ManageEngine
Log360

GETTING THE BEST OUT OF YOUR SIEM

THE HANDBOOK FOR SECURITY ANALYSTS

Includes interviews with 3 cybersecurity professionals!

Ram Vaidyanathan
& Tanya Austin

Table of Contents

Introduction

Cyberattacks have become more sophisticated and targeted in recent times. Adversaries are performing their due diligence beforehand, and acquiring the right infrastructure, compromising relevant user accounts, and developing specific capabilities to take down organizations. In such a climate, cybersecurity analysts need to play a critical role in their organizations' security function.

To accomplish this larger goal, cybersecurity analysts:

1. **Maintain standard configurations:**
   A cybersecurity analyst needs to ensure that all network resources are safely and correctly configured according to the organization's security policies and relevant compliance mandates.

2. **Assess risk:**
   The analyst needs to perform frequent risk assessments to understand the threats and vulnerabilities that exist in the network. They also need to be aware of the business impact of a possible security incident.

3. **Gain visibility into all activities in a network:**
   At any time, a security analyst should have visibility into all activities in the network. They should be able to source the relevant security logs from across the network to get this visibility.

4. **Monitor threats:**
   They should monitor security threats and indicators of compromise by using techniques such as event correlation, threat intelligence, anomaly detection and alerting.

5. **Perform forensic investigation:**
   In case an incident happens, they need to do forensic investigation to drill down to the root cause of the problem.

6. **Respond to threats:**
   They need to take the right actions in case a breach occurs. This can involve configuring automated response workflows, and improving security controls to ensure the breach doesn't happen again.

7. **Track important security metrics:**
   Many security analysts also track important security operations center-related metrics to ensure that their organization's security posture is constantly improved.

A security information and event management (SIEM) or security analytics solution is the most important part of a security analyst's arsenal as they perform these tasks. The right SIEM solution can help detect threats and mitigate incident. This book is about how a security analyst can make best use of the capabilities of a SIEM solution.

Why should you read this book?

We wrote this book to help you understand the 10 most important capabilities of a SIEM solution:

1. Log sourcing
2. Security analytics and reporting
3. Real time event correlation
4. Anomaly detection
5. Threat intelligence
6. Cloud monitoring
7. Application of cybersecurity frameworks
8. Compliance management
9. Log forensics
10. Incident response

By understanding these capabilities, you can get more out of your SIEM deployment. In Chapter 11, we also share tips and tricks from three security analysts whom we interviewed while writing this book. This may give you some practical takeaways that you can apply in your organization.

Chapter 1: Criticality of sourcing logs

Your SIEM solution must source and ingest logs from multiple devices in your network. You can then put these logs together and identify patterns that indicate a threat. Here are nine log sources that your SIEM solution needs to ingest logs from:

Network devices:

Routers, switches, and access points act as transporters of information. This makes them vulnerable to infiltration attempts. For example, in a SYN flood attack, a server is unable to establish a connection with a client because the IP address of the client is rigged to be unreachable. The server expects acknowledgement to come back from the client, but it never does. The server waits for acknowledgement for a certain time before the request is discarded.

This waiting period throttles the bandwidth of the server. Numerous fake requests, followed by the waiting period, leads to a denial of service of legitimate requests since the server is overwhelmed. To understand the attack vectors in such a situation, you can refer to logs from routers and other network devices. You can check your logs to see the IP address of the server sending multiple requests. You can also check the spike in traffic and the time span during which it happens to identify a potential SYN attack.

Authentication Servers:

User logon information from your authentication servers can reveal potential threats. For example, a logon failure due to a bad password might look harmless, but multiple failed logons could be due to a brute-force attack. Logon information from your authentication servers will show information such as the authentication packages used to authenticate a user. These logs will also reveal why a logon failure happened, how many times it happened, and at what time it happened. You can then start an investigation if required.

