSV files. Once imported, you can use watchlist name-value pairs for joins and filters in alert rules, threat hunting, workbooks, notebooks, and general queries.

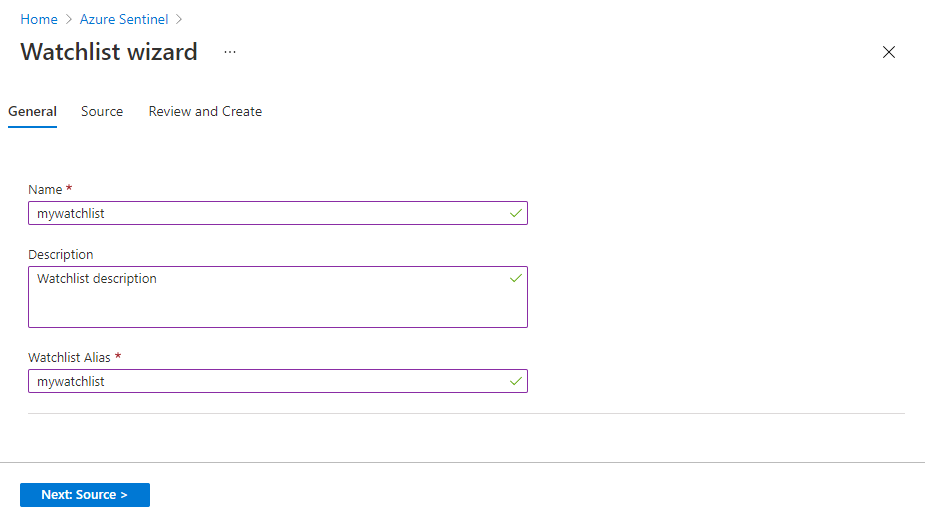
Importing business data as a watchlist. For example, import user lists with privileged system access, or terminated employees, and then use the watchlist to create allow and deny lists used to detect or prevent those users from logging in to the network.

**Insert Watchlist within Azure Sentinel:**

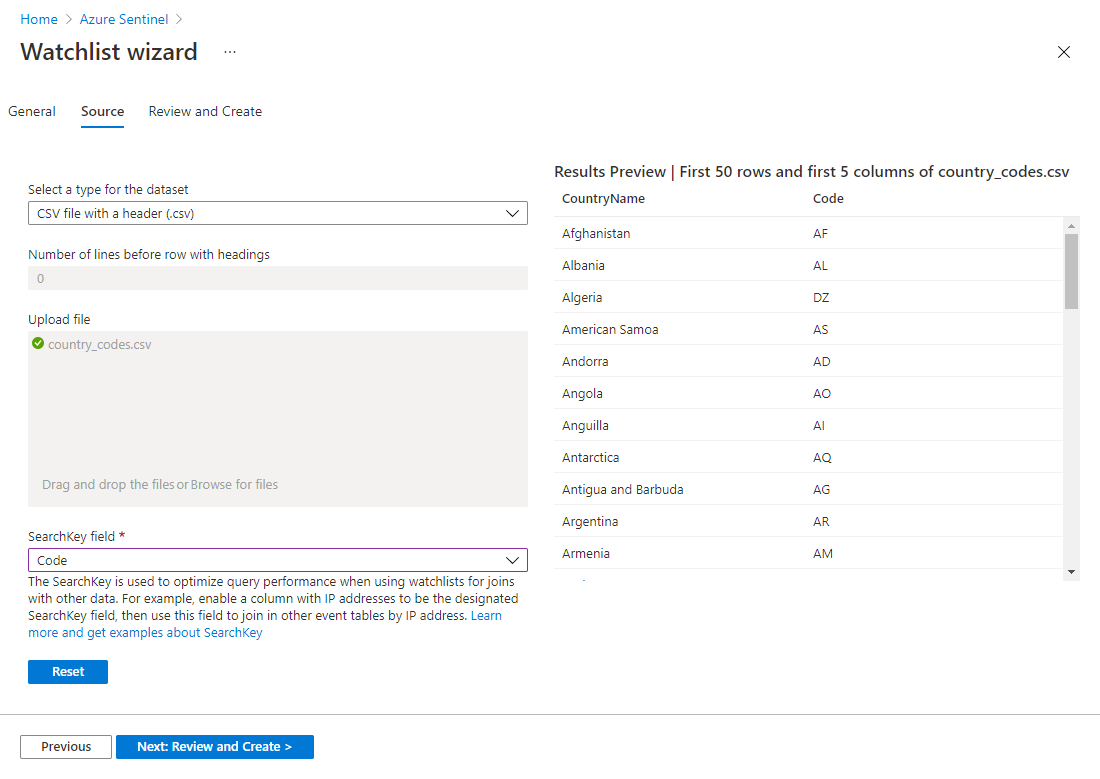
From the Azure portal, navigate to Azure Sentinel > Configuration > Watchlist and then select Add new.



On the General page, provide the name, description, and alias for the watchlist, and then select Next.



On the Source page, select the dataset type, upload a file, and then select Next.

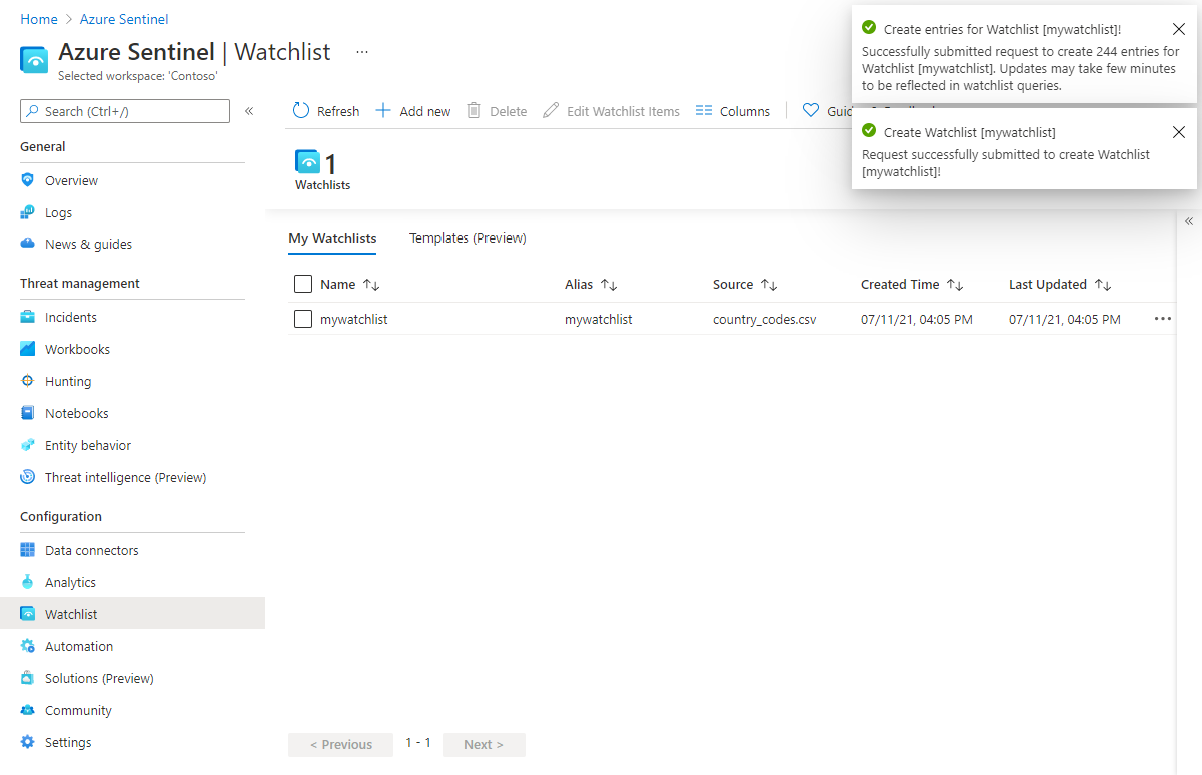


**Note**: File uploads are currently limited to files of up to 3.8 MB in size.

Review the information, verify that it is correct, and then select Create.

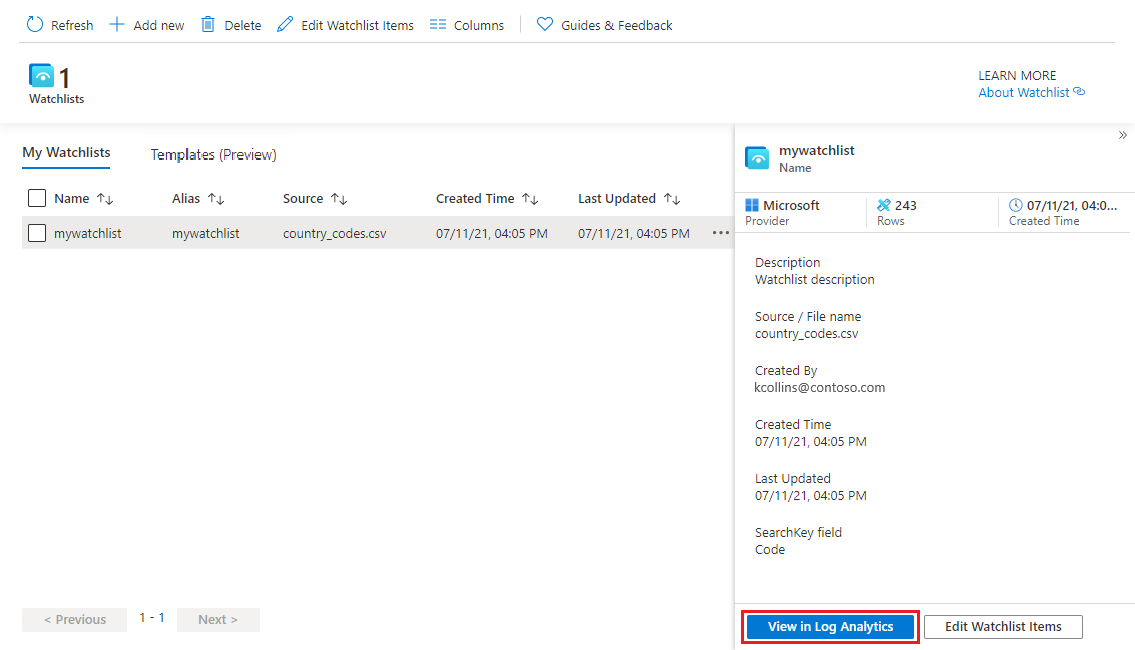


A notification appears once the watchlist is created.



**Use watchlists in queries**

From the Azure portal, navigate to Azure Sentinel > Configuration > Watchlist, select the watchlist you want to use, and then select View in Log Analytics.



The items in your watchlist are automatically extracted for your query, and will appear on the Results tab. The example below shows the results of the extraction of the ServerName and IpAddress fields.

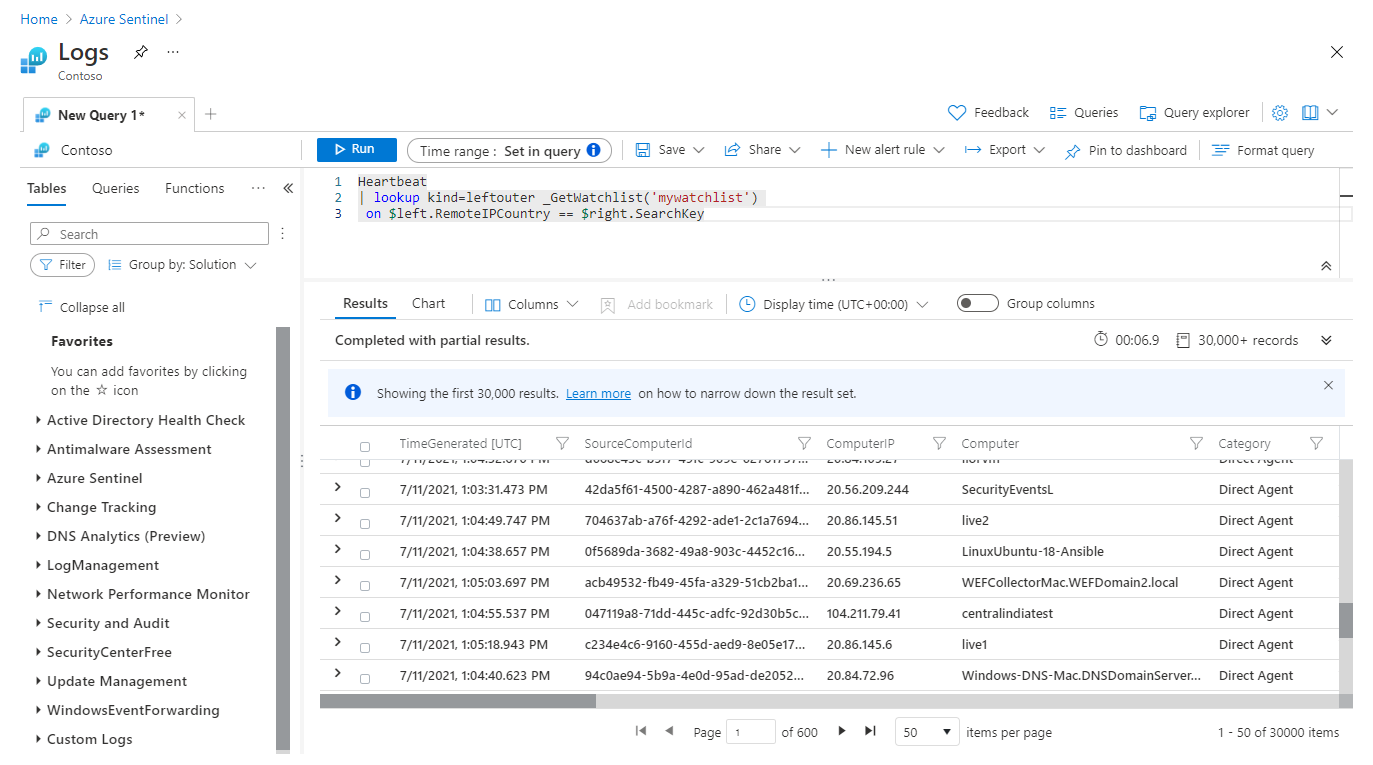
**Note:** The timestamp on your queries will be ignored in both the query UI and in scheduled alerts.



