coresecurity
by HelpSystems

The Daily Life of A SIEM

AN EVENT MANAGER USE CASE GUIDE

THE DAILY LIFE OF A SIEM: AN EVENT MANAGER USE CASE GUIDE

Event Manager is a Security Information Event Management (SIEM) solution that gives organizations insights into potential security threats across critical networks through data normalization and threat prioritization, relaying actionable intelligence and enabling proactive vulnerability management. This is possible via a centralized analysis of security data pulled from a variety of systems.

To put it another way, think of your IT environment as a water purification plant, in which the water represents data. Event Manager acts as the water quality test, ensuring that no matter where the water came from, it's safe to drink. It checks for indicators of impurities like bacteria or heavy metals, raising an alert if the quality does not pass muster.

In order to better demonstrate how this SIEM solution can benefit your organization on a daily basis, we have put together several use cases of the fictional Acme, Inc. to show how Event Manager provides not only robust security, but also streamlines your environment to ensure your security team can operate smoothly and efficiently.

USE CASE: SECURITY EVENT PRIORITIZATION

Security analyst Jim Johnson receives hundreds of notifications from different datastreams and can't read through them all, causing a significant backlog to build up.

DANGER:

In order to safeguard organizations against security threats, monitoring data is generated from sources across the IT environment, including networks, applications, devices, user activity logs, different operating systems, databases, firewalls, and network appliances. Most security events from these data sources are completely benign, like a syslog notification that an automated check for updates found that there were no new updates.

However, mixed in with these minutiae are critical security events, which is what Jim is looking for as he combs through these notifications. However, several roadblocks prevent him from efficiently and effectively addressing these issues.

First and foremost, the sheer volume of events makes it impossible for Jim to uncover security events quickly. This backlog can become very dangerous, as true security problems require urgent attention to prevent permanent damage.

Secondly, raw data from all of the numerous assets is not delivered in one common language. Different logs come in different formats, with different types of messages. Security analysts can't be expected to be experts in every type of language, adding time to the translation process.

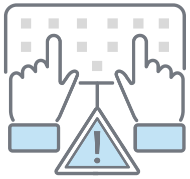
Lastly, security issues can easily be missed or mistaken as harmless without additional context from other sources and events. Given how much time it takes to address the volume and interpretation problems, it is nearly impossible to dedicate resources to attempt to manually correlate events.

REMEDY:

Event Manager specializes in distinguishing critical events from the noise with real time risk prioritization that can be tailored to suit any organization's needs. From there, automated escalation ensures that alerts go to the right person to take on investigation and remediation. Additionally, data is normalized, putting events into a common, readable format that doesn't require additional expertise. This saves analysts time from having to interpret information coming from so many different sources.

USE CASE: DETECTING SUSPICIOUS USER ACTIVITY

A new web administrator, Jane Smith, attempts to access confidential user data from Acme's customer database.



DANGER:

If Jane Smith is seeking to access this information for malicious purposes, she could wreak havoc against Acme. She could delete the entire database, crippling the business, or even sell the data. Even if she didn't mean to access this confidential data, Jane could have still done significant damage, purely from performing actions in systems that she may not be familiar with.

Regardless of whether Jane Smith is successful in downloading the data, this behavior certainly still warrants further inquiries. If no one spots that Jane Smith has attempted to access confidential information that is not pertinent to her job, there is nothing to stop her from trying again, perhaps in some other part of the IT environment.

REMEDY:

Since Jane is a web administrator, any interaction with a customer database would constitute a suspicious action, prompting Event Manager to create an event in real time. With such sensitive data at risk, Event Manager would prioritize this event, prompting a security analyst to freeze Jane Smith's account until analysis is completed and the issue has been resolved to prevent further log-in attempts.

From there, forensic analysis can take place. The security analyst can pull up exactly what activity Jane Smith performed, and examine any related commands executed that are suspicious, either by Jane or any other user. By seeing all the related events together, an analyst is able to define the risk involved in the activity and determine a final evaluation.

USE CASE: DETECT ANY CHANGE TO THE SECURITY CONFIGURATION

Late one evening, a rule in the firewall configuration at Acme, Inc. is modified by an administrator.

DANGER:

Security configurations are critical to the safety of any organization. Any change to any part of a security configuration can leave an organization dangerously exposed if done improperly. Misconfiguring a firewall leaves Acme open to any number of attacks and breaches. For this reason, any changes made to a security configuration must typically be reviewed and approved before implementation.