Workstations:

Workstation logs provide more granular data on logon and logoff information than the info present on domain controllers in your network. For example, a logon failure will be depicted as "client credentials are revoked." But why these were revoked can be attributed to many reasons that are difficult to figure out from just domain controller or authentication server logs. Workstation logs can tell you more detailed information such as a logon failure occurring due to a disabled account or due to an attempted logon during unauthorized hours.

Active Directory:

Monitoring Active Directory information can help you tackle most of your insider threat problems. These logs will reveal if any new user has been created or if any GPO settings or permissions have been altered; this information is essential to keep your network safe.

Third party applications:

Using third-party applications can sometimes contribute to the vulnerabilities your organization faces. Vet the third-party application you choose to partner with to check if they meet your security standards. Logging all interactions with third-party applications on your network can help you figure out if any related configurations or actions are resulting in alerts.

Databases:

Organizations use database servers to host highly sensitive information including financial data, personal data of stakeholders, and other confidential business information. It's possible for these data stores to be corrupted due to mismanagement by employees, and the valuable data they hold makes them a prime target for hackers. To combat this, it's important to perform around-the-clock database activity monitoring.

File Servers:

Logging file server information can help you get information about who accessed, created, modified, deleted, renamed, or copied a file. You can also find out if someone attempted to access a file and if they were denied access or if access permissions were changed.

Security Devices:

Logging traffic from firewalls and IDS or IPS solutions can help track blocked traffic, intrusion attempts, and any anomalous behavior that could indicate an external attack.

Cloud Platform Logs:

As companies adopt a hybrid and multi-cloud infrastructure, it becomes necessary for you to monitor all the cloud activity in the central console of your SIEM.

Formatting logs for analysis

Even the most rudimentary network can generate an overwhelming number of logs. Unless you format the logs into a usable form, it is difficult to analyze them. To accomplish this, your SIEM solution should add context to and be consistent with the labels of the logs. It also needs to display severities so that the right logs can be prioritized.

Adding context:
Adding contextual information about the event can save you several steps in the investigation process. For example, study these two formats:

- Format 1: 2020-07-15T23:00:27Z|WARN| AD object modified.
- Format 2: 2020-07-15T23:00:27Z|WARN| "ABC" OU name changed.

Format 2 reveals clear information about the event and helps speed up investigation.

Use consistent data and time formats: Since it's important to know when an incident occurred, format your logs to display a consistent time format in all places.

Display severity of event: Not all events are equal in severity, meaning different events require different approaches. Some security events have to be registered as lower priority, so you can identify incidents that need immediate action.

For instance, **2020-07-15T23:00:27|ATTENTION| "ABC" OU name changed** could be registered as a lower priority incident when compared to **2020-08-15T21:00:28|CRITICAL| "Access to File A denied"** since File "A" might be a sensitive file that an unauthorized entity is trying to access.

We recommend that you classify your security events as 1) Warning, 2) Attention, and 3) Critical, so you can respond to critical incidents first.

This approach to formatting your logs leads to improved readability, context, and response.

Sourcing logs with agent-based and agentless collection

If you have even a little experience with log collection, chances are you've heard the terms "agent-based" and "agentless."

Agent-based log collection: This method of log collection involves an agent—precursor software that needs to be installed on devices—to ensure that logs are being collected from them. This information is then transferred to the server intended to store these logs.

Here are four advantages of agent-based log collection:

1. **Deeper insights:**
   You get granular information about network processes and logs, which can help you form deeper insights.

2. **Network bandwidth efficiency:**
   You can program certain agents to filter out non-critical log data and only send the useful data over the network for analysis. This means less bandwidth is consumed while sending filtered data over the network.

3. **Better security:**
   Agents do not require permanent remote access for log collection, which results in better security. The security of an agent can be hardened using firewalls, making it more secure than agentless log collection.

4. **More reliability:**
   Agent-based solutions can monitor hosts even when disconnected from the LAN.