You can query data in any table against data from a watchlist by treating the watchlist as a table for joins and lookups.

Heartbeat

| lookup kind=leftouter \_GetWatchlist('IPlist') on $left.ComputerIP == $right.IPAddress

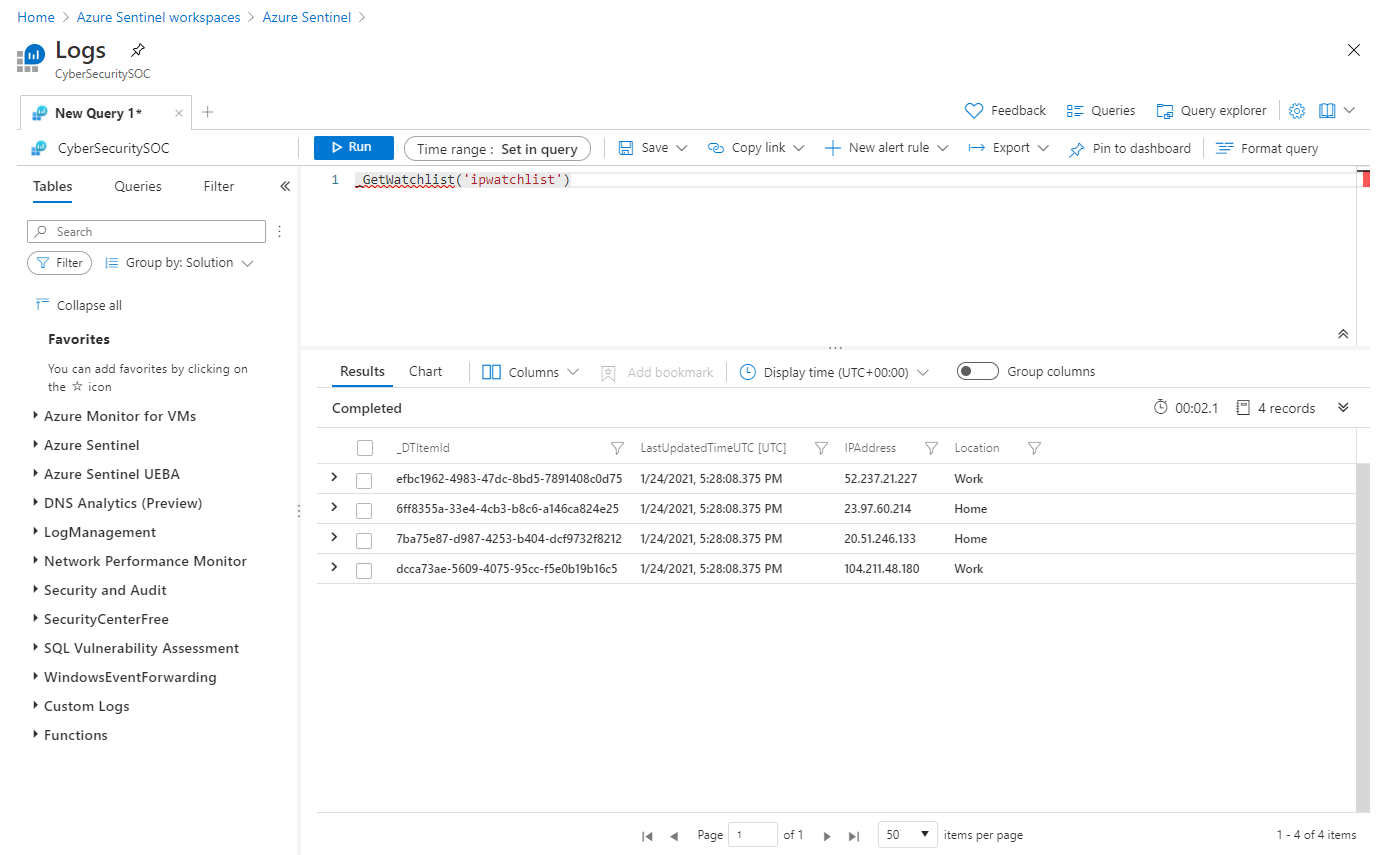


**Use watchlists in analytics rules**

To use watchlists in analytics rules, from the Azure portal, navigate to Azure Sentinel > Configuration > Analytics, and create a rule using the \_GetWatchlist('

In this example, create a watchlist called “ipwatchlist” with the following values:





Next, create the analytics rule. In this example, we only include events from IP addresses in the watchlist:

//Watchlist as a variable

let watchlist = (\_GetWatchlist('ipwatchlist') | project IPAddress);

Heartbeat

| where ComputerIP in (watchlist)

//Watchlist inline with the query

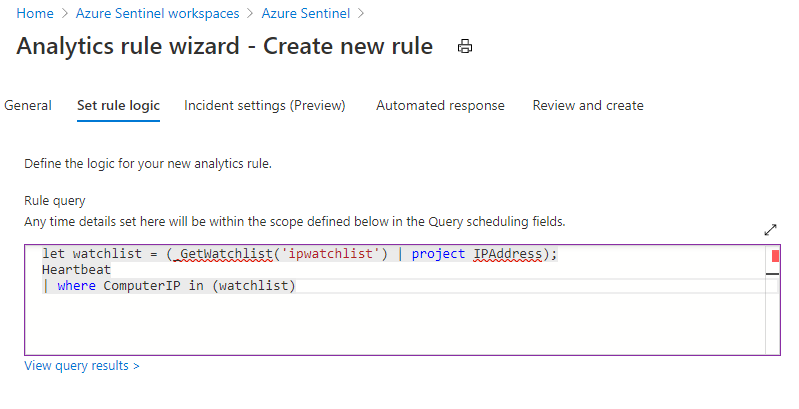
Heartbeat

| where ComputerIP in (

(\_GetWatchlist('ipwatchlist')

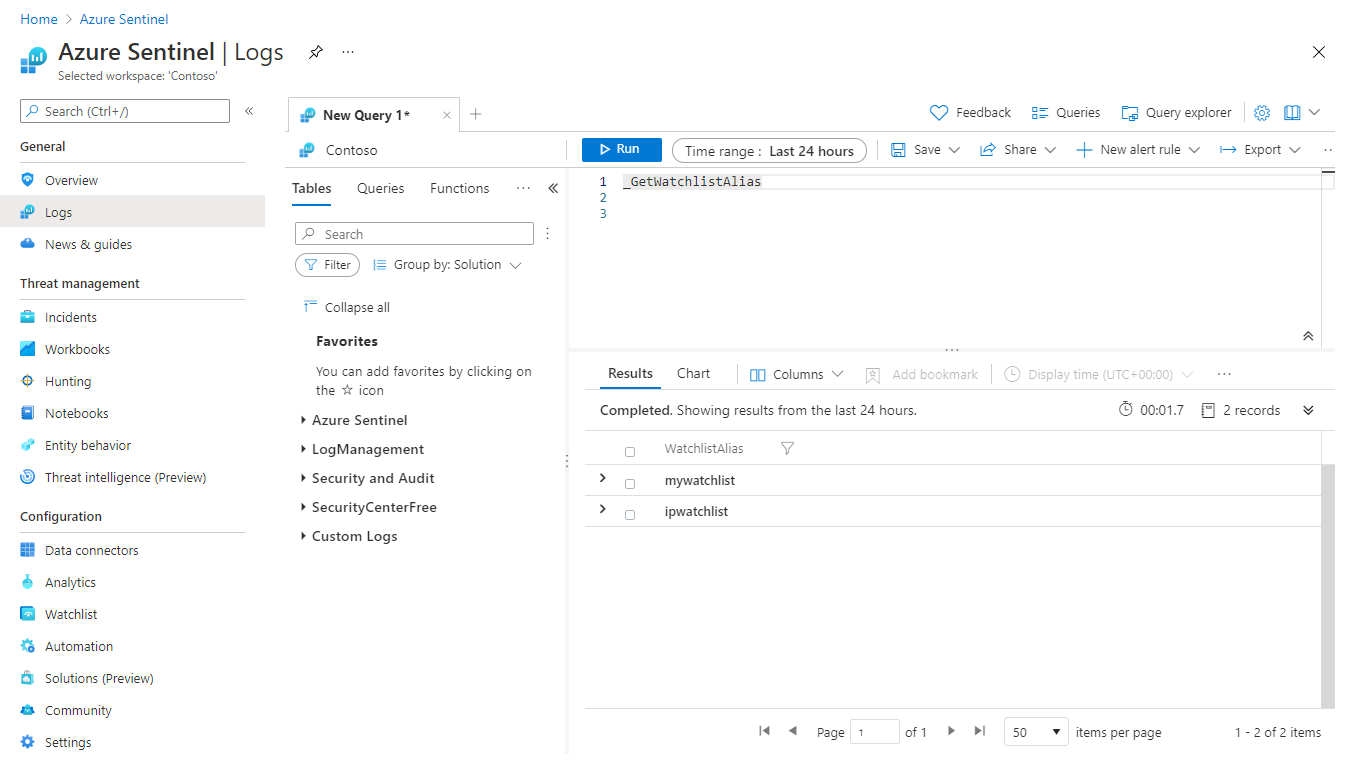
| project IPAddress)

)



**View list of watchlists aliases**

To get a list of watchlist aliases, from the Azure portal, navigate to Azure Sentinel > General > Logs, and run the following query: \_GetWatchlistAlias. You can see the list of aliases in the Results tab.



**Watchlist Added To Azure Sentinel**

| **Watchlists** |  |  |  |
| --- | --- | --- | --- |
| Date Added | Ticket # or Incident ID | Status | Ips/Domains Blocked |

**Process Owner**

SOC Manager

## Daily Operations Process

**Purpose**

This process is intended to guide the daily operations for the [CUSTOMER] Security Operations Center (SOC). This process provides a significant number of critical subordinate operational procedures that document the standard daily tasks that support effective SOC operations.

**Scope**

This process applies to the [CUSTOMER] SOC and covers its main operational activities across all shifts and situations.

**Process Summary**

All SOC personnel are responsible to manage the daily tasks of Security Operations. This process is the primary daily guide that establishes the operational tempo and individual daily procedures for the smooth operation of the SOC. All of the operational activities that must be accomplished within a given 8-hour period are spelled out in this process or its subordinate procedures. This includes; staffing, monitoring, problem & change, shift turn-over and the daily operations meeting. These are all rigorous procedures that drive the daily work effort for all SOC Analysts during their scheduled shifts.

**Shift Staffing and Scheduling Procedure**

The **Shift Staffing and Scheduling Procedures** ensures appropriate staffing and establishes standard shift schedules. This procedure will document and establish the shift schedules that are required to provide 8x5 operational monitoring. This procedure will also provide a process to cover planned and unplanned absences.

**Problem & Change Procedure**

The **Problem Ticket & Change Controls Procedures** document how the non-emergent processes associated with SOC operations are handled. This procedure will leverage the standard Customer IT problem and change process. This procedure will document how to manage daily operational problems or changes in:

* Monitored security devices
* Low priority alerts
* Any related Security Operations technology

**Shift Turnover Procedure**

The **Shift Turnover Procedures** provides a comprehensive and standard shift turn-over briefing to the replacement shift. The effective flow of operational and analytical information is critical to making informed security decisions. This procedure will ensure appropriate information exchange occurs during shift change.

**Daily Ops Call Procedure**

The **Daily Operations Meeting Procedures** will document all aspects of the daily operations call or meeting for the [CUSTOMER] security operations situational awareness. This is the daily operations call that informs a wider audience of important operational and analytical security information.

**Metrics**

* Incidents per Analyst Hour - Overall KPIs
* Incidents triaged by category by analyst - Personnel KPIs
* Service Center Tickets - Overall KPIs

**Roles & Responsibilities**

* SOC Manager owns the successful completion of all daily operational processes and procedures. The SOC manager is also responsible for ensuring these daily operational processes effectively support the SOC operations and for the continuous improvement of them.
* SOC Operations Lead owns the successful completion of all procedures executed during his/her presence in the SOC. The SOC Operations lead owns the documentation and measurement of all subordinate procedures as well as the continual improvements to them.
* SOC Analyst executes daily operational procedures as a matter of daily responsibility. The role of a SOC Analyst is the detailed and repeatable execution of all operational tasks as documented in this process and its subordinate procedures.

**Process Owner**

SOC Manager

## Daily Ops Meeting

**Description**

This is the daily operations call / meeting for the SOC, this call is intended to disseminate to a wider audience operational, analytical and infrastructure information pertaining to SOC operations.