REMEDY:

Because of the sensitive nature of security configurations, Event Manager can automatically detect this activity and generate an event. Once elevated to Acme's security analyst, they would check to make sure a ticket had been filed requesting the change, as security configuration changes would typically require documentation for review. They would also be able to use Event Manager to filter out any other actions of the administrator to ensure there was no other suspicious behavior prior or after the configuration change. After this inquiry is complete, the analyst would be able to assign the case to security specialist for further analysis, with Event Manager providing a full audit trail of the investigation.

USE CASE: DETECT OPERATIVE MAINTENANCE ACTIVITIES ON INFRASTRUCTURE

The date and time on Acme's application server have been changed.

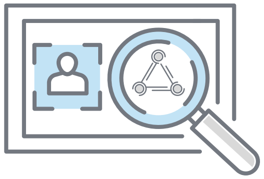
DANGER:

Adjusting the time and date can be a normal activity between servers. Organizations need to have the value synchronized between all servers in the network to avoid delays, so adjustments are continuously made. In most cases, this activity is done automatically with no human intervention. However, there are some date and time changes that could be done manually for malicious purposes, typically to hide actions or to deliberately cause lags in the network in order to crash it.

REMEDY:

When the date and time is changed by a non-automatic task, Event Manager can automatically detect this and create an event to send to an analyst. From there, the analyst can easily investigate if this change relates to normal date and time adjustments that were manually performed. For example, a server that needs to be manually updated for daylight savings. If not, the analyst can escalate the event to a security specialist for further investigation.

USE CASE: MONITOR EMPLOYEE BEHAVIOR



John Doe has worked for Acme Inc. for two years as a database administrator. Last Friday, John abruptly quit.

DANGER:

As a database administrator, John has access to everything in those databases, including user accounts, financial data, and customer information. Additionally, many administrators are given root access, also known as a superuser account. This means that John has access to everything – not just the databases he's in charge of.

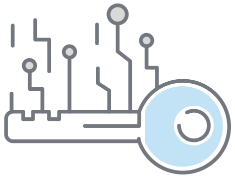
If John is leaving on bad terms, or has other motives for malicious behavior, there's a chance that he could have abused his privileges by stealing or altering data. Unfortunately, because of John's status both as an employee and as a database administrator, typical security alerts would not be activated, as all of these activities are permitted for his job role.

REMEDY:

As mentioned above, a security alert would not have been necessarily raised since John has permission to access secure data. However, with Event Manager, anything outside of ordinary behavior would have been logged as an event and stored. A security analyst can monitor John's historical activity to see if he's been engaging in activity that, while permitted, is not necessary for his job or is suspicious in some other way. The analyst can filter activity by user and check John Doe's account activity to audit his actions. Event Manager can even filter by the source IP to find out if John used another login from the same workstation—perhaps switching from his own user login of JDoe to that of a root or superuser account.

Additionally, Event Manager can check any recorded events from all accounts for a specific timeframe. The analyst could check all events from the 48-72 hour window before John's resignation to make sure large amounts of data weren't deleted, altered, or changed in some other way that would indicate potential espionage.

USE CASE: MONITOR AUTHENTICATION ACTIVITIES



John Smith, an IT admin, works during core business hours onsite, helping Acme staff with any issues they have at their workstations. One Wednesday at 9:00pm, however, John attempts to log in offsite.

DANGER:

As an IT admin, John would have some elevated privileges at a minimum, and may even have full root access. Any abnormal authentication attempts, even from someone who has proper credentials, is considered suspicious. Since John is only supposed to work core hours from within Acme headquarters, there should not be need for him to log on after hours, indicating potential malicious activity or stolen credentials.

REMEDY:

With Event Manager, any unusual authentication attempts would trigger an event creation that would be sent along to Acme’s security analyst for further investigation. Since Event Manager works in real time, even if John is successful in his attempted authentication, the analyst could immediately lock out John, or anyone else who makes abnormal authentication attempts.

USE CASE: PREVENT USERS FROM HAVING MORE THAN ONE ACTIVE SESSION

Joe Bloggs, a network administrator, is logged in under the username JBloggs, performing tasks at his workstation at Acme headquarters. JBloggs also appears to be logged in remotely from a location abroad.

DANGER:

It is extremely rare for anyone to require more than one active session in order to get their job done. Active sessions from different sources, be it different locations or operating systems, almost always indicates that credentials have been stolen. This is particularly dangerous for an administrator, who has additional privileges that can be used to access, alter, and delete critical data.

REMEDY:

Event Manager would create an event the moment a second active session was created for a single user, notifying an analyst with a treatment plan to freeze the account until further analysis can be performed.

