ManageEngine
Log360

How to stay ahead of **cybercriminals using SIEM**

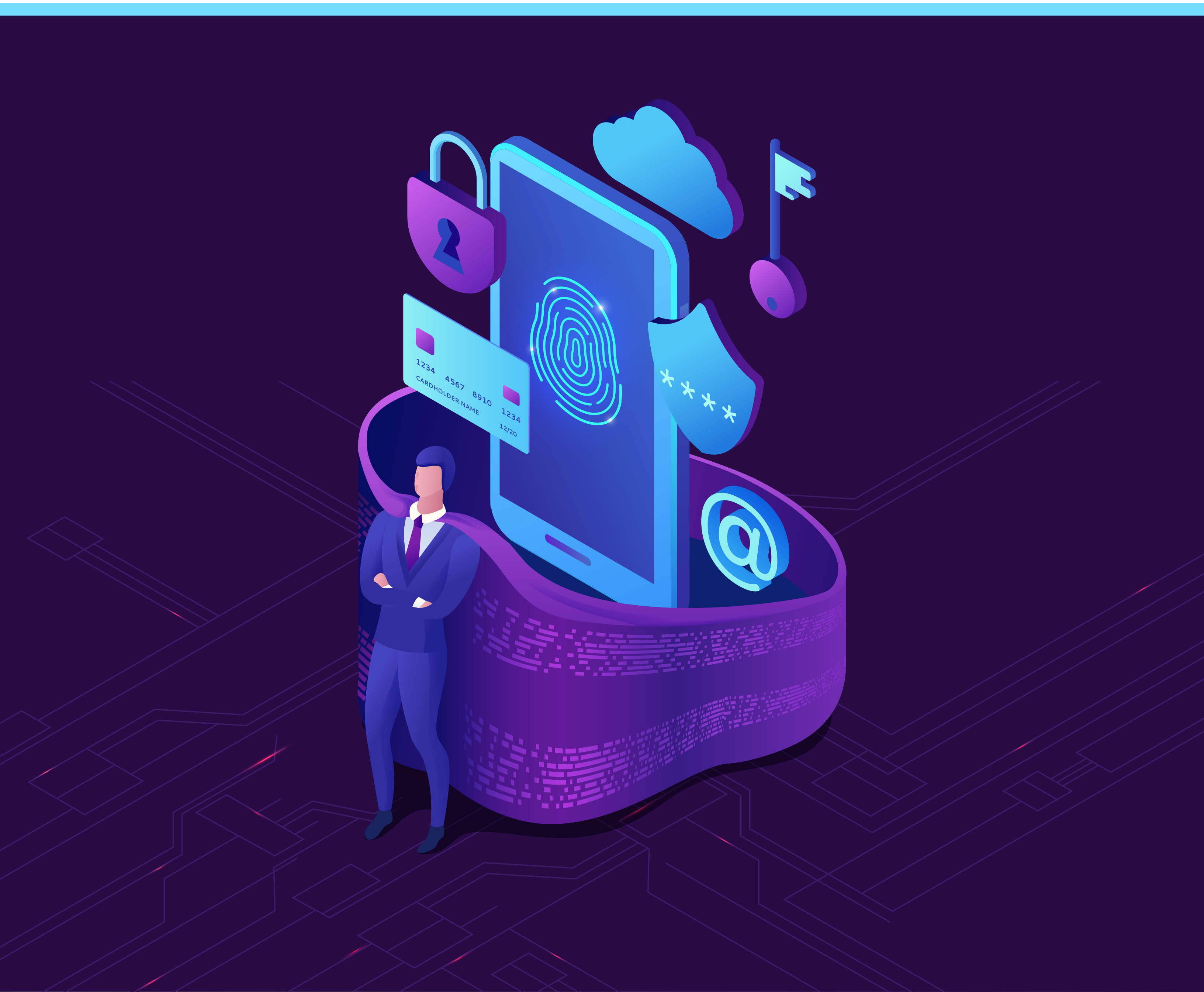


Table of Contents

The business landscape today

Here's an alarming fact: a cybercriminal can breach into 93% of organizations' networks. This is one of the findings by Positive Technologies as part of its new study of pentesting projects. Combining this with the trend of organizations becoming more interconnected, it poses great opportunities for cybercriminals and major concerns for organizations.