Steps

* All parties join standard daily operations call conference bridge
* Parties on call:

1. SOC Analysts & Senior SOC Analysts
2. IR Team representative
3. Others as needed

* All parties to the call are logged in the shift-log
* Cover Daily Ops Call Agenda
* Optional

1. SOC Manager
2. SOC Leadership team

Agenda

* Operational

1. Callouts
2. Significant activity
3. Upcoming operational events

* Analytical

1. Daily analysis (current significant Incidents/Alerts/events)
2. Emerging attacks or threats
3. General Internet trends

* Open Discussion

1. Issues/concerns
2. Any other related items

**Process Owner**

SOC Manager

## Problem Tickets and Change Controls

**Initiating a Trouble Ticket**

There are 2 categories for trouble ticket creation.

* [CUSTOMER] - Used when the issue will be resolved by [CUSTOMER]'s Teams
* Azure Sentinel - Used when the issue needs to be resolved by Microsoft Customer Support

**Initiating a Change Control**

* Specify the customer's change control process here. (i.e. Remedy)

**Process Owner**

SOC Manager

## Shift Staffing Schedule

**Description**

The [CUSTOMER] Security Operations Center (SOC) is currently running a 9x5 operation to maintain adequate monitoring of potentially adverse information security events. In the future, [CUSTOMER] may elect to run 24x7x365 operations if the current coverage does not suffice. This procedure will define how both SOC shift schedules will be staffed.

**Shift Scheduling**

Temporary Staffing Model

This staffing model is centered around the 8 hr. (extended) business working hours. This schedule is used under special circumstances such as training or holiday rotation. Each work week consists of four (4) SOC Analysts and four (4) Senior SOC Analysts

* SOC Analysts will monitor for 2 or 4 hours at a time and alternate from actively monitoring the SOC Triage Tagged Incidents and performing other SOC Analyst duties.
* Each analyst will be responsible for a total of 4 or 6 hours of active monitoring per day.
* One analyst will be the Primary Analyst on console, and another analyst will be Secondary Analyst on console.
* Analysts will rotate console duties throughout the duration of each shift.

**Planned Absence**

* When requesting vacation, submit your request via E-Mail to the SOC Operations Lead
* A Senior SOC Analyst will cover for any planned vacations or other planned absences within their shift team if needed
* Vacations will be coordinated as far in advance as possible to ensure for appropriate shift coverage

1. All vacations should be scheduled a minimum of 2 weeks in advance

**Unplanned Absence**

1. Contact a SOC Analyst

* Call or page Manager or Director (SOC Contacts)
* Senior SOC Analyst to provide or arrange coverage

1. Contact SOC Manager/Operations Lead

**Process Owner**

SOC Manager

## Shift Turnover

**Description**

The Shift Turn-over procedure defines what needs to be done to allow for accurate and appropriate pass-on of shift information from one shift to the next.

**Steps**

See the Shift Logs for activity during outgoing shifts.

**Information to cover:**

1. All callouts and any new Incidents that may have been created
2. Review open tickets assigned to the SOC
3. Any new Alerts/events of interest that did not warrant a new Incident
4. Significant operational activity and analytical information

**Review all tracking pages:**

1. Action Item Log
2. Filter Request Log

**New shift should immediately complete:**

1. Review Intelligence Reports
2. Review all e-mail from other SOC Analysts and SOC Management
3. Review nightly update e-mail

**Sign previous shift log** to acknowledge that you have completed

**Process Owner**

SOC Manager

## Weekly Operational Process

**Description**

This process is intended to guide the weekly operations for the [CUSTOMER] Security Operations Center (SOC). This process provides a significant number of critical subordinate operational procedures that document the standard weekly tasks that support effective SOC operations.

**Scope**

This process applies to the SOC and covers its main operational activities across all shifts and situations.

**Process Summary**

The Senior SOC Analyst and any additional appointed personnel are responsible to manage the weekly SOC tasks. All of the operational activities that must be accomplished within a given weekly time frame are spelled out in this process or its subordinate procedures. This includes; Weekly Intelligence Report, Weekend Event Analysis and Review, Weekly Threat Report, Weekly SLA Attainment, and Weekly Incident Statistics.

**Weekly Threat Intelligence Report Procedure**

The Weekly Threat Intelligence Report provides the SOC and its ancillary teams with weekly up-to-date situational awareness concerning items related to the company as well as items on a regional/global scale.

**Process Owner**

SOC Manager

## Weekly Threat Intelligence Report

**Example**

**Sample Security Threat Intel Report**

[CUSTOMER] Confidential – Internal use only

**Statistics and Issues**

* Azure AD outage occurred on 03/15/2021 due to the number of SQL reads.
* 220 Azure Sentinel Incidents were opened and 74 Incidents were closed this week.
* A large spike in port 3389/TCP traffic was observed on 04/12/2021.

**Key Articles of Interest**

**In Wake of Resurgence, US-CERT Issues Alert About Dridex**

US-CERT issued a technical alert about the Dridex banking Trojan today, about two weeks after the malware was found being used in a large phishing campaign heavily targeted at users in the United Kingdom. Palo Alto Networks reported they saw this campaign after witnessing a brief decrease in Dridex activity in September, following the arrest of a Moldovan man purported to be a key player in a cybercrime gang that used Dridex.

**FBI, Security Vendors Partner for DRIDEX Takedown**

Multiple command-and-control (C&C) servers used by the DRIDEX botnet have been taken down by the Federal Bureau of Investigation (FBI), following the action taken by the National Crime Agency (NCA) in the UK.

**Samsung's mobile payments acquisition LoopPay breached by hackers**

A report on Wednesday revealed that LoopPay, the U.S.-created mobile payment system acquired by Samsung in February, was the target of a hacker attack in March. But the most interesting wrinkle in the story is the fact that the hackers who executed the attack on the South Korea-based company appear to be from China, thus framing the incident as a case of international, possibly corporate, espionage, rather than just another hack.

**Microsoft Patch Tuesday for October 2015**

October's Patch Tuesday is upon us and with only six bulletins, it's one of lightest releases we've seen. The six bulletins are split down the center with three rated as Critical and three rated as Important. This release addresses a total of 30 CVEs half of which are patched in Internet Explorer. The other two Critical bulletins patch remote code execution vulnerabilities in the Microsoft VBScript and Jscript scripting engines as well as the Microsoft Windows Shell. The Windows Shell bulletin patches a use-after-free vulnerability that is triggered by having a victim open a maliciously crafted windows toolbar object. The remote code execution would occur in the user context of the victim's user account.

**Android ransomware uses Google's own design principles against victims**

The Android.Lockdroid.E ransomware uses Google's design principles and an open-source project against users, warned Symantec security researcher Dinesh Venkatesan in a blog post.The malware developers used Google's Material Design language and open-source project MaterialDrawer to create a lockscreen with a more professional-looking user interface. The malware also uses Material Design to display personal data it gathers from device logs, making the fraudulent legal notice more convincing.

## Reporting Process

**Purpose**

The purpose of this process is to establish the standard reporting methodologies and to ensure that critical analytical security information is included, tracked, and effectively reported on.

**Scope**

This process applies to the Incidents/Alerts/events that are generated in Azure Sentinel, including all annotation tags and actions generated by the SOC in its monitoring and alerting function.

**Process Summary**

Business requirements owners will define informational requirements. The Lead SIEM Engineer will design, update, and maintain all required reports (i.e. Workbooks) within Azure Sentinel. The SOC Analysts will provide analytical comments and summaries to SOC work products as needed. On a regular basis the SOC Team will use Azure Sentinel's Workbooks to produce reports and provide availability and access. These reports are central to answering business questions about personnel performance, security operations, threat statistics, vulnerability statistics and KQL query performance.

The **Periodic Reports Procedures** establishes the standard reports that will be run on a regular basis. These include daily, weekly, and monthly reports to produce actionable information relating to security operations, threat statistics, vulnerability statistics, and query performance. The complete documentation will be maintained in the Use Case procedure appendices. The lead engineer is responsible for all reporting. The periodic reporting procedure will document which reports will be run and how often.

**Metrics**

* All reports document and present metrics

**Roles & Responsibilities**

* **SOC Manager** owns the successful completion of all daily operational processes and procedures. The SOC manager is also responsible for ensuring these daily operational process effectively support SOC operations and for continually improving them.
* **SOC Analyst** execute daily operations procedures as a matter of daily responsibility and owns the successful completion of all procedures executed during his/her presence in the SOC. SOC Analysts own the documentation and measurement of all subordinate procedures as well as the continual improvements to them. The role of a SOC Analyst is the detailed and repeatable execution of all operational tasks as documented in this process and its subordinate procedures.
* **Lead SOC Engineer** is responsible for the successful completion of all reporting processes. This lead engineer is also responsible for developing the content to satisfy defined requirements which are documented in the Use Case procedures.

**Applicable Policies & Standards**

* Link to Policies and Standards

**Process Linkages**

* Subordinate Procedures

1. Periodic Reports

* Related Process & Procedures

1. Incident Management Process
2. Metrics Process

**Process Owner**

SOC Manager

## Periodic Reports

**Purpose**

Senior SOC Analysts will be responsible for producing daily and weekly reports and monthly metrics as detailed in the SOC Roles & Responsibilities. Senior SOC Analysts own the following reports and processes.

**SOC Weekly Threat Report**

This page details the sources and processes to create the Weekly Threat Report.

* SOC Weekly Threat Report Instructions
* SOC Weekly Threat Report Archive

**SOC Monthly Metrics**

This page details how to collect and produce monthly performance metrics

* Monthly Metrics

**Process Owner**

SOC Manager

# SOC Technology Processes & Procedures

| Process Name | Procedures | Description/Comments |
| --- | --- | --- |
| Design Process |  |  |
|  | Architecture | Holds all architecture design documents for all services |
|  | Data Retention | Describes the data retention requirements for all services |
|  | Network Diagrams | Customer network diagrams for line of business applications |
|  | Content Development Design | Procedure on how to develop content |
|  | Azure Infrastructure Monitoring | Azure Standards that are in place to monitor for Threats and Failure |
|  | Engineering Incident Management | Procedure for dealing with system problems |
|  | User Access Control Design | Details regarding how ACL will be setup for all components and users |

## Design Process

**Purpose**

The purpose of this process is to document the methodology by which the initial conceptual design of the content that the SOC will use within Azure Sentinel and the procedures for on-going changes to design components. The process will include procedures for Use Cases and Analytics Modeling as well as many other content design procedures.

**Scope**

The scope of this process includes the initial configuration and the approach to update key parameters that impact the effectiveness and efficiency of Azure Sentinel. The scope of this process is strictly limited to the [CUSTOMER] SOC. The Modeling Procedure will document the parameters relative to networks, servers, endpoints, applications, and category levels. The use case procedure will address business and analytical requirements as well as objectives, any compliance requirements, and other technology problems to be solved.

**Process Summary**

The Lead Engineer will provision and maintain the appropriate conceptual design content in Azure Sentinel. This process consists of two main subordinate procedures and many secondary procedures which are all concerned with the content and design structure of Azure Sentinel.

The Use Cases procedure is the key component for meeting compliance business requirements. This procedure will document the requirements gathering process, the steps required to analyze and implement monitoring analytics within Azure Sentinel and all the associated documentation required by the business. These requirements will fit a number of general categories; Regulatory (PCI, SOX, HIPAA, PII, FFIEC, etc), General Security, Policy Compliance, System Administration, Metrics, and Network.

Metrics

* Use cases defined, tracked & completed
* Interactive Workbook statistics defined, tracked & completed

1. Workbook Reports defined, tracked, & completed

**Roles & Responsibilities**

* SOC Manager is responsible for the overall success of this process. The SOC manager ensures the resources are available to support Azure Sentinel Analytic design and on-going modifications.
* Lead Engineer is responsible for interfacing with local organizations to obtain essential modeling data to set parameters in Azure Sentinel; and to develop use cases to support business requirements/objectives with efficient implementation.
* SOC Lead is responsible for providing SOC related requirements and objectives that will allow Azure Sentinel to effectively support the SOC.
* SOC Analyst is responsible for providing feedback on modeling and use case design effectiveness. The SOC Analyst is responsible for the 24x7x365 monitoring of solutioned Use Case content.
* Network Management is responsible for providing essential network topology and log data.
* Information Systems Management is responsible for requirements verification, prioritization and escalation.

More information on specific roles and responsibilities is available in Roles & Responsibilities.

**Process Owner**

SOC Manager

## Architecture

**Description**

Holds all architecture design documents for all services. Update this page with applicable Architecture Design Documents and Visio's.

## Data Retention Standard

**Description**

This will maintain all the data retention requirements for Azure Sentinel managed by the SOC. Please describe the retention requirement as well as any special business justification for each particular business unit and their associated data being stored within Azure Sentinel.

**CUSTOMER OR BUSINESS UNIT NAME**

Per Regulatory Compliance Requirements, Production data, and other data identified as required for compliance, is stored for a period of 1 year. Data remains "Hot" within Azure Sentinel for a period of 90 days in the Log Analytics Workspace assigned to Azure Sentinel.

**Governing Requirements for Data Retention**

Below are the Standards that are governed by.