From there, the analyst would investigate the actions of the user. In order to differentiate between the two sessions, Event Manager allows you to filter by workstation. That way, the analyst could see the tasks performed by the Acme headquarters workstation and compare them to that of the workstation abroad to assess each session independently.

USE CASE: PCI COMPLIANCE

Like many organizations, Acme must adhere to certain industry regulations. Due to the nature of their business, Acme needs to stay compliant with PCI DSS.

DANGER:

The Payment Card Industry Data Security Standard (PCI DSS) aims to ensure organizations that deal with credit cards properly manage and secure sensitive credit card data to reduce theft and fraud. In order to remain compliant with this regulation, PCI compliant infrastructures and applications must pass each and every requirement and be reverified at least on an annual basis. Though it's a critical cybersecurity standard, proving and remaining adherent can be quite challenging. Losing verification not only shows that data is at risk, it can bring a business to a standstill.

REMEDY:

Acme can stay compliant by relying on Event Manager's PCI view, which detects and displays information relevant to PCI, including login failure events, privilege escalation and subsequent actions taken, changes by a root account, user inactivity events, and account lockouts.

The PCI view will also help Acme prove compliance to assessors by generating built-in reports designed to highlight compliance with PCI DSS. Additionally, compliance views and reports are also available for other regulations like GDPR, BRCA, and SOX, in case Acme falls under other regulations.

USE CASE: LOG ALL CHANGES, ADDITIONS, OR DELETIONS TO ANY ACCOUNT WITH ROOT OR ADMINISTRATIVE PRIVILEGES (PCI DSS REQUIREMENT)

Alice Johnson, a web administrator, discovers changes were made to the server by a web marketer, Bob Jones.

DANGER:

Bob Jones should not have administrative privileges and could have unintentionally caused serious damage. Elevated access should be limited to only those who need it and understand how it is used. More worrisome is how Bob received these privileges. Mistakes are possible, particularly if there are identical or similar usernames involved. However, the addition of privileges is often indicative of malicious activity.

Once someone has root privileges, they can make any number of changes to the IT environment and have access to confidential data. It's vital to know not only what someone with administrative privileges is doing, but who granted them that privilege in the first place. This has become so important that it is now a featured requirement of the PCI Data Security Standard, which is particularly concerned with customer data privacy.

REMEDY:

The moment Bob received root privileges, Event Manager would have sent an alert to a security analyst notifying them of it, due to the sensitive nature of the activity. The security analyst would be able to track down not only what Bob did with his newfound access, but when, where, and who granted him this access.

USE CASE: LIMIT REPEATED ACCESS ATTEMPTS (PCI)

Acme employee Lauren Ipsum's user account, LIpsum, has had over 100 login attempts over the past hour, even though Lauren is out sick.

DANGER:

Repeated access attempts like brute force attacks take advantage of limitless login attempts and are designed to relentlessly try combinations until the account is hacked. Once logged in, the attacker has full control over Lauren's account, and can easily access Acme's data.

REMEDY:

These repeated login attempts would trigger a repetition event to be created, which would be prioritized and escalated to a security administrator. Given the rapid nature of such attacks, the real time event creation would give the administrator enough time to act quickly to lock the account to prevent access from being granted.

From there, the analyst would need to verify that authentication parameters are set to require that a user's account be locked out after no more than six invalid logon attempts to prevent such attacks from occurring again. Additionally, such parameters are a requirement of the PCI Data Security Standard.

USE CASE: MULTI-TENANCY

Acme has recently acquired an organization that focuses on managing IT services for other companies, including security monitoring.

DANGER:

When managing IT services for different companies, using a single instance SIEM solution would require monitoring all the data from every customer under one umbrella and without any segregation. This not only violates best practices, but is also a dangerous security and privacy risk. In order to use a single instance SIEM solution safely, Acme would need to purchase one copy per company they manage. This approach costs not only a significant of money, but also time, due to the upkeep and basic administration of so many individual solutions.

REMEDY:

Event Manager multi tenancy capabilities allow for easy management of so many different partitions. Customer accounts are segregated and easily managed through one centralized solution. Acme can rapidly detect and respond to threats, even for substantial, complex networks with high volumes of security events to manage. Acme will also be able to provide ample flexibility for each individual customer, tailoring each instance as needed.

USE CASE: SECURITY MONITORING ON A BUDGET

Back when Acme first began as a relatively small company, CISO John Locks needed to build a strong security portfolio, and was concerned they could not afford all the solutions they needed—including a SIEM.

