Managed SIEM:

Building cyber resilience with an integrated, tailored and shared approach.

Solution brief: use cases

verizon

Managed Security Information and Event Management (Managed SIEM) is an event monitoring service built for organizations that want to take their cyber security investment to the next level. Managed SIEM allows them to take monitoring and analytics information gathered on their SIEM into the Verizon SOC or Unified Security Portal, allowing our team of highly skilled security analysts to monitor specific events and send timely alerts. The Managed SIEM service offers the following:

- Integrated operational model leveraging both customer and Verizon security / intelligence capabilities.
- Tailored solution that grows with the customer, including a ramp-up process to align with capabilities as each is implemented and integrated.
- Shared Verizon SOC (24x7) in region leveraging existing facilities and mature operational experience.

A note on terminology.

The most common term is "use case" (UC), but the service has some "use case scenarios" (UCS) that can belong to different use cases. To avoid confusion, we provide examples where appropriate. Depending on a person's background and familiarity with SIEM solutions, terms like "use case", "use case scenario", or "correlation rule" are frequently (and incorrectly) used interchangeably.

The use case term originally comes from software engineering and the Unified Modeling Language (UML), and is defined as a means for specifying the required usages of a system. For SIEM solutions, different people will view UC in different ways depending on their function within an organization.

There are generally four views within the SIEM practice:

- Organizational or enterprise
- Business
- Functional
- Technical

Each view could be expressed in use cases but this would only cause confusion. Therefore Verizon's Managed SIEM solution uses the following terms:

- Enterprise use case = monitoring program scope
- Business use case = monitoring objective
- Functional use case = SIEM use case
- Technical use case = SIEM use case scenario
- Detection rules = actual implementation on the SIEM. Use cases will typically contain multiple detection rules.

Example:

A healthcare organization is required to implement a monitoring program. Besides the different security objectives that every organization needs to meet, its primary monitoring objective is to ensure the confidentiality and integrity of healthcare data.

One of the possible SIEM use cases to achieve this objective is **User Account Activity Monitoring**. To implement this UC, you would need to monitor the logs for different things which are listed as use case scenarios. In this example, this could be a **Brute Force Attack** scenario. The actual technical implementation will then require one or more detection rules.

Example detection rules for the Brute Force Attack scenario are:

- Detection of very large amount of failed logins to one host
- Limited amount of failed logins followed by one successful login
- Limited amount of failed logins on multiple systems

Use Case Scenario (UCS).

Verizon's Managed SIEM offering is designed around the implementation, maintenance and monitoring of use case scenarios (UCS) that are run on a certain amount of logs coming from multiple log sources. The workload of a SOC can always be brought back to these three factors (UCS, volume, amount of sources), which is why all need to be known and managed diligently.

Verizon's Managed SIEM offering allows a customer to select from standard UCS maintained by Verizon. The list of use cases and use case scenarios can be found later in this document.

Custom SIEM content

Obviously, there will be some requirements that cannot be met with standard UCS. Verizon's Managed SIEM service also allows for custom SIEM content. Custom SIEM content can be one of the following:

- A UCS
- A report
- A log parser

Only a UCS will impact the security monitoring load on the SOC. However, all three items have an additional workload impact throughout the life cycle of the SIEM Content (maintenance, tuning, updating, etc). This is why Verizon's Managed SIEM allows a SIEM engineer to handle these custom elements as needed.

The best example to illustrate this is a custom parser. If an organization has an in-house developed software platform with very specific log lines, a custom parser will be needed. Every single time the application log file format is changed, the parser needs to be changed.

UCS as intellectual property

Use cases (UC) and use case scenarios (UCS) can't really be claimed as intellectual property. All typical UC have their roots in security best practices, and industry or regulatory standards. If you search the Internet for use cases, you will find plenty of resources providing lists of UC and UCS.

The reason this is important is because scenario development is often confused with software development. Verizon's default stance is that we can't claim intellectual property rights over UC, and therefore cannot transfer it. Additionally, we won't delete SIEM content like detection rules, parsers or reports at the end of the Managed SIEM contract term.

Contextual information

SIEM engines have the ability to ingest more than log data - they are also able to use contextual information. Contextual information at a minimum falls under these categories:

- Threat intelligence: Automated feeds of IP addresses, email addresses, domain names, files hashes or URLs that can be used to match against certain properties of log entries
- Business asset information: Examples include location, criticality/availability/integrity ratings, business owner, user
- Vulnerability information: Information about security vulnerabilities of assets
- Other information such as asset functions, network topology, and user identity information

SIEM engines use this contextual data to enrich logs or alerts in order to run certain UCS. Typical examples are the detection of hosts that belong to botnets (through detection of command and control traffic), or traffic to / from Tor-nodes. Both of these scenarios rely on the availability in the SIEM of known botnet and Tor node IP addresses. These IP addresses are matched against IP addresses in the logs.