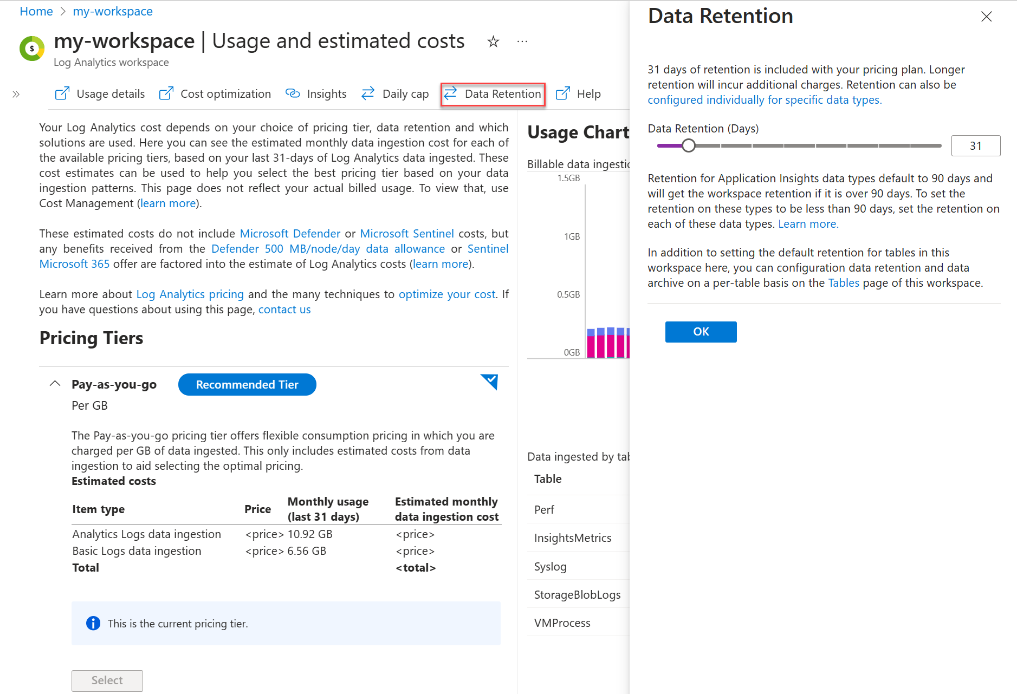
* PCI DSS-40
* Sarbanes-Oxley

**Data Retention**

The following steps describe how to configure how long log data is kept in your workspace. Data retention at the workspace level can be configured from 30 to 730 days (2 years) for all workspaces unless they are using the legacy Free pricing tier. Retention for individual data types can be set as low as 4 days. Learn more about pricing for longer data retention. To retain data longer than 730 days, consider using Log Analytics workspace data export @ <https://docs.microsoft.com/azure/azure-monitor/logs/logs-data-export>.

**Workspace level default retention**

1. In the Azure portal, from your workspace, select Usage and estimated costs from the left pane.
2. On the Usage and estimated costs page, click Data Retention from the top of the page.
3. On the pane, move the slider to increase or decrease the number of days and then click OK. If you are on the free tier, you will not be able to modify the data retention period and you need to upgrade to the paid tier in order to control this setting.



When the retention is lowered, there is a several day grace period before the data older than the new retention setting is removed. The Data Retention page allows retention settings of 30, 31, 60, 90, 120, 180, 270, 365, 550 and 730 days. If another setting is required, that can be configured using Azure Resource Manager using the retentionInDays parameter. When you set the data retention to 30 days, you can trigger an immediate purge of older data using the immediatePurgeDataOn30Days parameter (eliminating the several day grace period).

NOTE: This may be useful for compliance-related scenarios where immediate data removal is imperative. This immediate purge functionality is only exposed via Azure Resource Manager.

Workspaces with 30 days retention may actually retain data for 31 days. If it is imperative that data be kept for only 30 days, use the Azure Resource Manager to set the retention to 30 days and with the immediatePurgeDataOn30Days parameter.

NOTE: that the Log Analytics purge API does not affect retention billing and is intended to be used for very limited cases. To reduce your retention bill, the retention period must be reduced either for the workspace or for specific data types.

**Retention by data type**

It is also possible to specify different retention settings for individual data types from 4 to 730 days (except for workspaces in the legacy Free pricing tier) that override the workspace level default retention.

**Additional Resources that may be helpful**

<https://docs.microsoft.com/azure/azure-monitor/logs/manage-cost-storage#troubleshooting-why-usage-is-higher-than-expected><https://docs.microsoft.com/azure/azure-monitor/logs/manage-cost-storage#understanding-nodes-sending-data>

**Process Owner**

SOC Manager

## Network Diagrams

**Description**

This topic serves as the repository for all Network Diagrams obtained by the SOC. All new diagrams should be uploaded to this page under the appropriate category. Additionally, please update any diagrams that are out of date.

**CUSTOMER OR BUSINESS UNIT DIAGRAMS**

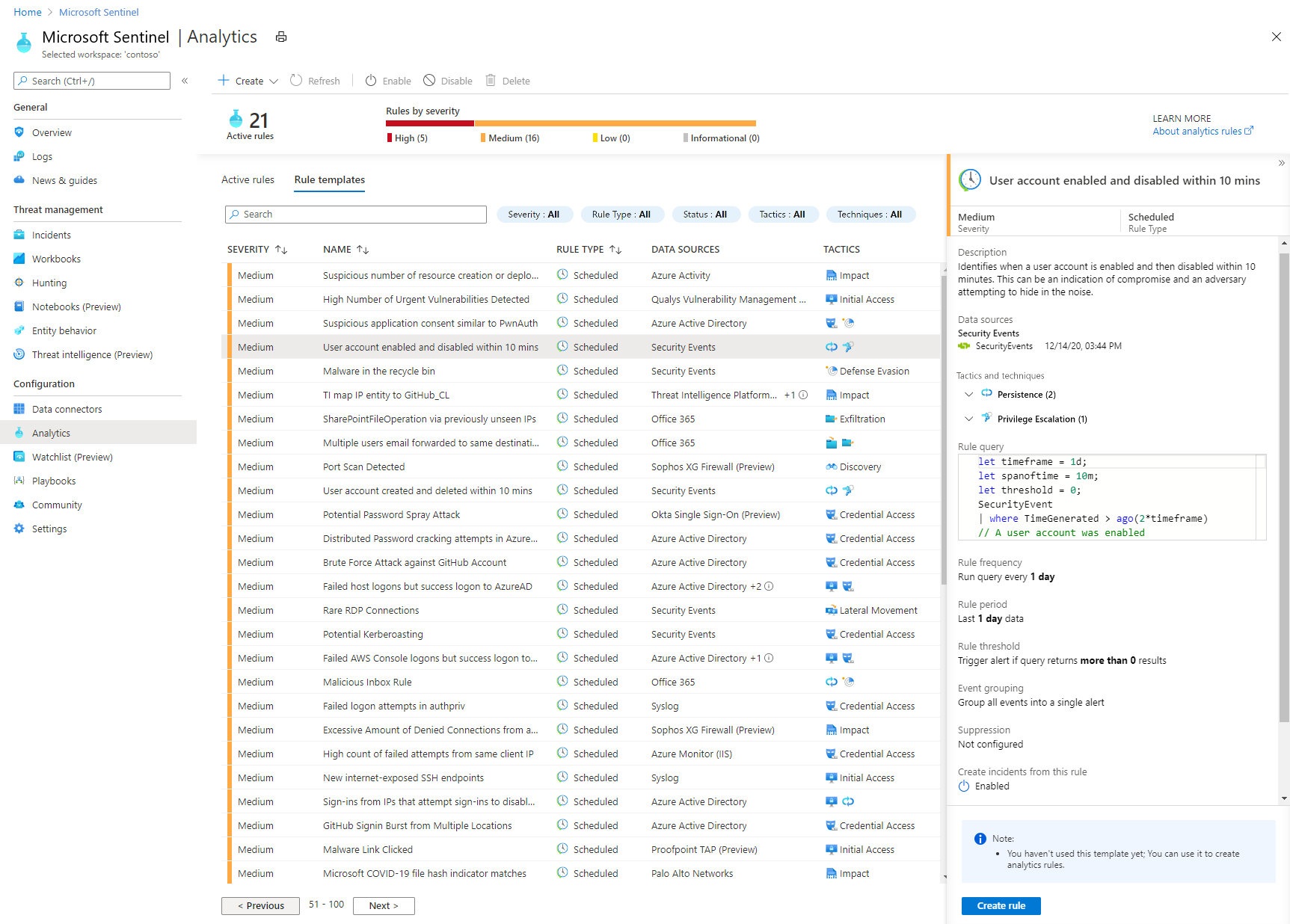
## Content Development Design

**Create analytic rules to detect threats**

The Analytic Rules you Create will search for specific events or sets of events across your environment, alert you when certain event thresholds or conditions are reached, generate incidents for your SOC to triage and investigate, and respond to threats with automated tracking and remediation processes.

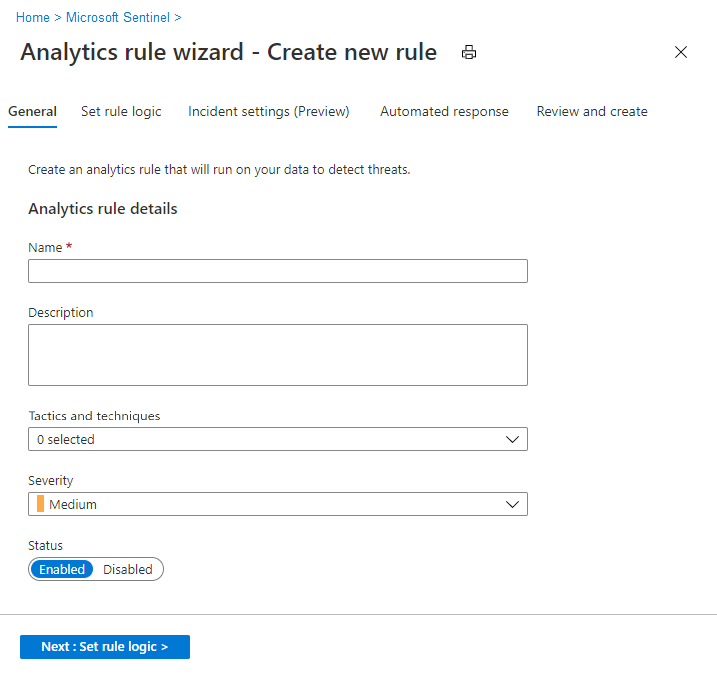
**Create an analytic rule with a scheduled query**

1. From the Azure Sentinel navigation menu, select Analytics.
2. In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.



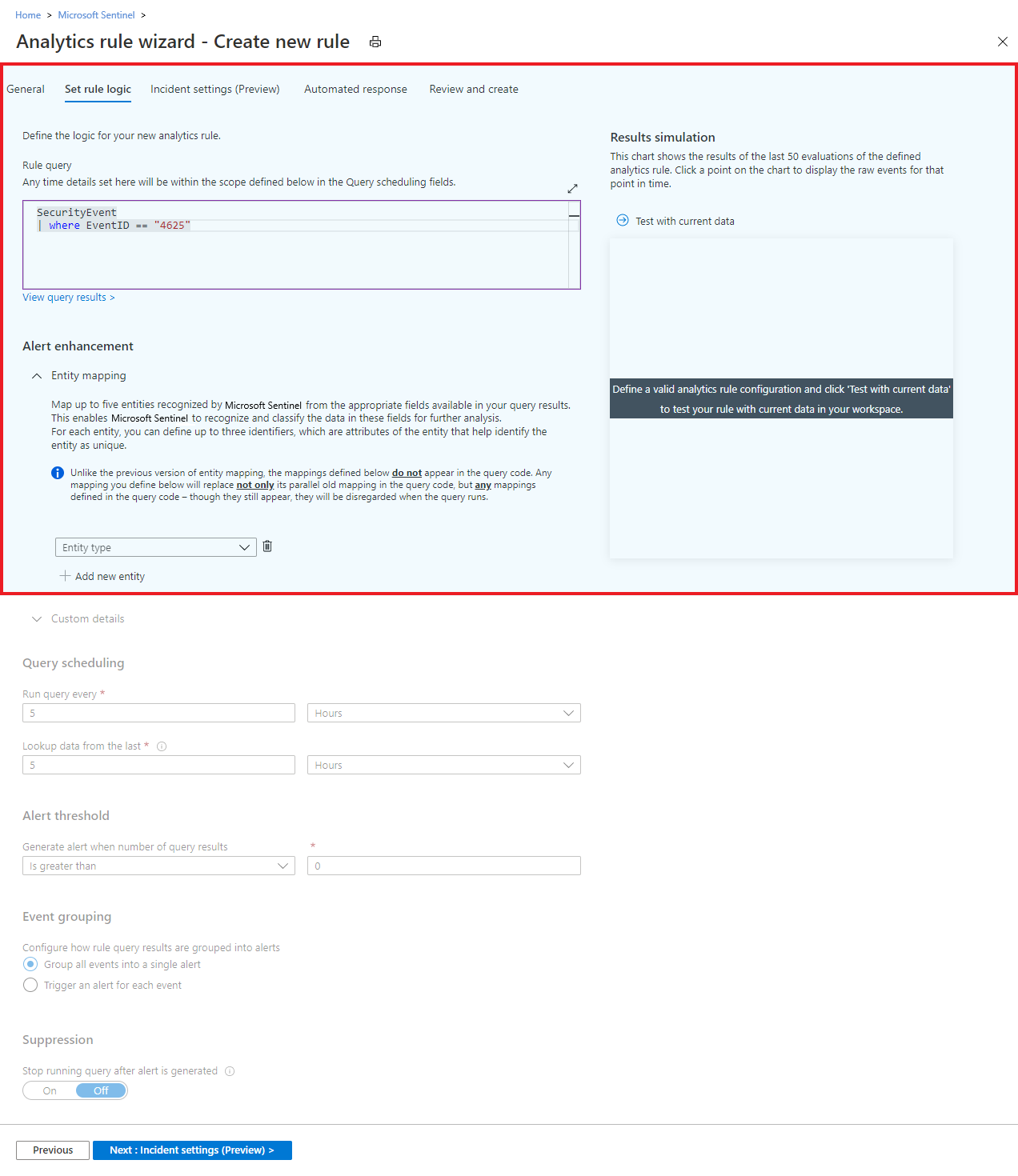
**Analytics rule wizard - General tab**

1. Provide a unique Name and a Description.
2. In the Tactics field, you can choose from among categories of attacks by which to classify the rule. These are based on the tactics of the MITRE ATT&CK framework.
3. Set the alert Severity as appropriate.
4. When you create the rule, its Status is Enabled by default, which means it will run immediately after you finish creating it. If you don’t want it to run immediately, select Disabled, and the rule will be added to your Active rules tab and you can enable it from there when you need it.