Agentless log collection:
Agentless log collection relies on existing software and applications installed on the devices to collect log data. This means there is no agent playing the middle man for the collection of device logs. This saves you the necessity of having to update the agent and ensures seamless log collection.

Here are three advantages of agentless log collection:

1. **Less intrusiveness, easy & fast to deploy:**
   Since there's no agent being deployed, this log collection method requires minimal configuration.

2. **Lower maintenance cost:**
   There's no need for frequent updates and upgrades.

3. **Suitable for large nodes deployment:**
   Agentless collection is easier for new administrators to get the hang of. If you're using cost-effective but less robust deployment tools, agentless log collection is preferable.

You should have the option to configure both agent-based and agentless log collection depending on your requirements.

Three ways to get logging right

Here are three ways to ensure that you're not just collecting logs, but gaining actionable insights from them.

1. **Log sourcing:**
   The previous section discussed all the sources you need to be logging from. While your organization might have its own logging needs, it's very important that you collect logs from these crucial log sources to make sure you're keeping tabs on essential network resources.

2. **Check for log tampering:**
   Hackers may attempt to evade defenses so you can't catch them. Their immediate goal may be to clear your audit logs so you can't see the nefarious activities they've carried out. Look for Event ID 1102 in your logging solution. This event ID is generated when security logs are cleared. We suggest that you set up notifications when this event occurs. Your SIEM solution will provide information about the user account that cleared the logs.

3. **Low latency logging:**
   Test your log ingestion mechanism to see if your logs are being quickly ingested so that you're monitoring events in real time.

Chapter 2: Getting security analytics right

After your SIEM solution sources logs from around your network and ingests them into a usable format, it needs to interpret meaningful patterns and communicate actionable insights. For this, it should make sense of both real-time and historical data. You should know what user performed what activity, on which host, and at what time. You should be able to achieve both data-centric security and user-centric security.

Data-centric and user-centric security

With data-centric security, you can keep a close eye on all critical data assets and make sure that it does not fall into the wrong hands.

With user-centric security, you can keep a close tab on the activities performed by different users in the network. Whenever a user performs any activity that is suspicious, you can get notified about it.

Developing use cases as a starting point

The best starting point to build your security analytics is to develop highly effective use cases. These use cases would be the answers to the most pressing security challenges that your organization faces.

The use cases you develop should include both essential and complex use cases. While essential use cases involve the basic security hygiene factors almost every company needs, complex use cases involve unique challenges. The analyst firm Gartner outlines several essential and complex use cases that you can build within your security analytics solution.

Here are some examples of essential use cases:

- Monitor for threats such as ransomware and email compromise.
- Comply with regulatory mandates such as PCI DSS, HIPAA, SOX, and GDPR.
- Understand your current security risks using cybersecurity frameworks such as NIST and MITRE ATT&CK.

Here are some examples of complex use cases:

- Defend against threats across distributed geographies.
- Look for high volumes, velocities and varieties of data collection.
- Look for threats across multitenancy environments.

Building value from insights and reports

Your SIEM should provide insights and reports about each use case. You should be able to answer the following questions:

- What activity was performed?
- Who performed the activity?
- Where was the activity performed?
- When was the activity performed?
- How was the activity performed?

You should be able to view a report that displays all the important information in an organized manner. You should also be able to drill down into any of the details provided, choose the specific date range that needs to be considered for the analysis, and export the report in different file formats such as CSV, PDF, and HTML.

Chapter 3: Finding patterns with event correlation

An event A happening all by itself in one part of the network may or may not be malicious. An event B happening all by itself in another part of the network may or may not be malicious. So too with event C and event D.

But if these four events happen one after the other in quick succession, the story could be something sinister. The ability to stitch together seemingly unrelated events as one incident is called event correlation.