This use of contextual data is not to be confused with the contextual data that a security analyst uses while investigating alerts. Analysts can rely on contextual data from many other sources in unstructured forms.

The Verizon Managed SIEM service comes with a threat intelligence feed that is quality controlled by Verizon. Additional commercial or community feeds can also be fed into the SIEM but depending on their quality it may increase false positives.

Real-time versus not real-time

Some UCS will generate alerts in real-time as they occur, but this is not true for all of them. There are reasons why some UCSs are better handled not in real-time:

- Reporting purposes. For example, UCS that detect specific assets being added to the infrastructure don't need an immediate escalation
- To enable other UCS. For example, detecting failed logins for regular users is required to detect brute force attacks
- To track longer term trends
- For tuning of new UCS
- Low severity UCS

It is possible that one UCS has rules that act differently, so a UCS with a combination of real-time and not real-time rules may sometimes be needed.

Impact of log sources on UCS

Not all scenarios will work by default. Some UCS will only work when specific data points in logs are available.

For example, a UCS to detect mail-based malware can only be detected if the mail content is analyzed.

SIEM product caveats

It is important to realize that the implementation of UCS, with the intake of logs or contextual information, has a system impact. Key points:

- The most obvious factor is that log volume, UCS, and reports can impact performance
- Depending on the technology, a high number of concurrent SIEM searches might occur when a high volume of UCS or reports are run
- Feeding a lot of contextual data into the SIEM may create a lot of overhead when the SIEM needs to enrich logs and alerts with this information

All of the above should be validated with the SIEM vendor to make sure that the amount of data and the number of UCS chosen is supportable by the existing / planned hardware.

verizon

Verizon Managed SIEM:
List of Use Cases and Use Case Scenarios

verizon

User activity monitoring

Integrity compromise: Collects information on a possible system integrity compromise, such as to detect someone attempting to disable auditing to cover their tracks.

Privileged account created: Collects information to detect the creation of new accounts with elevated rights.

Privileged access failure: A failed attempt to log in using a privileged account was detected.

Login failure: A login failure for a regular account was detected, or a user forgetting his/her password needs to be investigated.

Privileged access success: Registers successful logins of privileged accounts.

Asset detection

New key asset detected: Detection of new web servers, mail servers and DNS servers added to the network.

Compromise

Remote shell detected: Detects whether a compromised host has a shell open from an external host. Attackers use shells to control hosts remotely.

Exploit against a vulnerable system: Detects whether an exploit was launched against a system that is known to be vulnerable to that type of attack (through vulnerability data available in the SIEM).

Potential hacked account: A successful login was detected for a user account that was subject to a password guessing attack in the last x days.

Credential attacks

Authentication brute force attack: Detects a large amount of login attempts towards a system. This might be due to a configuration issue.

Data leakage

Connection to exfiltration site: A connection to a data exfiltration site was detected. Exfiltration sites are typically included in threat intelligence feeds based on URL or IP address, but can also be detected by DLP functionality in security devices.

Possible data exfiltration: Detection of a potential insider threat actor who is trying to exfiltration data using cloud storage drive providers like Google Drive, One Drive or Dropbox, or by using about channels such as SSH. It can also be detected by DLP functionality in security devices.

Exploit

2017 vulnerabilities: Detects exploit attempts using vulnerabilities reported in 2017.

2018 vulnerabilities: Detects exploit attempts using vulnerabilities reported in 2018.

Industrial control

Possible ICS attack: An identified exploit that is known to cause security issues on industrial control systems.

Mail attacks

Mass mailer: This scenario will trigger when bulk email traffic is being detected from the same source to a large number of destinations in a short time frame. Although bulk email may be legitimate traffic, it may also be caused by a spreading computer virus.

Mass mailing to single external address: Detection of large amounts of mail being sent from the customer's network to a single external email address.

Malware

Backdoor traffic: A backdoor Trojan differs from a Trojan in that it also opens a backdoor on a compromised system. They are also sometimes called Remote Access Trojans (RAT). They are popular because they have the potential to allow remote administration of a system.

Aggressive worm: Trojans which have the ability to spread in a very fast way by being able to use social media, p2p networks, instant messaging, etc. They usually serve the same malicious purpose as other Trojans, such as the creation of a botnet for launching large-scale attacks or spam campaigns.

Malware distributor: A system used to distribute malware. Many exploit servers will redirect a victim system to a malware distributor to download additional malware.

Virus detected: Triggers when an AV found malware on a host.

Internal malware traffic: Internal malware traffic or activity has been detected within the customer environment. The presence of malicious software may disrupt computer operation, gather sensitive information, or gain access to private computer systems. The main goal of poisoning networks with malware is to steal sensitive information of personal, financial or business importance.

Inbound malware traffic: This scenario will trigger when malicious traffic inbound to the customer network is detected.

Outbound malware traffic: This UCS will trigger when malware traffic or activity has been detected from the customer network to the Internet. This may indicate compromised hosts within the customer environment.