**Define the rule query logic and configure settings**

* In the Set rule logic tab, you can either write a query directly in the Rule query field, or create the query in Log Analytics and then copy and paste it here.
* Queries are written in Kusto Query Language (KQL). Learn more about KQL concepts and queries, and see this handy quick reference guide.
* The example shown in this screenshot queries the SecurityEvent table to display a type of failed Windows logon events.



* Here's another sample query, one that would alert you when an anomalous number of resources is created in Azure Activity. AzureActivity | where OperationName == "Create or Update Virtual Machine" or OperationName =="Create Deployment" | where ActivityStatus == "Succeeded" | make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller

**Rule query best practices**

* The query length should be between 1 and 10,000 characters and cannot contain "search " or “union ”.
* Using ADX functions to create Azure Data Explorer queries inside the Log Analytics query window is not supported.
* When using the bag\_unpack function in a query, if you project the columns as fields using "project field1" and the column doesn't exist, the query will fail. To guard against this happening, you must project the column as follows: project field1 = column\_ifexists("field1","")

**Alert enrichment**

* Use the Entity mapping configuration section to map parameters from your query results to Azure Sentinel-recognized entities. Entities enrich the rules' output (alerts and incidents) with essential information that serves as the building blocks of any investigative processes and remedial actions that follow. They are also the criteria by which you can group alerts together into incidents in the Incident settings tab.

Learn more about entities in Azure Sentinel.

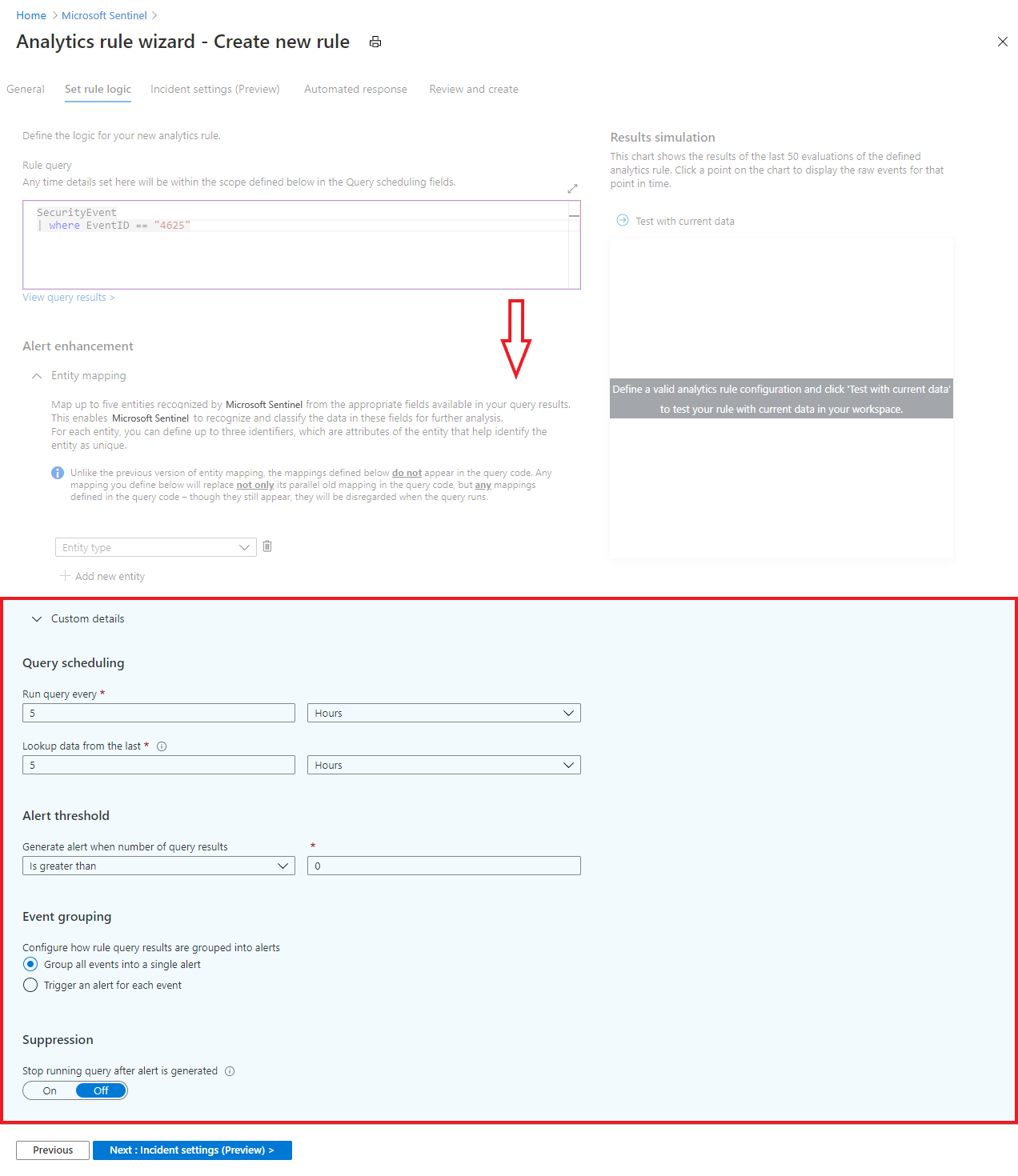
See Map data fields to entities in Azure Sentinel for complete entity mapping instructions, along with important information about backward compatibility.

* Use the Custom details configuration section to extract event data items from your query and surface them in the alerts produced by this rule, giving you immediate event content visibility in your alerts and incidents.

Learn more about surfacing custom details in alerts, and see the complete instructions.

**Query scheduling and alert threshold**

* In the Query scheduling section, set the following parameters:

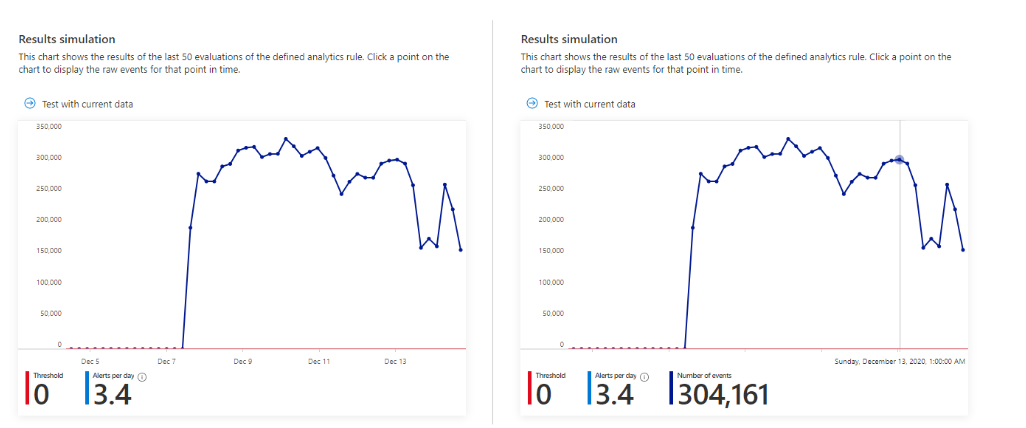


* Set Run query every to control how often the query is run - as frequently as every 5 minutes or as infrequently as once every 14 days.
* Set Lookup data from the last to determine the time period of the data covered by the query - for example, it can query the past 10 minutes of data, or the past 6 hours of data. The maximum is 14 days.
* Use the Alert threshold section to define the sensitivity level of the rule. For example, set Generate alert when number of query results to Is greater than and enter the number 1000 if you want the rule to generate an alert only if the query returns more than 1000 results each time it runs. This is a required field, so if you don’t want to set a threshold – that is, if you want your alert to register every event – enter 0 in the number field.

**Results simulation**

In the Results simulation area, on the right side of the wizard, select Test with current data and Azure Sentinel will show you a graph of the results (log events) the query would have generated over the last 50 times it would have run, according to the currently defined schedule. If you modify the query, select Test with current data again to update the graph. The graph shows the number of results over the defined time period, which is determined by the settings in the Query scheduling section.

Here's what the results simulation might look like for the query in the screenshot above. The left side is the default view, and the right side is what you see when you hover over a point in time on the graph.



If you see that your query would trigger too many or too frequent alerts, you can experiment with the settings in the Query scheduling and Alert threshold sections and select Test with current data again.

**Event grouping and rule suppression**

* Under Event grouping, choose one of two ways to handle the grouping of events into alerts:

1. Group all events into a single alert (the default setting). The rule generates a single alert every time it runs, as long as the query returns more results than the specified alert threshold above. The alert includes a summary of all the events returned in the results.
2. Trigger an alert for each event. The rule generates a unique alert for each event returned by the query. This is useful if you want events to be displayed individually, or if you want to group them by certain parameters - by user, hostname, or something else. You can define these parameters in the query.
3. Currently the number of alerts a rule can generate is capped at 20. If in a particular rule, Event grouping is set to Trigger an alert for each event, and the rule's query returns more than 20 events, each of the first 19 events will generate a unique alert, and the 20th alert will summarize the entire set of returned events. In other words, the 20th alert is what would have been generated under the Group all events into a single alert option.

**What's the difference between events and alerts?**

An event is a description of a single occurrence of an action. For example, a single entry in a log file could count as an event. In this context an event refers to a single result returned by a query in an analytics rule.

An alert is a collection of events that, taken together, are significant from a security standpoint. An alert could contain a single event if the event had significant security implications - an administrative login from a foreign country outside of office hours, for example.

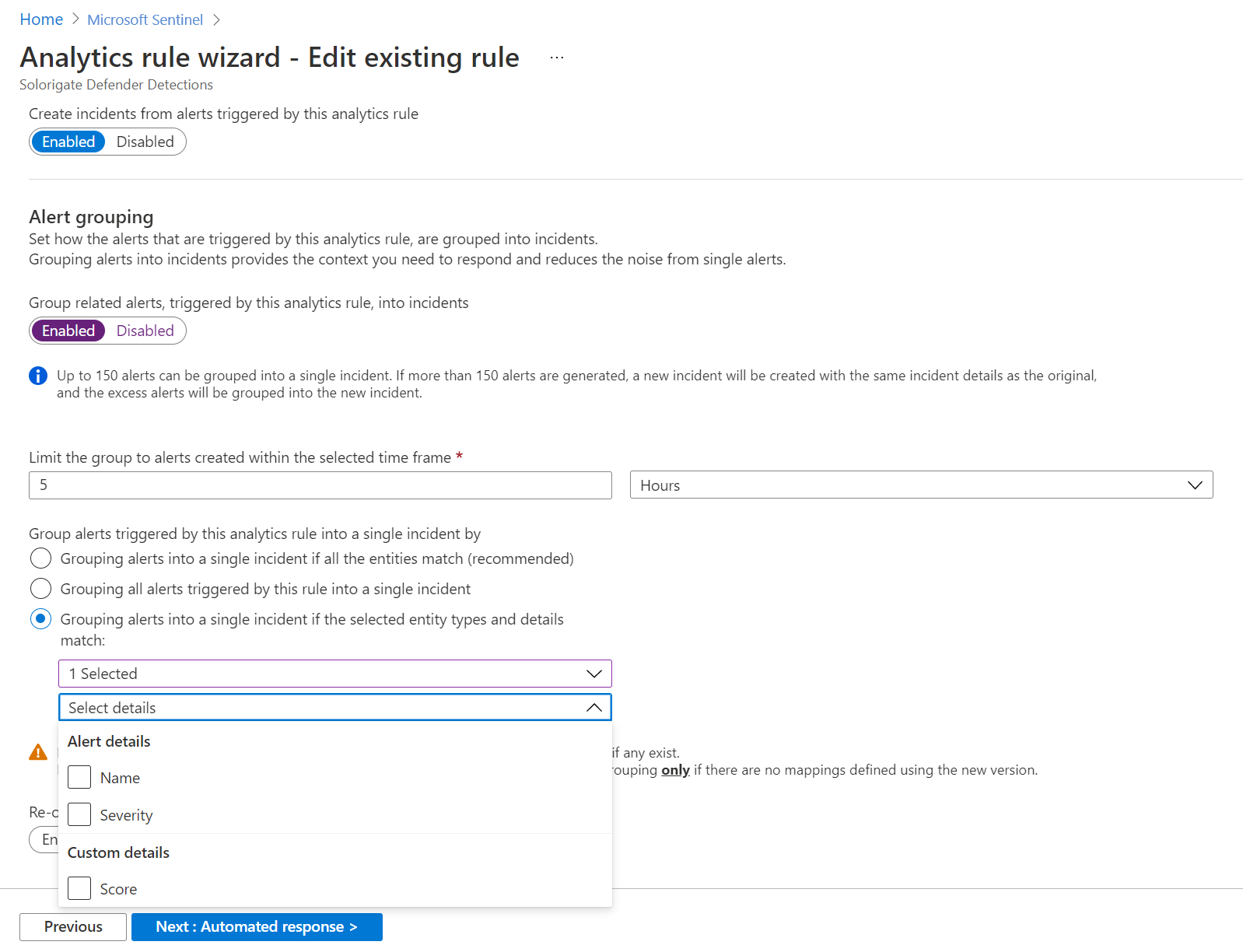
By the way, what are the incidents? Azure Sentinel's internal logic creates incidents from alerts or groups of alerts. The incidents queue is the focal point of SOC analysts' work - triage, investigation and remediation.