Each organization contains not only their own data, but also that of their business partners. So, an organization falling victim to a data extortion attack for example would mean that its business partners are looped into the attack as well. The last year has shown that this is a real cause for concern. This is why it's not just imperative for organizations to secure their networks, but essential.

Using SIEM to stay ahead of cybercriminals

While the current landscape is worrying, it's not a lost cause. Cybersecurity solutions are gearing up to tackle new threats, and the next generation of solutions are promising if implemented correctly. If you're looking to secure your network, SIEM is a way to go.

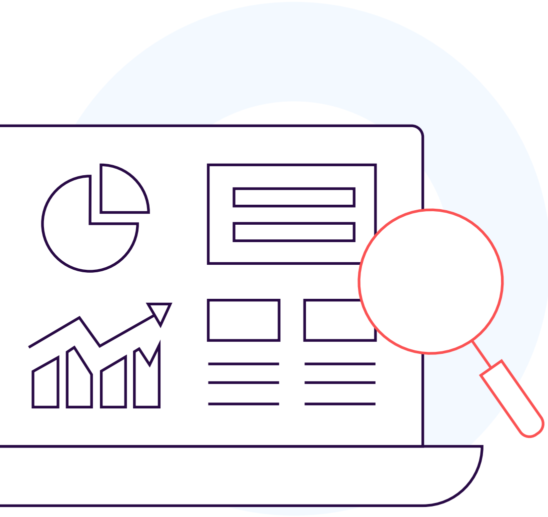
Apart from monitoring your network's logs and issuing alerts, SIEM solutions with automation and AI built in go a long way in reducing incidence response times as well as human error. Here are four ways you can stay ahead of cybercriminals using SIEM solutions:

- ✓ **Getting your environment monitoring right**
- ✓ **Setting up a robust threat hunting system**
- ✓ **Avoiding human error using AI and automation**
- ✓ **Having an incidence response plan**

Getting your environment monitoring right

The first step is to use a SIEM solution to monitor every corner of your network. SIEM solutions run on logs and you need to ensure that all necessary logs are fed into the solution. Once a SIEM solution collects the necessary logs, it can compile the information into reports, graphs, and other formats that can be used by security analysts to detect anomalies, correlate events, and identify anything of concern.

Here are a few examples of sources from which logs can be fetched:



Workstations and endpoints

- User computers
- Printers

Active Directory networks

- DNS servers
- Domain controllers

Business applications

- Exchange servers
- Web servers
- Databases
- Microsoft 365

Perimeter devices

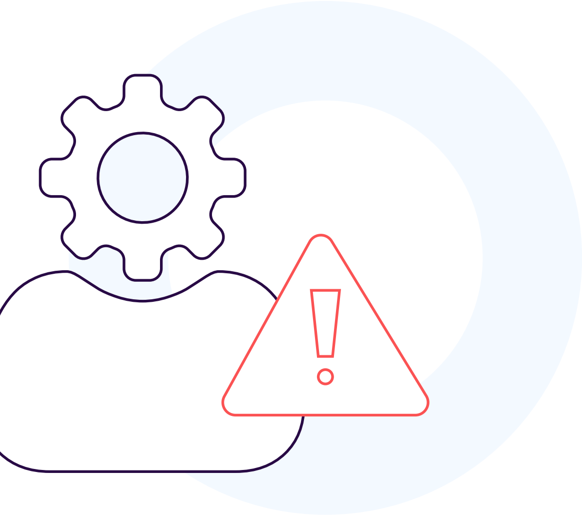
- VPNs
- Firewalls

Cloud applications

- Amazon Web Server
- Azure AD
- Google Cloud
- Salesforce

All these sources of log data can be compiled to provide necessary information about your environment. However, the amount of logs collected is massive, so manually sifting through them to find patterns is time-consuming, labor intensive, and poses the risk of human error. Automation can negate these drawbacks.