Security attacks can be complex. But even the most complex attacks use the same basic groundwork. There's got to be an initial logon by the attacker through some sort of account compromise. Or if a malicious insider is involved, there would just be a legitimate logon. After the logon, the attacker could traverse through the network accessing different servers, changing configurations, relaxing security policies, and even deleting files. It'd be your job to trace the attacker's path and figure out that their sequence of actions is dangerous.

Event correlation can detect potential attacks, as well as provide you with the timeline of malicious actions performed. It does this by sifting through volumes of log data and identifying patterns of activity that may signal an oncoming breach.

For example, think of an attacker who slips through your firewall's defenses, logs on to a Windows server, accesses the database server application installed on it, and deletes critical data. The attacker's log trail is spread across multiple locations. Event correlation's power lies in the fact that it can work with thousands of logs from various devices, pick out this specific sequence of events from your firewall, Windows server, and database server, and alert you within seconds.

Your security analytics solution should give a list of prebuilt correlation rules. These are rules that are built into the solution out-of-the-box by the vendor and would include the most popular use cases. You can use these prebuilt correlation rules to ward off threats such as brute force, cryptojacking, and known ransomware signatures.

Apart from prebuilt rules, you also need the flexibility to build your own correlation rules. After all, every organization is unique and it would be impossible to preempt all the types of threats each organization could face. You know your organization best; so, depending upon the risk your industry and company is exposed to, you can use this flexibility to build your own rules.

Chapter 4: Spotting anomalies with user and entity behavior analytics

Sophisticated attackers are fully aware of the different ways companies attempt to preempt their moves. Therefore, they get innovative and look for new ways to gain an initial foothold, move laterally, delete their footprints to avoid detection, escalate privileges and exfiltrate data. With information about attacks being shared openly nowadays, cybercriminals know that they have to keep changing their modus operandi to increase their chances of success. To achieve this, they use techniques such as:

Zero day attacks:

Threat actors use relatively unknown exploits to compromise a network. Since little information about the exploit is known, you will find it difficult to detect.

Living off the land attacks:

This happens when the attacker uses trusted or whitelisted applications to further their cause. For example, PowerShell, a trusted tool used by system administrators, can be used for malicious reasons, such as domain enumeration, reconnaissance, and even propagating malware. Since PowerShell is a trusted application, it may not sound any alarm and the attack may slip under your radar.

Advanced persistent threat (APT):

In this attack, the adversary gains access into a network, remains undetected for a long time, and slowly steals information. The cybercriminal may achieve this by laying low and gradually escalating privileges. Since the activities are spread over time, you might find it hard to detect an APT.

If you only use a rules-based threat detection system, your network will not be protected adequately. A rules-based system relies on you to write conditions, and it will look for scenarios where these conditions are breached. If a condition is violated, you will receive an alert. There are three issues with this approach:

1. It is difficult for you to predict the cyber kill chain in every possible attack and write a rule to detect it. An attack could follow a completely new sequence of actions that you couldn't have predicted. This is what threat actors leverage as they conduct zero-day, living-off-the-land, and APT attacks.

2. In large and complex networks, the number of users and hosts can be large. In these scenarios, it is difficult to write a rule based on the activity performed by each user or host.

3. You only learn about an attack after it has already started.

To protect against threats that are harder to detect, you should use machine learning-powered user and entity behavior analytics (UEBA). With UEBA, your security analytics solution can learn what constitutes normal behavior for each user and entity in the network, and can create a baseline of regular activities for each user and entity.

An anomaly, by definition, is something that deviates from what is expected. Any activity that deviates from this baseline gets flagged as an anomaly. Every time a user or entity registers an anomaly, the risk score is increased. If and when the risk score goes beyond a certain threshold, you can investigate the issue.

There are primarily three types of anomalies that you can analyze:

1. **Time anomaly:**
   This happens when an activity occurs at a time that falls out of the expected time buckets. For example, a user could exhibit a time anomaly when they logon to the domain at 3am when they typically logon between 8am and noon.