Azure Sentinel ingests raw events from some data sources, and already-processed alerts from others. It is important to note which one you're dealing with at any time.

* In the Suppression section, you can turn the Stop running query after alert is generated setting On if, once you get an alert, you want to suspend the operation of this rule for a period of time exceeding the query interval. If you turn this on, you must set Stop running query for to the amount of time the query should stop running, up to 24 hours.

**Configure the incident creation settings**

In the Incident Settings tab, you can choose whether and how Azure Sentinel turns alerts into actionable incidents. If this tab is left alone, Azure Sentinel will create a single, separate incident from each and every alert. You can choose to have no incidents created, or to group several alerts into a single incident, by changing the settings in this tab.



**Incident settings**

In the Incident settings section, Create incidents from alerts triggered by this analytics rule is set by default to Enabled, meaning that Azure Sentinel will create a single, separate incident from each and every alert triggered by the rule.

If you don’t want this rule to result in the creation of any incidents (for example, if this rule is just to collect information for subsequent analysis), set this to Disabled.

If you want a single incident to be created from a group of alerts, instead of one for every single alert, see the next section.

**Alert grouping**

In the Alert grouping section, if you want a single incident to be generated from a group of up to 150 similar or recurring alerts (see note), set Group related alerts, triggered by this analytics rule, into incidents to Enabled, and set the following parameters.

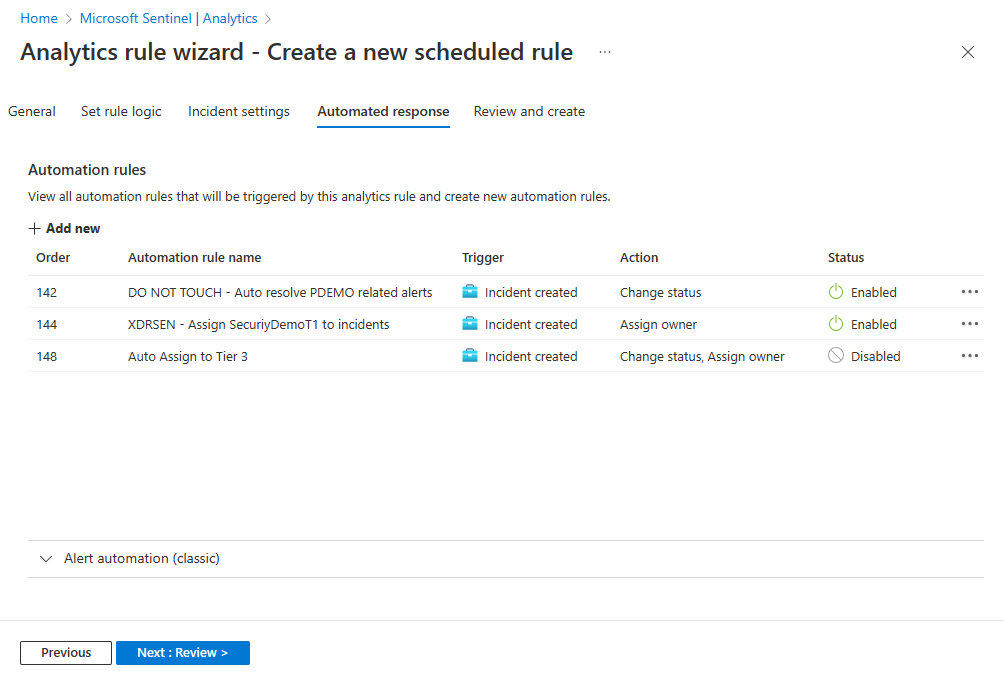
* Limit the group to alerts created within the selected time frame: Determine the time frame within which the similar or recurring alerts will be grouped together. All of the corresponding alerts within this time frame will collectively generate an incident or a set of incidents (depending on the grouping settings below). Alerts outside this time frame will generate a separate incident or set of incidents.
* Group alerts triggered by this analytics rule into a single incident by: Choose the basis on which alerts will be grouped together:

1. Group alerts into a single incident if all the entities match: Alerts are grouped together if they share identical values for each of the mapped entities (defined in the Set rule logic tab above). This is the recommended setting.
2. Group all alerts triggered by this rule into a single incident: All the alerts generated by this rule are grouped together even if they share no identical values.
3. Group alerts into a single incident if the selected entities match: Alerts are grouped together if they share identical values for some of the mapped entities (that you can select from the drop-down list). You might want to use this setting if, for example, you want to create separate incidents based on the source or target IP addresses.

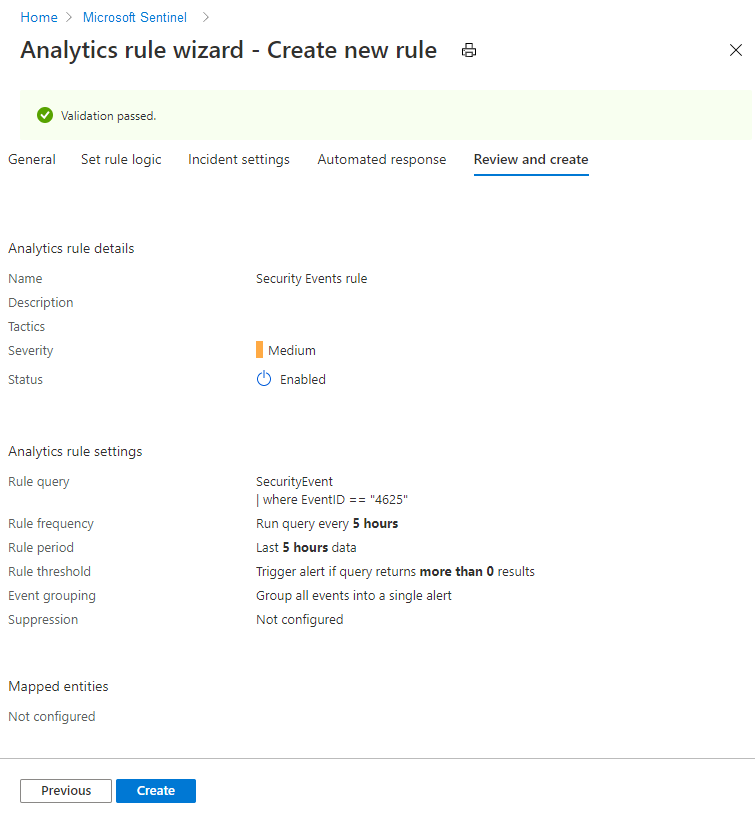
* Re-open closed matching incidents: If an incident has been resolved and closed, and later on another alert is generated that should belong to that incident, set this setting to Enabled if you want the closed incident re-opened, and leave as Disabled if you want the alert to create a new incident.

**Set automated responses and create the rule**

In the Automated responses tab, select any playbooks you want to run automatically when an alert is generated by the custom rule. For more information on creating and automating playbooks, see Respond to threats.



1. Select Review and create to review all the settings for your new alert rule. When the "Validation passed" message appears, select Create to initialize your alert rule.



**View the rule and its output**

* You can find your newly created custom rule (of type "Scheduled") in the table under the Active rules tab on the main Analytics screen. From this list you can enable, disable, or delete each rule.
* To view the results of the alert rules you create, go to the Incidents page, where you can triage, investigate incidents, and remediate the threats.

**Troubleshooting**

See the following Link: <https://docs.microsoft.com/azure/sentinel/tutorial-detect-threats-custom#troubleshooting>

NOTE: SOC managers should be sure to check the rule list regularly for the presence of auto-disabled rules.

**Process Owner**

SOC Manager

## Azure Infrastructure Monitoring

**Configuration and change management**

Azure reviews and updates configuration settings and baseline configurations of hardware, software, and network devices annually. Changes are developed, tested, and approved prior to entering the production environment from a development and/or test environment.

The baseline configurations that are required for Azure-based services are reviewed by the Azure security and compliance team and by service teams. A service team review is part of the testing that occurs before the deployment of their production service.

**Vulnerability management**

Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure is also able to draw on the resources of the Microsoft Security Response Center (MSRC). The MSRC identifies, monitors, responds to, and resolves security incidents and cloud vulnerabilities around the clock, every day of the year.

**Vulnerability scanning**

Vulnerability scanning is performed on server operating systems, databases, and network devices. The vulnerability scans are performed on a quarterly basis at minimum. Azure contracts with independent assessors to perform penetration testing of the Azure boundary. Red-team exercises are also routinely performed and the results are used to make security improvements.

**Protective monitoring**

Azure security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include the Microsoft Monitoring Agent (MMA) and System Center Operations Manager. These tools are configured to provide time alerts to Azure security personnel in situations that require immediate action.

**Incident management**

Microsoft implements a security incident management process to facilitate a coordinated response to incidents, should one occur.

If Microsoft becomes aware of unauthorized access to [CUSTOMER]'s data that's stored on its equipment or in its facilities, or it becomes aware of unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of customer data, Microsoft takes the following actions:

* Promptly notifies the customer of the security incident.
* Promptly investigates the security incident and provides customers detailed information about the security incident.
* Take reasonable and prompt steps to mitigate the effects and minimize any damage resulting from the security incident.

An incident management framework has been established that defines roles and allocates responsibilities. The Azure security incident management team is responsible for managing security incidents, including escalation, and ensuring the involvement of specialist teams when necessary. Azure operations managers are responsible for overseeing the investigation and resolution of security and privacy incidents.

**Process Owner**

Microsoft

## Engineering Incident Management

**Description**

This page describes how to escalate system issues to the engineering team. It will also cover how the engineering team will manage their Incidents and workload.

**Workflow**

At a high level, the engineering incident management process works like this:

1. An Incident is opened in Azure Sentinel and the SOC Analyst tags the Incident with SOC-Engineering to assign the Incident to the SOC Engineering team.
2. The engineers review the Incidents, assign an owner and prioritize
3. The owner works through the issues until resolution
4. Incident is closed

**Detailed Steps**

**Opening an Incident**

1. Within the Azure Sentinel, navigate to the Incidents Blade and search for tagged Incidents with "SOC-Engineering". These should be Incidents that require a SOC Engineer to look into for refinement.
2. In the Comments, provide as much description as possible
3. Validate the specific events that show the problem through a KQL query and attach the events to the incident by using a Bookmark.
4. Notify the SOC Engineering team via Teams, Email or some other method.

**Incident Review**

1. An Engineer will review each Incident to see if it is valid, if not the SOC Analyst who submitted the Incident to the SOC Engineering team will be notified with a detailed explanation.
2. If the Incident is valid, an owner from the SOC Engineering team is assigned and the Incident is prioritized.

**Resolution**

1. The Incident owner is responsible for providing updates as they become available. At a minimum, the Incident should be updated weekly unless the SOC Engineer assigned updates the tag to Stage = 'On Hold'.

**Incident Closure**

1. When the problem is resolved, the Incident can be closed. This is done by assigning a tag - Stage = Closed and changes the Status of the Incident to Closed along with setting the Classification to one of the following depending on the Engineering Reason:

* False Positive - incorrect alert logic
* False Positive - incorrect data

1. If required, this Workbook should be updated. ie: flows, connector tracking, installation instructions, etc...
2. If appropriate, the SOC should be notified with any changes and instructions.

**Process owner**

SOC Manager

## User Access Control Design

**Permissions in Azure Sentinel**

Azure Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.

Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Azure Sentinel. The different roles give you fine-grained control over what users of Azure Sentinel can see and do. Azure roles can be assigned in the Azure Sentinel workspace directly (see note below), or in a subscription or resource group that the workspace belongs to, which Azure Sentinel will inherit.

**Roles for working in Azure Sentinel**

**Azure Sentinel-specific roles** All Azure Sentinel built-in roles grant read access to the data in your Azure Sentinel workspace.

* Azure Sentinel Reader can view data, incidents, workbooks, and other Azure Sentinel resources.
* Azure Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.)
* Azure Sentinel Contributor can, in addition to the above, create and edit workbooks, analytics rules, and other Azure Sentinel resources.
* Azure Sentinel Automation Contributor allows Azure Sentinel to add playbooks to automation rules. It is not meant for user accounts.

NOTE: For best results, these roles should be assigned on the resource group that contains the Azure Sentinel workspace. This way, the roles will apply to all the resources that are deployed to support Azure Sentinel, as those resources should also be placed in that same resource group. Another option is to assign the roles directly on the Azure Sentinel workspace itself. If you do this, you must also assign the same roles on the SecurityInsights solution resource in that workspace. You may need to assign them on other resources as well, and you will need to be constantly managing role assignments on resources.

**Additional roles and permissions to consider**

Users with particular job requirements may need to be assigned additional roles or specific permissions in order to accomplish their tasks.