Avoiding human error using AI and automation



Use of ML and AI is growing among SIEM solutions as these technologies can effectively identify anomalies in an organization's network. For example, ManageEngine Log360 uses ML and AI technologies to detect unusual behavior of employees. This can help detect malicious insiders using patterns that are often missed when manually correlating events.

A key point to note is that human intervention cannot be completely avoided yet. However, AI and ML can significantly reduce incidence response times, because it can analyze large data sets faster than manual scrutiny. This also reduces the need for human labor and, as a result, human error.

Setting up a robust threat hunting system

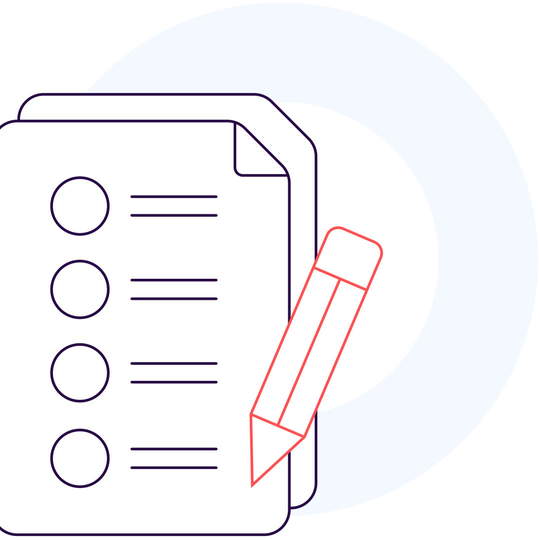
Cyberattacks are constantly evolving, and hackers are becoming increasingly competent in identifying and exploiting loopholes inside an organization's network. While organizations can defend against attack types that have already occurred, identifying attack patterns that exploit zero-day vulnerabilities for example is more difficult.

This is why organizations have to implement a system that can detect malicious actors and hidden attacks that may have slipped through your initial defense systems. SIEM solutions can utilize real-time event response systems that can alert you about any lurking threats. These solutions can retrieve data from a global list of blacklisted IPs or other sources of threat information and correlate the data with logs from your network to see if there has been a security breach.

At this point, if an alert has been triggered, one can assume that an attack is already underway. So, the organization should jump to mitigation measures to reduce the damage as much as possible. While early attack detection is great, it only solves half the problem. Fully successful mitigation includes early attack detection combined with a strong incident response.

Having an incident response plan

A security incident could be an internal or external incident, and an organization should be prepared to deal with both. SIEM solutions are capable of providing real-time alerts of major security incidents. Moreover, more comprehensive SIEM solutions also let you configure your alerts so that if there is a malicious activity in a critical database, or a sensitive file has been accessed by an unauthorized employee, the solution can alert the security team immediately.



The second half of dealing with an incident is the response plan. Automation can play a crucial role here as time is everything. What if there is nobody immediately available to trigger an incidence response plan? In these cases, pre-configuring an incidence response plan for certain critical incidents will give the security team a time buffer to implement additional security measures while the SIEM solution takes care of the initial incident response measures.