Network attacks

IRC traffic: This UCS will collect information gathered from traffic from or to Internet Relay Chat Servers (IRC). Because IRC connections are usually unencrypted and typically span long time periods, they are an attractive target for DoS/DDoS attackers and hackers. Also, hosting IRC servers on a corporate network may violate the corporate policy.

DoS attempt on host: A vast amount of connections or resource-intensive requests are being made to a single host which might overwhelm it and make it unavailable. This is often described as a denial-of-service (DoS) attack. The attack itself could be performed by either exhausting the network bandwidth of the connection, or by sending incomplete three-way handshake packets so the memory of the host will be saturated.

Reconnaissance

Internal scanning traffic: The purpose of this UCS is to collect information on internal hosts scanning other internal hosts, and/or flooding other internal hosts with a large amount of data. Although it is not unusual that some servers send a lot of data within a network, this UCS will collect events which are not typically seen in large volumes within legitimate network traffic.

Outbound scanning traffic: This UCS will collect events generated from traffic which can be abused to perform outbound reconnaissance using NetBios; RDP or SNMP to gather information from systems outside the customer network.

Inbound scan traffic: Inbound scanning traffic using SNMP; RDP or NetBios Sweep can lead to revealing critical information on hardware and OS from the customer's network. This information can be used by malicious people to attack other services on the network.

Authorized vulnerability scan: Vulnerability scans regularly run by companies are the best way to gather and map vulnerabilities within the corporate network. This UCS will collect events provided from known company vulnerability scanners in the corporate network.

Authorized vulnerability scan by providers: This UCS aggregates events coming from known vulnerability scan providers to the company's network, and the potential reply traffic from customer assets to a scan.

Unauthorized vulnerability scan: Detects vulnerability scans not performed from the company's vulnerability scanning IP range, or not from a known vulnerability scanning provider.

Web application assessment: The focus of this UCS is set to web-related security events generated from internal sources or targeted internal web servers. This scenario collects multiple events from a variety of web-based security events to reveal web server assessments.

Port scanning: A single host is scanning multiple ports in a short time frame on the same destination, or scanning multiple hosts with the same destination port. This type of traffic is usually part of reconnaissance and might be a prelude to a more serious attack.

Risk-based

High risk event: If risk-based SIEM UCS are feasible on the specific SIEM, this will trigger when an incident has a high rating.

Suspicious behavior (1)

Suspicious P2P traffic: Multiple events show suspicious P2P activity.

Sinkhole: Sinkhole is a previously malicious domain controlled by a non-malicious party for research or victim identification. Traffic to sinkholes helps identify infected hosts. Some security products have functional sinkhole connections to known command and control servers.

Outbound anonymizer use: The (attempted) use of an anonymizer service was detected. These services are often linked to suspicious activity and/or software, or to circumvent security measures.

Phishing site accessed: A connection to a known phishing website was seen.

Suspicious software URL: An (attempted) connection to a known URL was detected which is related the use or download of potentially unwanted software (adware, spyware, etc.)

Malicious domain or URL access: An (attempted) connection was detected to a domain which known to be related to malicious activity.

Untrusted country: This UCS detects communication between a company and company-identified untrusted country.

Suspicious behavior (2)

Host to BotNet command & control traffic: A connection is seen from an internal system to a known botnet command and control server. These botnets are used by cyber criminals across the globe to steal banking information. However, they can easily be used for other types of data or identity theft as well. They can capture keystrokes, perform form grabbing, and send captured data to a remote attacker. Other than capturing credentials, they also have the capability to group infected clients into different botnets and turn systems into SOCKS proxies.

Tor inbound traffic: Consistent streams of events are seen from an external system with an IP address belonging to known TOR servers.

Traffic from suspicious IP address: Detected communications originating from a watchlist host that is characterized as suspicious. The host's IP address has been associated with one of the following watch list categories: exfiltration site, exploit server, malicious host and/or malware distributor.

Outbound emerging intelligence: Traffic detected for an emerging threat. Traffic was detected, related to an IP address that is listed on a subset of the OSINT intelligence feed covering the indicators seen in the most recent 30 days. It consists of recently reported indicators in the public domain and is matched against outbound customer traffic.

Exploit from untrusted IP: An exploit to a customer host was seen sourcing from a known untrusted IP address.

Connection from proxy to botnet command & control: A connection is seen from a proxy server to a known botnet command and control server.

Connection to command & control malicious domain or URL: This UCS is part of the suspicious behavior category and will create incidents based on events in which traffic to a C2 malicious domain is detected.

Web attacks

Buffer overflow detected: Occurs when an HTTP request contains an entity that exceeds the length setting that is defined in the security policy (also called length violations).

SQL injection: Code injection technique used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injections exploit security vulnerabilities in an application. An example would be when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements, or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. This UCS bundles SQL injections based on SQL injection events generated by security devices.

Command injection: A command injection was seen in web traffic.

verizon

verizonenterprise.com