* **Working with playbooks to automate responses to threats** Azure Sentinel uses playbooks for automated threat response. Playbooks are built on Azure Logic Apps, and are a separate Azure resource. You might want to assign to specific members of your security operations team the ability to use Logic Apps for Security Orchestration, Automation, and Response (SOAR) operations. You can use the Logic App Contributor role to assign explicit permission for using playbooks.
* **Connecting data sources to Azure Sentinel** For a user to add data connectors, you must assign the user write permissions on the Azure Sentinel workspace. Also, note the required additional permissions for each connector, as listed on the relevant connector page.
* **Guest users assigning incidents** If a guest user needs to be able to assign incidents, then in addition to the Azure Sentinel Responder role, the user will also need to be assigned the role of Directory Reader. Note that this role is not an Azure role but an Azure Active Directory role, and that regular (non-guest) users have this role assigned by default.
* **Creating and deleting workbooks** For a user to create and delete an Azure Sentinel workbook, the user will also need to be assigned with the Azure Monitor role of Monitoring Contributor. This role is not necessary for using workbooks, but only for creating and deleting.

**Other roles you might see assigned**

In assigning Azure Sentinel-specific Azure roles, you may come across other Azure and Log Analytics Azure roles that may have been assigned to users for other purposes. You should be aware that these roles grant a wider set of permissions that includes access to your Azure Sentinel workspace and other resources:

Azure roles: Owner, Contributor, and Reader. Azure roles grant access across all your Azure resources, including Log Analytics workspaces and Azure Sentinel resources.

Log Analytics roles: Log Analytics Contributor and Log Analytics Reader. Log Analytics roles grant access to your Log Analytics workspaces.

For example, a user who is assigned the Azure Sentinel Reader role, but not the Azure Sentinel Contributor role, will still be able to edit items in Azure Sentinel if assigned the Azure-level Contributor role. Therefore, if you want to grant permissions to a user only in Azure Sentinel, you should carefully remove this user’s prior permissions, making sure you do not break any needed access to another resource.

**Azure Sentinel roles and allowed actions**

The following table summarizes the Azure Sentinel roles and their allowed actions in Azure Sentinel.

| Role | Create and run playbooks | Create and edit analytic rules and other Azure Sentinel resources \* | Manage incidents (dismiss, assign, etc.) | View data, incidents, workbooks, and other Azure Sentinel resources |
| --- | --- | --- | --- | --- |
| Azure Sentinel Reader |  | - |  | ✔️ |
| Azure Sentinel Responder |  | - | ✔️ | ✔️ |
| Azure Sentinel Contributor |  | ✔️ | ✔️ | ✔️ |
| Azure Sentinel Contributor + Logic App Contributor | ✔️ | ✔️ | ✔️ | ✔️ |

* Creating and deleting workbooks requires the additional Monitoring Contributor role. For more information, see Additional roles and permissions @ <https://docs.microsoft.com/azure/sentinel/roles#additional-roles-and-permissions>

**Custom roles and advanced Azure RBAC**

Custom roles. In addition to, or instead of, using Azure built-in roles, you can create Azure custom roles for Azure Sentinel. Azure custom roles for Azure Sentinel are created the same way you create other Azure custom roles, based on specific permissions to Azure Sentinel and to Azure Log Analytics resources.

Log Analytics RBAC. You can use the Log Analytics advanced Azure role-based access control across the data in your Azure Sentinel workspace. This includes both data type-based Azure RBAC and resource-context Azure RBAC. For more information, see:

* Manage log data and workspaces in Azure Monitor
* Resource-context RBAC for Azure Sentinel
* Table-level RBAC

Resource-context and table-level RBAC are two methods of providing access to specific data in your Azure Sentinel workspace without allowing access to the entire Azure Sentinel experience.

**Process Owner**

SOC Manager

# SOC Tools and Resources

## Technical Resources

| **Topic** | **URL Link** | **Description/Comments** |
| --- | --- | --- |
| Networking |  |  |
|  | [IPv4 Subnetting](https://packetlife.net/media/library/15/IPv4_Subnetting.pdf) | Details around IPv4 Subnetting & CIDR Notation |
|  | [IPv6 Subnetting](https://ftp.apnic.net/apnic/training/eLearningHandouts/2017/20170215/20170215-IPv6-AaS-Handouts.pdf) | Details around IPv6 Subnetting to include packet details |
|  | [Network Address Translation](https://en.wikipedia.org/wiki/Network_address_translation) | NAT Details |
|  | [Common Internet Ports](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers) | Common Internet Ports for SOC Analysts |
| Linux |  |  |
|  | [Linux Networking](https://tldp.org/LDP/nag2/nag2.pdf) | Linux Network Administrators Guide |
|  | [Common Linux Commands](https://appletree.or.kr/quick_reference_cards/Unix-Linux/Linux%20Command%20Line%20Cheat%20Sheet.pdf) | General Linux Commands |
|  | [Intrusion Analysis with Linux](https://www.sans.org/media/score/checklists/ID-Linux.pdf) | Linux Intrusion Discovery Guide |
| Security Guides |  |  |
|  | [SANS Glossary](http://www.sans.org/security-resources/glossary-of-terms/) | SANS Glossary of Security Terms |
|  | [Threat Encyclopedia](http://www.trendmicro.com/vinfo/us/threat-encyclopedia/) | Search through Threat Encyclopedia |
|  | [Sophos Threatsaurus](https://www.sophos.com/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=en) | The A-Z Guide to Security Threats |
|  | [TCPDump](https://cdn.comparitech.com/wp-content/uploads/2019/06/tcpdump-cheat-sheet-1.pdf) | TCPDump Cheat Sheet |
|  | [Wireshark User's Guide](https://www.wireshark.org/docs/wsug_html/) | How-to-guide on Wireshark |
|  | [Wireshark Filters](https://wiki.wireshark.org/DisplayFilters) | Wireshark Display Filters |
|  | [Metasploit Guide](https://www.exploit-db.com/docs/english/44040-the-easiest-metasploit-guide-you%E2%80%99ll-ever-read.pdf) | Metasploit User's Guide |
|  | [Netcat Guide](https://cdn.comparitech.com/wp-content/uploads/2019/07/netcat-Cheat-Sheet.pdf) | Netcat Cheat Sheet |
|  | [Network DDoS Guide](https://us-cert.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf) | DDoS Incident Cheat Sheet |
|  | [Memory Forensics Guide](https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf) | Memory Forensics Cheat Sheet |
|  | [NMAP Guide](https://www.stationx.net/nmap-cheat-sheet/) | NMAP Cheat Sheet |
|  | [Log Review - Security Incidents](https://www.sans.org/brochure/course/log-management-in-depth/6) | Critical Log Review Checklist for Security Incidents |
|  | [Keylogger Applications](https://usa.kaspersky.com/resource-center/definitions/keylogger) | Understanding Keylogger Applications |
|  | [P2P File Sharing](https://en.wikipedia.org/wiki/Peer-to-peer_file_sharing) | Understanding Peer-2-Peer File Sharing Applications |
|  | [Security Incident Questionnaire](https://zeltser.com/media/docs/security-incident-questionnaire-cheat-sheet.pdf) | Security Incident Questionnaire Checklist |
|  | [Microsoft Logon Types](https://learn.microsoft.com/windows-server/identity/securing-privileged-access/reference-tools-logon-types?WT.mc_id=Portal-fx) | Microsoft Logon Codes Explained |
|  | [Analyzing Malicious Documents](https://digital-forensics.sans.org/media/analyzing-malicious-document-files.pdf) | Reverse Engineering Malicious Documents Guide |
|  | [Reverse Eng Malware](https://zeltser.com/media/docs/malware-analysis-cheat-sheet.pdf) | Reverse Engineering malware Cheat Sheet |
|  | [Building a Cybersecurity Strategy](https://resources.sei.cmu.edu/asset_files/Newsletter/2021_102_001_651837.pdf) | Six Key Cybersecurity Engineering Activities for Building a Cybersecurity Strategy |

## Threat intelligence Sources

| **Topic** | **URL Link** | **Description/Comments** |
| --- | --- | --- |
| IP / URL / Domain Reputation | [IP Blocklist Check](https://whatismyipaddress.com/blacklist-check) | Verify the IP Address hasn't been blocklisted |
|  | [Project Honey Pot](http://www.projecthoneypot.org/search_ip.php) | Project Honey Pot - System for Identifying Spammers and Spambots |
|  | [DShield lookup](http://www.dshield.org/sources.html) | Internet Storm Center IP & Ports lookup |
|  | [MX Lookup](http://mxtoolbox.com/) | Lists MX Records for a Domain in Priority Order |
|  | [Website Reputation](http://urlvoid.com/) | Website Reputation Checker Tool |
|  | [Research IPs](http://robtex.com/) | Research IPs, DNS, Spammers |
|  | [Virus Total](https://www.virustotal.com/) | Online Service that analyzes IPs, Domains, URL, and Files for malware |
|  | [Validate HTTP Requests](http://www.rexswain.com/httpview.html) | See Exactly what an HTTP request returns to your Browser |
|  | [Malware Domain List](http://www.malwaredomainlist.com/mdl.php) | Tool for determining if Domains are associated with Malware |
| Real-time Threat Monitoring |  |  |
|  | [Malware URL](http://www.malwareurl.com/) | Tool for tracking suspicious URLs |
|  | [Security Wizard](http://www.securitywizardry.com/radar.htm) | Security Wizard for Cyber Threat intelligence |
|  | [Threat Descriptions](https://www.f-secure.com/en/web/labs_global/threat-descriptions) | F-Secure Labs - Threat Descriptions |
|  | [Shadow Server](https://www.shadowserver.org/wiki/pmwiki.php/Main/HomePage) | Intelligence on the darker side of the Internet |

# SOC Incident Actions

## Suspicious PowerShell Command Line

**Actions to Take:**

1. Examine the PowerShell command line to understand what commands were executed. Note: the content may need to be decoded if it is Base64-encoded.

2. Search the script for more indicators to investigate - for example IP addresses (potential C&C servers), target computers etc.

3. Explore the timeline of this and other related machines for additional suspect activities around the time of the alert.

4. Look for the process that invoked this PowerShell run and their origin. Consider submitting any suspect files in the chain for deep analysis for detailed behavior information.

5. Escalate and contact your incident response team for potential forensics analysis and remediation.

**An Anomalous Scheduled Task was Created**

**Actions to Take:**

**1. Validate the alert, collect artifacts, and determine scope**

**2. Inspect the file or URL/IP for suspicious characteristics – is it digitally signed? How prevalent is it? Where is it located? Do the domain registration and hosting history look normal?**

**3. Review the machine timeline for suspicious activities that may have occurred before and after the time of the alert.**

**4. Look for the presence of relevant artifacts on other systems. Identify commonalities and differences between potentially compromised systems.**

**5. Submit relevant files for deep analysis and review resulting detailed behavioral information.**

**6. If alert characteristics and machine behavioral evidence constitute a true positive escalate and contact your incident response team for potential forensic analysis and remediation.**

**Initiate containment & mitigation**

**Actions to Take:**

**1. Record all relevant artifacts to be used in mitigation rules and as new threat intel**

**2. Contact the user to check if the observed behavior was intended.**

**3. Update AV signatures and run a full scan. The scan might reveal and remove previously-undetected malware components.**

**4. Ensure that the machine has the latest security updates. In particular, ensure that you have installed the latest software, web browser, and Operating System versions.**

**5. If credential theft is suspected, reset all relevant users passwords.**

**6. Disconnect the machine from the network to prevent any threat attack progression.**

**7. Block communication with relevant URLs or IPs at the organization’s perimeter.**

**8. If initial investigation confirms suspicions, escalate and contact your incident response team for forensic analysis.**

**An Uncommon File was Created and Added to a Run Key**

**Actions to Take:**

**1. Examine the file in question. Do you recognize it?**

**2. Check the machine timeline for the machine in question. Do you see evidence of a breach?**

**3. Update AV signatures and run a full scan. This may uncover previously undetected indicators of compromise.**

**4. If you determine this may be an attack, reset all relevant user passwords, disconnect the machine from the network to prevent any threat attack progression, escalate, and contact your incident response team for potential forensics analysis and remediation.**

**5. Work with your incident response team and Remove the registry key and file in question.**

**PowerShell dropped a Suspicious File on the Machine**

**Actions to Take:**

**1. Investigate the machine timeline for any other indicators around the time of this alert**

**2. Validate contextual information about the relevant components such as file prevalence, other machines it was observed on etc.**

**3. Run a full malware scan on the machine, this may reveal additional related components.**

**4. Consider submitting the relevant file(s) for deep analysis for detailed behavioral information.**

**5. If initial investigation confirms suspicions, escalate and contact your incident response team for forensic analysis.**

**Device tried to access a phishing site**

**Actions to Take:**

**1. Investigate the machine timeline for any other indicators around the time of this alert**

**2. Validate contextual information about the relevant components such as file prevalence, other machines it was observed on etc.**

**3. Run a full malware scan on the machine, this may reveal additional related components.**

**4. Consider submitting the relevant file(s) for deep analysis for detailed behavioral information.**

**5. If initial investigation confirms suspicions, escalate and contact your incident response team for forensic analysis.**

**MDE detected malware**

Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber-attacks. A malware is considered active if it is found running on the machine or it already has persistence mechanisms in place. Active malware detections are assigned higher severity ratings. Because this malware was not remediated and is active, take precautionary measures and check for residual signs of infection.