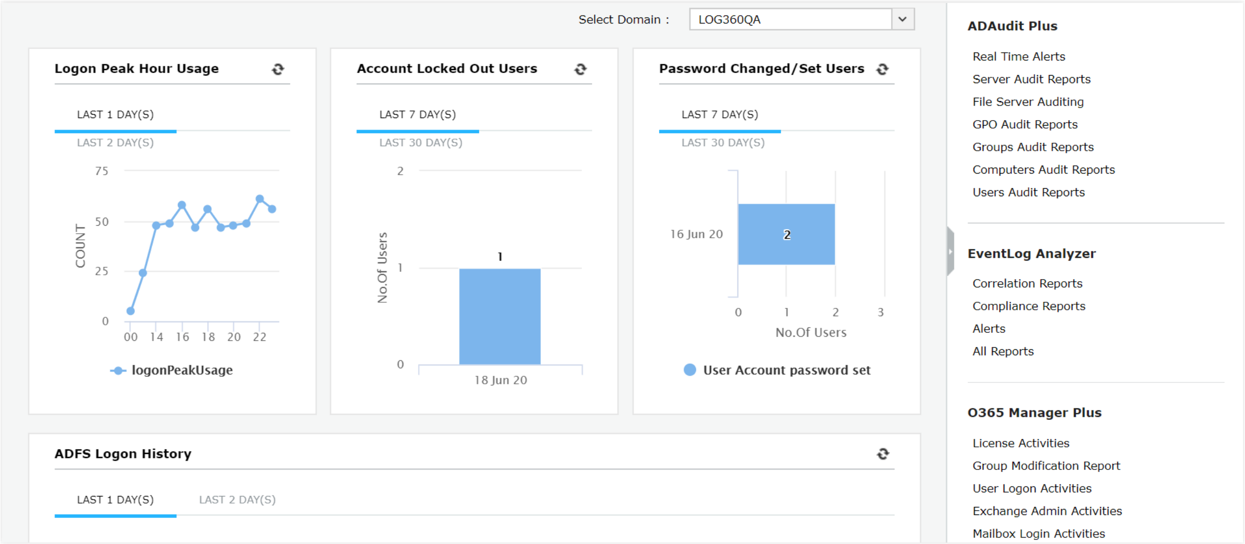
For example, Log360's alerts dashboard comes with the ability to configure custom scripts for certain alerts should the organization deem it necessary. This ensures an immediate response is in place to stop any ongoing attack and gives IT teams time to devise countermeasures to patch flaws, remove malicious web shells, revoke access to critical files and systems, and more to reduce the damage being caused.

Going one step further with Log360

Log360 is a comprehensive SIEM and security orchestration, automation, and response (SOAR) solution that is easy to use with its intuitive interface and offers powerful capabilities. The solution can take care of all the functions mentioned so far and more to ensure your organization is secure. Here's what you can do with Log360:

Comprehensive log management and AD change auditing

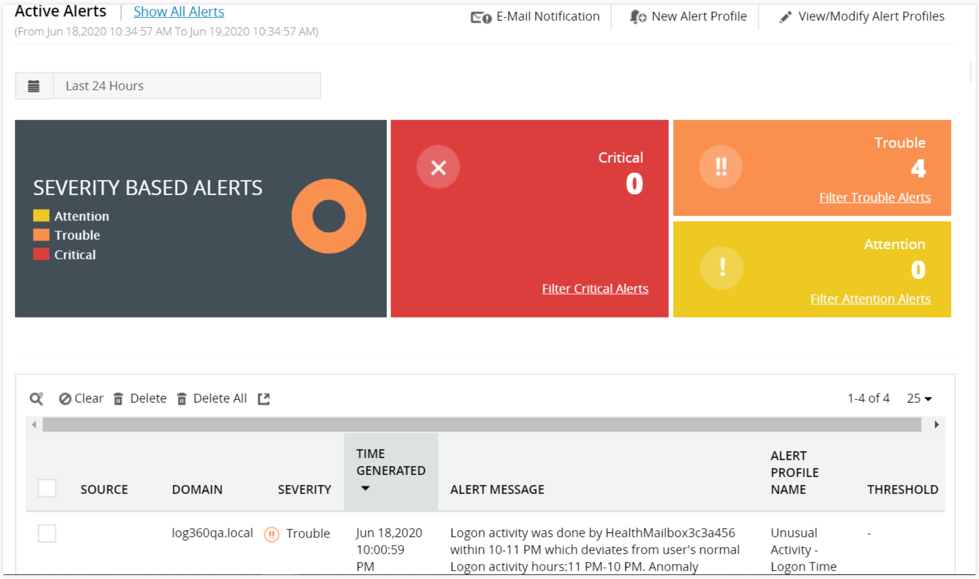
Log360 supports an exhaustive list of sources for log collection such as database platforms, web servers, routers and switches, hypervisors, vulnerability scanners, Linus and Unix systems, firewalls, VPNs, and endpoint security solutions. All the information collected is translated to a common format and displayed in easy-to-read charts and graphs in the dashboard.