DANGER:

Oftentimes, security teams for many small and mid-sized organizations find themselves with no monitoring solution. This is typically due to budget constraints, though there is sometimes an assumption that security monitoring can be done manually if an IT environment is not particularly large. Since many enterprise solutions are primarily designed with large organizations in mind, it can be difficult for such organizations to find a solution that meets their needs or price requirements.

REMEDY:

Event Manager has a free option with smaller organizations in mind, providing access to the enterprise version for a limited number of assets or set capacity, providing increased visibility into their security environments, and enabling proactive vulnerability management.

Having a free version of an enterprise tool provides particular advantages. Acme gets access to all of the functionality, allowing them to take full advantage of the tool, learn how to use it, and decide if it's a good fit. From there, Event Manager can grow with Acme. Instead of having to replace a free tool with an enterprise solution, Acme can simply upgrade to monitor more or an unlimited amount of assets.

APPLICATION MONITORING

Each organization has unique data sources that also need monitoring. Event Manager provides a holistic view of your entire environment by connecting these sources, like a homegrown database or third-party applications. Streamlining your environment in this way reduces the number of consoles your security team has to look at and can provide further insights and protection.

USE CASE: MONITOR ACTIVITY FROM THIRD PARTY APPLICATIONS FOR CORRELATION

A new, credentialed, user account, DbCooper, was created at Acme, Inc. Immediately after creation, the DbCooper account performed several actions within Acme's financial applications. Five minutes later, the account was then deleted.

DANGER:

Since all of this activity is permitted internally, it isn't indicative of a breach and would not be caught by typical anti-malware. Without constant monitoring, this event could easily fly under the radar and not be caught for weeks or months, if at all. This is particularly unnerving when it comes to financial applications, since both confidential data and significant amounts of money are at risk.

REMEDY:

With Event Manager, this event would be caught, escalated, and an analyst would be alerted in real time, allowing Acme to act fast to ensure minimal damage. Event Manager enables third party applications to be integrated into its centralized console, streamlining the monitoring and escalation process. Additionally, it enables an analyst to be able to find correlating events, providing a new angle from which to assess the security picture.

An analyst would be able to see exactly what occurred within the financial application, and if any other suspicious activity took place during that time frame elsewhere in the system. Additionally, the analyst can see who created the new DbCooper account. From there, they could investigate if the DbCooper account, or the user that created it, performed any other suspicious activities.

USE CASE: IDENTIFY INFECTED SYSTEMS

Acme breathes a sigh of relief after its antivirus software prevents a destructive piece of malware from infecting the company's servers. Though glad a breach was avoided, the security team would like to perform a detailed investigation.

DANGER:

While antivirus software can thwart many attacks, the first line of defense for any company should be ensuring that employees are practicing good preventative habits and watching for signs indicative of deliberate insider attacks. Continual reckless behavior increases the chances of harmful malware slipping through the cracks of even the most robust antivirus solutions.

REMEDY:

Integrating an antivirus solution with Event Manager allows security analysts to find correlating events. Not only would analysts receive real time alerts about potential breaches, they could also use other datasources to find events that help isolate where the infection attempt originated.

USE CASE: INTEGRATION WITH NETWORK MONITORING

To enhance their business Acme's IT team has recently introduced several new applications into their environment. Unfortunately, the security team is unaware of these recent additions.

DANGER:

Acme, like many other organizations, has new assets set up by members of their IT staff, who are outside of the security team. There is often a long delay between when a new device or application is deployed and when it is integrated into a security monitoring tool. Threat actors can take advantage of this delay and use new data sources to breach an organization unnoticed, gaining access and stealing data before a tool is ever monitored.

REMEDY:

Acme's network monitoring tool, Intermapper, creates a map of their network, displaying all that is occurring on an organization's network, like performance issues, outages, bandwidth, and any other changes in the network, including the appearance of new devices.

Event Manager can integrate with Intermapper, ensuring the security team will immediately become aware of the presence of a datasource that needs to be monitored for security events. By eliminating the long absence of coverage, potential malicious activity will no longer go unnoticed.

SUMMARY

Ultimately, the goal of Event Manager is to get security teams the most crucial information the moment it becomes available. By consolidating and normalizing data sources, events are given context that can clarify what is a true threat, and what is simply a harmless activity. Instead of being bogged down in a sea of security warnings, with the entire team receiving endless notifications, alerts are sent only when necessary to the right analysts. These use cases are a small glimpse into the streamlined security infrastructure that Event Manager can help create. To see just how Event Manager looks in your environment, contact one of our experts for a personalized demo today.

coresecurity
by HelpSystems

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.