**Actions to Take:**

**1. Validate the alert and scope the suspected breach.**

**a. Find related machines, network addresses, and files in the incident graph.**

**b. Check for other suspicious activities in the machine timeline.**

**c. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures.**

**d. Submit relevant files for deep analysis and review file behaviors.**

**e. Identify unusual system activity with system owners.**

**2. If you have validated the alert, document the suspected breach.**

**a. Record relevant artifacts, including those you need in mitigation rules.**

**3. Escalate - Contact & work with your incident response team, or contact Microsoft Support for investigation and remediation services. NOTE: If you don’t have an incident response team, contact Microsoft Support for architectural remediation and forensic.**

**a. Stop suspicious processes. Block prevalent malware files across the network.**

**b. Isolate affected machines.**

**c. Identify potentially compromised accounts. If necessary, reset passwords and decommission accounts.**

**d. Block relevant emails, websites, and IP addresses. Remove attack emails from mailboxes.**

**e. Update antimalware signatures and run full scans.**

**f. Make sure the machine is completely updated and all your software has the latest patch.**

**g. Deploy the latest security updates for Windows, web browsers, and other applications.**

**Additional Actions to Consider:**

**1. Install and run Microsoft’s Malicious Software Removal Tool (see https://www.microsoft.com/download/malicious-software-removal-tool-details.aspx).**

**2. Run Microsoft’s Autoruns utility and try to identify unknown applications that are configured to run at login (see https://technet.microsoft.com/sysinternals/bb963902.aspx).**

**3. Run Process Explorer and try to identify unknown running processes (see https://technet.microsoft.com/sysinternals/bb896653.aspx).**

**Internal Brute-Force Attack**

**Actions to Take:**

**1. Check with account owners to determine if the logon attempts were legitimate.**

**2. Review processes responsible for the logon attempts. If the processes are unfamiliar and corresponding executables are not signed system files, submit the files for deep analysis and review detailed behavioral information from the analysis results.**

**3. Review the machine timeline for any suspicious activities that have occurred around the time of the alert. Identify and review other affected machines.**

**4. If the attempts were malicious, review all successful attempts from the affected accounts. Contain and mitigate the breach—stop suspicious processes, isolate affected machines, decommission compromised accounts or reset their passwords, block IP addresses and URLs, and install security updates.**

**5. Escalate and contact your incident response team, or contact Microsoft support for forensic analysis and remediation services.**

**Unusual sequence of failed logons**

<https://docs.microsoft.com/azure/active-directory/identity-protection/howto-identity-protection-simulate-risk>

**Actions to Take:**

**1. Validate and scope the alert.**

**a. Check the source of the failed login attempts. Contact system and account owners to identify unexpected activity.​**

**b. Check other machines for suspicious network communications from the same location.​**

**c. Check the timelines of all involved machines for other suspicious activities.​**

**d. Check the process tree of all involved machines for unfamiliar processes. Check files for prevalence, their locations, and digital signatures.​**

**e. Submit relevant files for deep analysis and review file behaviors. ​**

**2. Escalate - Contact & work with your incident response team, or contact Microsoft support for investigation and remediation services.**

**3. Contain and mitigate the breach.**

**a. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset passwords, block IP addresses and URLs, and install security updates.​**

**Impossible Travel Activity**

<https://docs.microsoft.com/azure/active-directory/identity-protection/howto-identity-protection-simulate-risk>

**Actions to Take:**

**1. Validate and scope the alert.**

**a. Check the source of the failed logon attempts for the user. Contact system and account owners to identify unexpected activity.​**

**b. Check the location where the performed failed sign in activities came from. Check whether they originated outside of the users standard login location and how long before a login was noticed from their normal location. Within how many minutes?**

**c. Check If the IP addresses are known and safe, add them in the IP address range page to improve the accuracy of the alerts. Otherwise if Malicious, add them to the ThreatIntelligence as Indicators/IOCs.**

**2. If the Identity has been compromised, escalate and work with your incident response team, or contact Microsoft support for forensic analysis and remediation services.**

**Suspicious Attachment Opened**

**Actions to Take:**

**1. Validate the alert.**

**a. Inspect the attachment. Review the process that opened it and its behaviors.**

**b. Check for other suspicious activities in the machine timeline.**

**c. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures.**

**d. Submit relevant files for deep analysis and review file behaviors.**

**e. Identify unusual system activity with system owners.**

**2. Scope the incident. Find related machines, network addresses, and files in the incident graph.**

**3. Escalate and work with your incident response team, or contact Microsoft support for investigation and remediation services.**

**a. Contain and mitigate the breach. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset passwords, block IP addresses and URLs, and install security updates.**

**Unfamiliar Sign-in Properties**

<https://docs.microsoft.com/azure/active-directory/identity-protection/howto-identity-protection-simulate-risk>

**Consideration:**

**This risk event type considers past sign-in properties (e.g. device, location, network) to determine sign-ins with unfamiliar properties. The system stores properties of previous locations used by a user, and considers these "familiar". The risk event is triggered when the sign-in occurs with properties not already in the list of familiar properties. The system has an initial learning period of 30 days, during which it does not flag any new detections. We also run this detection for basic authentication (or legacy protocols). Because these protocols do not have modern properties such as client id, there is limited telemetry to reduce false positives. We recommend our customers to move to modern authentication. For more information - https://go.microsoft.com/fwlink/?linkid=2016528**

**Password Spray**

<https://www.microsoft.com/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/>

**Actions to Take:**

**Four easy steps to disrupt password spray attacks...**

**1. Use Cloud Authentication - In the cloud, we see billions of sign-ins to Microsoft systems every day. Our security detection algorithms allow us to detect and block attacks as they’re happening. Because these are real time detection and protection systems driven from the cloud, they are available only when doing Azure AD authentication in the cloud (including Pass-Through Authentication).**

**2. If you're using AAD, then you're covered with Smart Lockout. If you're using ADFS, enable Smart Lockout - https://docs.microsoft.com/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection.**

**3. Use Attack Simulator to proactively evaluate your security posture and make adjustments - https://techcommunity.microsoft.com/t5/microsoft-security-and/announcing-the-public-preview-of-attack-simulator-for-office-365/ba-p/162412.**

**4. Work with your Identity Global Admin and Enable MFA. A password is the key to accessing an account, but in a successful password spray attack, the attacker has guessed the correct password. To stop them, we need to use something more than just a password to distinguish between the account owner and the attacker. The three ways to do this are below:**

**a. Risk-based MFA**

**b. Always-on MFA**

**c. Azure MFA as Primary Auth**

**5. NOTE: We strongly recommend enabling always-on multi-factor authentication for all admins in your organization, especially subscription owners and tenant admins. Seriously, go do this right now. For the best experience for the rest of your users, we recommend risk-based multi-factor authentication, which is available with Azure AD Premium P2 licenses. Otherwise, use Azure MFA for cloud authentication and ADFS. In ADFS, upgrade to ADFS on Windows Server 2016 to use Azure MFA as primary authentication, especially for all your extranet access.**

**6. If an Identity has been compromised, escalate and work with your incident response team, or contact Microsoft support for forensic analysis and remediation services.**

**Anonymous IP Address**

<https://docs.microsoft.com/azure/active-directory/identity-protection/howto-identity-protection-simulate-risk> This risk event type indicates sign-ins from an anonymous IP address (e.g. Tor browser, anonymizer VPNs). Such IP addresses are commonly used by actors who want to hide their login telemetry (IP address, location, device, etc.) for potentially malicious intent. For more information - <https://go.microsoft.com/fwlink/?linkid=2016442>

**Actions to Take:**

**1. Validate that the IP Address is Malicious.**

**2. Run Playbook Get-IPReputation - This pulls down known malicious info about the IP from Virus Total.**

**3. If no results return, IP is not listed. Validate the login with the User.**

**4. If results from VT are malicious, run VT Query in Sentinel.**

**a. Create a Bookmark, assign entities.**

**b. Attach Bookmark to current Incident.**

**c. Make notes of what known IOC's are associated with the IP Address.**

**5. Validate the login with the User.**

**6. After validation, if the login was malicious, have the user reset their password.**

**7. If an Identity has been compromised, escalate and work with your incident response team, or contact Microsoft support for forensic analysis and remediation services.**

**Adaptive application control policy violation was audited**

**Actions to Take:**

**1. Review the list of applications that were run.**

**2. Review the application control policy that is applied to this machine by visiting the Adaptive Application Controls section in the Azure Security Center portal.**

**3. Review the list of existing rules in each of the rule collections (publisher/path/hash), and identify the rules that have triggered an audit event for the above applications.**

**4. If you have identified a rule that should allow the above applications to run, review the users that ran them.**

**5. In case you wish to allow them and change the application control policy applied to this machine policy group, make sure to add them to the appropriate rules that you have identified in step #3. Otherwise - contact the specific user and escalate this alert for further investigation.**

**6. If the above applications are not currently allowed by one of the rules that you have identified in step #3, and in case that you wish to allow them, make sure to add a new rule to this machine policy group.**

**Suspicious authentication activity**

**Actions to Take:**

**1. Validate the login with the User.**

**2. Enforce the use of strong passwords and do not re-use them across multiple resources and services.**

**3. In case this is an Azure Virtual Machine, set up an NSG allow list of only expected IP addresses or ranges. (see https://azure.microsoft.com/documentation/articles/virtual-networks-nsg/)**

**4. In case this is an Azure Virtual Machine, lock down access to it using network JIT (see https://docs.microsoft.com/azure/security-center/security-center-just-in-time)**

**5. If an Identity has been compromised, escalate and work with your incident response team, or contact Microsoft support for forensic analysis and remediation services.**

**Failed SSH Brute Force Attack**

**Actions to Take:**

**1. In case this is an Azure virtual machine, add the source IP to NSG block list for 24 hours (see https://azure.microsoft.com/documentation/articles/virtual-networks-nsg/)**

**2. Use SSH Keys where possible instead of Passwords for SSH Access to your VMs and Linux Machines (see Use SSH keys to connect to Linux VMs - Azure Virtual Machines | Microsoft Docs)**

**3. If you are using Passwords instead of SSH Keys, then enforce the use of strong passwords and do not re-use them across multiple resources and services (see http://windows.microsoft.com/Windows7/Tips-for-creating-strong-passwords-and-passphrases)**

**4. In case this is an Azure virtual machine, Create an allow list for SSH access in NSG (see https://azure.microsoft.com/documentation/articles/virtual-networks-nsg/)**

# SOC Training

## Leverage Microsoft Learn for Role-Based Training for Information Security Professionals in Azure



**Protect against security threats on Azure**

****

[**Start Here**](https://learn.microsoft.com/learn/modules/protect-against-security-threats-azure/1-introduction/?WT.mc_id=Portal-fx)

**25 min - Module - 8 Units**

Learn how Azure can help you protect the workloads that you run both in the cloud and in your on-premises datacenter.

Learning objectives After completing this module, you'll be able to:

* Strengthen your security posture and protect against threats by using Azure Security Center.
* Collect and act on security data from many different sources by using Azure Sentinel.
* Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
* Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.

**Cloud-native security operations with Azure Sentinel**

This learning path describes basic architecture, core capabilities, and primary use cases of its products. You'll also learn about differences and Get familiar with Azure Sentinel, a cloud-native, security information and event management (SIEM) service.

****

**6hrs 19min / Learning Path / 7 Modules**

Prerequisites Familiarity with security operations in an organization Basic experience with Azure services Basic knowledge of operational concepts such as monitoring, logging, and alerting An Azure Sentinel instance in your Azure subscription

**   **

**  **

[**Intro to Sentinel**](https://learn.microsoft.com/learn/modules/intro-to-azure-sentinel/1-introduction/?WT.mc_id=Portal-fx)[**Deploy Sentinel**](https://learn.microsoft.com/learn/modules/azure-sentinel-deploy-configure/?WT.mc_id=Portal-fx)[**Threats in Sentinel**](https://learn.microsoft.com/learn/modules/analyze-data-in-sentinel/?WT.mc_id=Portal-fx)[**Incident Management**](https://learn.microsoft.com/learn/modules/incident-management-sentinel/?WT.mc_id=Portal-fx)

[**Threat Hunting**](https://learn.microsoft.com/learn/modules/hunt-threats-sentinel/?WT.mc_id=Portal-fx)[**Threat Response**](https://learn.microsoft.com/learn/modules/threat-response-sentinel-playbooks/?WT.mc_id=Portal-fx)[**Query & Visualize**](https://learn.microsoft.com/learn/modules/query-data-sentinel/?WT.mc_id=Portal-fx)

**Additional Sentinel Learning Modules and Badges!**

| **Sentinel Learning Modules** |  |
| --- | --- |
| [**SC-200 part 4**](https://learn.microsoft.com/learn/paths/sc-200-utilize-kql-for-azure-sentinel/?WT.mc_id=Portal-fx) | **SC-200 part 4: Create queries for Azure Sentinel using Kusto Query Language (KQL)** |
| [**SC-200 part 5**](https://learn.microsoft.com/learn/paths/sc-200-configure-azure-sentinel-environment/?WT.mc_id=Portal-fx) | **SC-200 part 5: Configure your Azure Sentinel environment** |
| [**SC-200 part 6**](https://learn.microsoft.com/learn/paths/sc-200-connect-logs-to-azure-sentinel/?WT.mc_id=Portal-fx) | **SC-200 part 6: Connect logs to Azure Sentinel** |
| [**SC-200 part 7**](https://learn.microsoft.com/learn/paths/sc-200-create-detections-perform-investigations-azure-sentinel/?WT.mc_id=Portal-fx) | **SC-200 part 7: Create detections and perform investigations using Azure Sentinel** |
| [**SC-200 part 8**](https://learn.microsoft.com/learn/paths/sc-200-perform-threat-hunting-azure-sentinel/?WT.mc_id=Portal-fx) | **SC-200 part 8: Perform threat hunting in Azure Sentinel** |

** **

** **

****