Select Domain : LOG360QA

Figure 1: The dashboard of the auditing module in Log360

Apart from displaying data, Log360 stores logs securely to generate reports that can be used for auditing and compliance management purposes. There are preconfigured reports for compliance mandates such as HIPAA, SOX, the GDPR, and more, that come in handy when meeting compliance requirements. Log360 also uses logs to generate alerts for critical incidents and trigger incident response mechanisms if configured.



(From Jun 18,2020 10:34:57 AM To Jun 19,2020 10:34:57 AM)

Last 24 Hours

Critical 0

Trouble 4

Attention 0

1-4 of 4

□	SOURCE	DOMAIN	SEVERITY	TIME GENERATED	ALERT MESSAGE	ALERT PROFILE NAME	THRESHOLD
□		log360qa.local	Trouble	Jun 18,2020 10:00:59 PM	Logon activity was done by HealthMailbox3c3a456 within 10-11 PM which deviates from user's normal Logon activity hours:11 PM-10 PM. Anomaly	Unusual Activity - Logon Time	-

Figure 2: The alerts dashboard in Log360

Threat intelligence

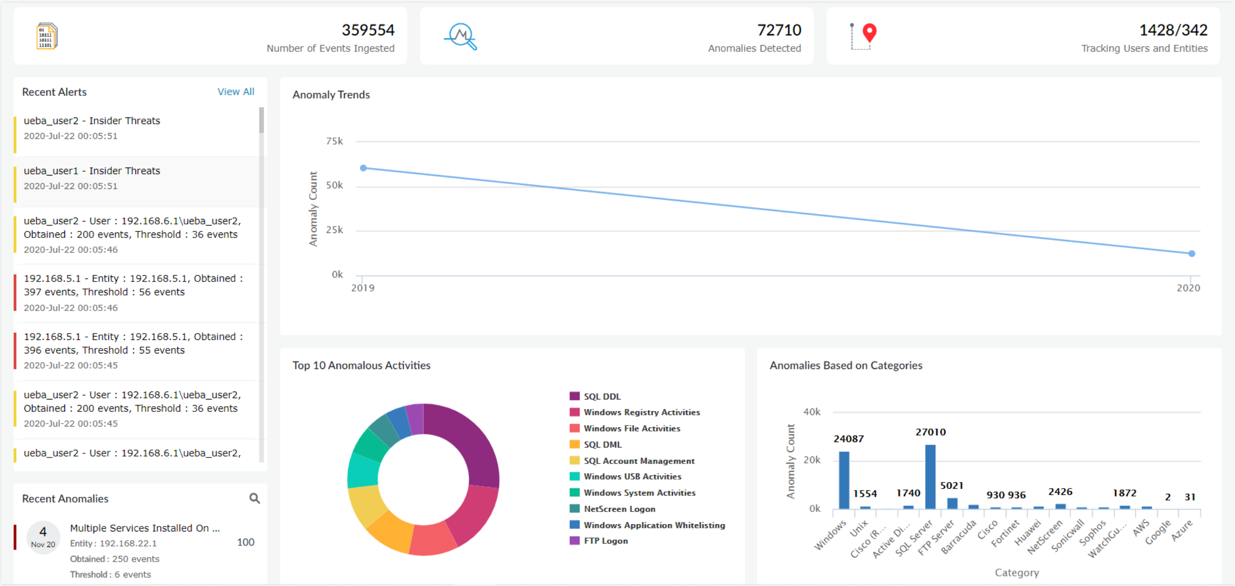
Log360 comes with a robust set of threat intelligence functions that help security teams detect internal and external threats, and hunt for potential hidden attacks and malicious actors. Log360 can:

- Correlate a global blacklist of IPs with the IPs interacting with your network and trigger alerts when there is a match.
- Use **STIX**, a structured language for cyberthreat intelligence solutions.
- Use **TAXII**, a transport mechanism for sharing cyberthreat intelligence.
- Use **AlienVault OTX**, the world's most authoritative open-source threat information sharing and analysis network.

UEBA powered by AI

Automation is an integral part of Log360. A step further in this direction is using ML and AI. This is where user and entity behavior analytics (UEBA) comes into play. UEBA is an anomaly detection cybersecurity technique that can be used to detect signs of anomalous activities of users, hosts, or other entities inside the organization.

The UEBA solution learns about the behavior patterns of the users and entities inside an organization to create a baseline for normal behavior. The solution then uses this baseline to detect anomalous behavior and calculates a risk score, so that security teams can use the scores to detect signs of insider threats, account compromise, or data exfiltration well before damage is done.



359554
Number of Events Ingested

72710
Anomalies Detected

1428/342
Tracking Users and Entities

Recent Alerts View All

ueba_user2 - Insider Threats
2020-Jul-22 00:05:51

ueba_user1 - Insider Threats
2020-Jul-22 00:05:51

ueba_user2 - User : 192.168.6.1\ueba_user2, Obtained : 200 events, Threshold : 36 events
2020-Jul-22 00:05:46

192.168.5.1 - Entity : 192.168.5.1, Obtained : 397 events, Threshold : 56 events
2020-Jul-22 00:05:46

192.168.5.1 - Entity : 192.168.5.1, Obtained : 396 events, Threshold : 55 events
2020-Jul-22 00:05:45

ueba_user2 - User : 192.168.6.1\ueba_user2, Obtained : 200 events, Threshold : 36 events
2020-Jul-22 00:05:45

ueba_user2 - User : 192.168.6.1\ueba_user2,

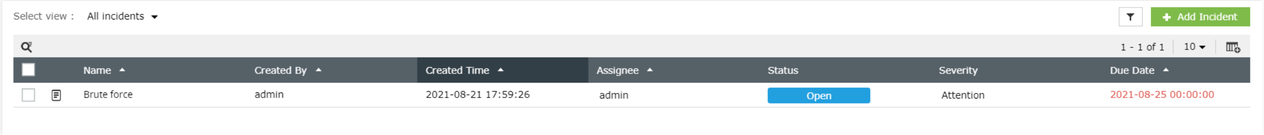
Recent Anomalies

4 Nov 20 Multiple Services Installed On ... 100
Entity : 192.168.22.1
Obtained : 250 events
Threshold : 6 events

Figure 3: The UEBA dashboard in Log360

End-to-end incident management

Log360 comes with a strong set of functions to help organizations build an end-to-end incident management plan. The solution's threat intelligence platform can effectively take care of incident detection and real time alerting, while incident workflows can be used to set up incident response mechanisms that get triggered immediately. This reduces the mean time to detect and mean time to resolve an incident—two important criteria on which successful mitigation measures are based.