2. **Count anomaly:**
   When the number of activities performed by a user or on a host exceeds what is considered normal for a specific time period, a count anomaly occurs. For example, if the number of accesses of a file between 3pm and 4pm exceeds what is considered normal for that one hour time aggregate, it will trigger a count anomaly.

3. **Pattern anomaly:**
   This results from an unexpected sequence of events. For example, a user called Steve logs on to a host with the IP address 192.168.10.1 at 7pm. While it is normal for Steve to log on to that machine, it is not normal for him to be logged on at that time. This sequence will trigger a pattern anomaly.

Measuring risk accurately with peer group analysis

Peer group analysis is a technique to make your risk scoring more accurate. With this technique, you can identify users or hosts with similar characteristics or behavioral patterns and classify them as one group. You can build better security by comparing the observed behavior of a user or host to that of the relevant peer group. The user or host risk score can be positively or negatively impacted depending on the peer group.

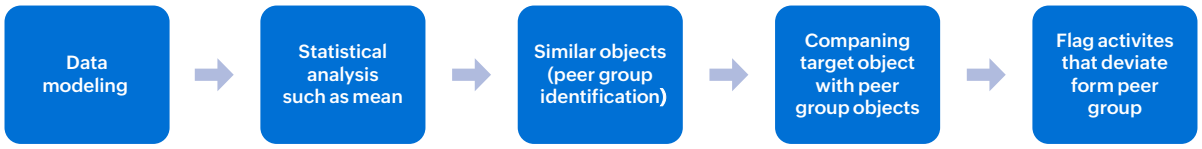


Figure 4-1: Peer grouping for better risk scoring

There are many situations where peer grouping can help build more accurate risk scores. Here are some examples:

1. **First time access of a resource by a user:**
   A user accesses a critical database server for the first time. Without peer group analysis, this activity would be deemed risky. But if the user belongs to the peer group of marketing analysts who typically access this database server, the activity will not be flagged.

2. **Logon time anomaly by a user:**
   A user logs on to the network at a time that deviates heavily from their baseline of expected behavior. If there is no peer group analysis, this could be considered risky. But if the user is a member of a peer group that shows logon activity at that time, the risk score will be lower. In Figure 4-2 below, see an example of an Anomaly Report.

3. **An IT administrator installs unusual software:**
   An IT administrator installs unusual software on a specific host. This could lead to a pattern anomaly and the IT administrator's risk score could rise. However, after peer group analysis, it's discovered that this user is a part of peer group called "IT administrators" and this anomalous action does not really deviate from the average behavior of that group. Therefore, the risk score is not raised as much.

4. **There is an abnormal number of file reads on a host by a user:**
   A sensitive server holds numerous business-critical files on trademarks and product roadmaps. A user reads some of these files and deviates from their expected behavior. Without peer group analysis, the user's risk score from this action might suggest alarming activities.But after peer group analysis, you learn this behavior is typical of a group that contains 100 other members. Therefore, the risk score is not impacted that much.

5. **Thirty users belonging to different departments access a database over a weekend:**
   An engineering-related database is accessed by 30 users belonging to departments such as IT, pre-sales, sales, and product management. Without peer group analysis, this seems like a risky activity and each user's risk score will rise. However, with peer group analysis, all of these users are classed into one group and the risk score is not increased as much.