Select view : All incidents ▾

☐	Name ▲	Created By ▲	Created Time ▲	Assignee ▲	Status	Severity	Due Date ▲
☐	Brute force	admin	2021-08-21 17:59:26	admin	Open	Attention	2021-08-25 00:00:00

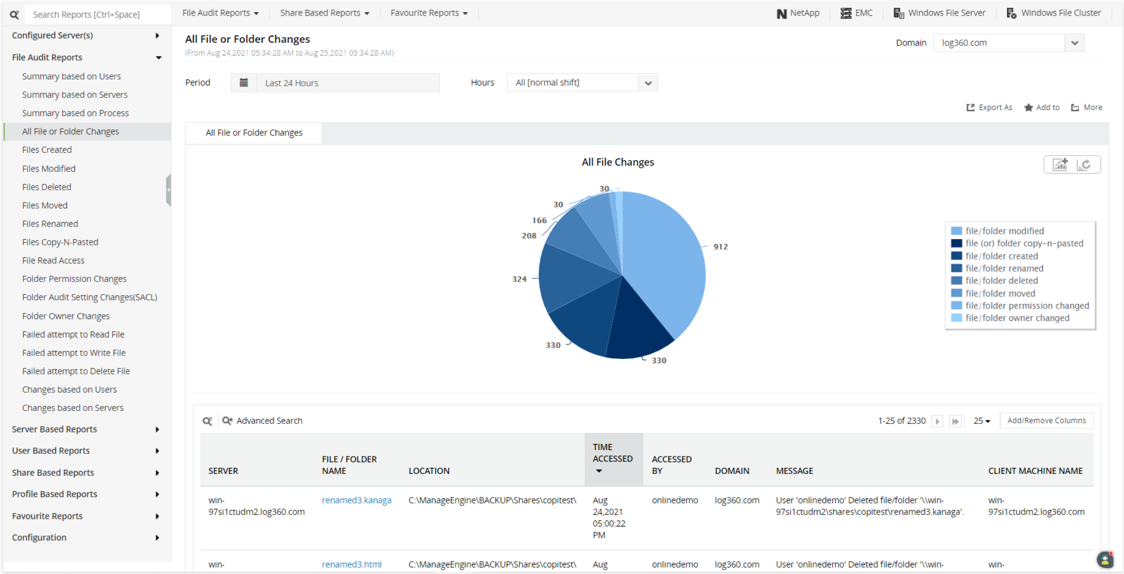
Figure 4: Incident management in Log360

Not some run-of-the-mill SIEM solution

Apart from the features mentioned above, Log360 is capable of many other powerful functions that enhance the security of an organization. Log360 is an effective SOAR solution through which incident resolutions are expedited by prioritizing security threats, automating incidence responses, and accelerating incident investigation and response.

Log360 gives greater visibility into your data like allowing you to specifically monitor and secure personally identifiable information in file servers, spot unusual behavior on such files, and even block USB ports to prevent data leaks.

Apart from all this, Log360 also takes care of your organization's cloud environment security and lets you gain visibility into your AWS, Azure, Salesforce, and Google Cloud Platform cloud infrastructures. It lets you monitor changes to your users, network security groups, virtual private clouds, permission changes, and more that occurs in your cloud environment in real time.



All File or Folder Changes
(From Aug 24,2021 05:34:28 AM to Aug 25,2021 05:34:28 AM)

Domain: log360.com

Period: Last 24 Hours

Hours: All [normal shift]

SERVER	FILE / FOLDER NAME	LOCATION	TIME ACCESSED	ACCESSED BY	DOMAIN	MESSAGE	CLIENT MACHINE NAME
win-97si1ctudm2.log360.com	renamed3.kanaga	C:\ManageEngine\BACKUP\Shares\copitest\	Aug 24,2021 05:00:22 PM	onlinedemo	log360.com	User 'onlinedemo' Deleted file/folder '\\win-97si1ctudm2\shares\copitest\renamed3.kanaga'.	win-97si1ctudm2.log360.com
win-	renamed3.html	C:\ManageEngine\BACKUP\Shares\copitest\	Aug	onlinedemo	log360.com	User 'onlinedemo' Deleted file/folder '\\win-	win-

Figure 5: All file changes monitoring in Log360

Log360 can thus take care of an organization's on-premise as well as cloud security by going beyond what traditional SIEM solutions can offer.

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote

Download