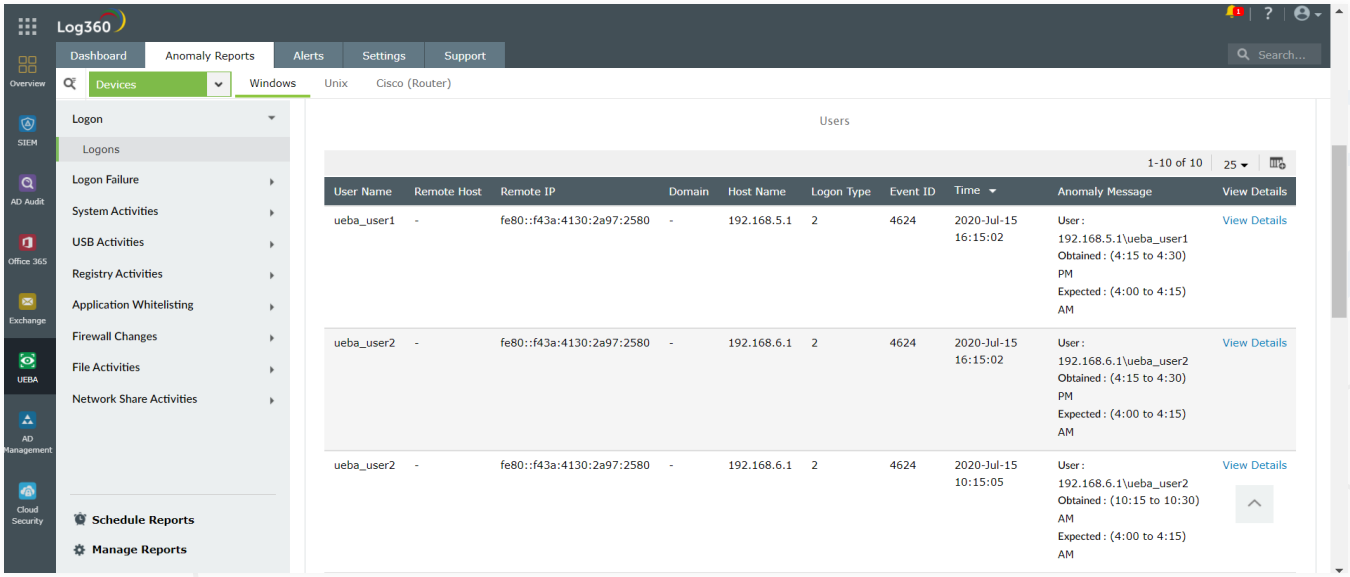


Figure 4-2: Analytics on logon time anomalies on Windows devices in Log360

Using seasonality for even better risk scoring

Numerous products, such as chocolates, summer clothes, workout gear, and Halloween costumes, belong to seasonal markets. The demand for these products typically peaks for a few days or months, and then tapers off. Depending on the market, the sales attributed to seasonality can vary. For instance, the sales of winter clothes during the winter months might eclipse the sales in the rest of the year.

In an organization's network, users, and hosts could exhibit seasonal behavior such as:

1. A database server that's heavily queried on Monday every week.

2. A user who works on alternate Saturdays.

3. A user who accesses a particular file server only once a month and, typically, on the last working day of the month.

These three examples involve rare occurrences that are seasonal in nature. But, are they anomalies? No, they are not.

These three activities (and others like it), although they are rare and deviate from what is expected, are not anomalies. Because they start to be accepted as normal after they occur a few times, they will be scored as normal activities that follow a seasonal trend.

The machine learning algorithms used to detect anomalies must be able to account for seasonality. They should understand seasonal effects on the behavior of users and hosts, and be able to identify a particular activity as non-anomalous, even if it is rare. After accounting for seasonality, no red flags will be raised and risk scores should not be raised. And what if the activity had occurred outside of this "seasonal window?" That would be an anomaly as the use case below illustrates.

Understanding seasonality with a real life example

Your IT company conducts special activities on the first and third Saturday of every month. On Saturday morning, your security analytics platform notices an employee logging into the network. Strangely, it's the second Saturday of the month. A lesser trained system would accept this; after all, the employee was online the previous Saturday, so why not today? But a well-trained system will spot seasonal anomalies like this. It knows the difference between the various Saturdays of a month. An alarm is activated and the risk score of the employee increases.

Chapter 5: Responding better with threat intelligence

Gartner, a leading research and advisory company, defines threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

This definition helps us understand the following aspects of threat intelligence:

1. Threat intelligence helps organizations detect threats observed throughout the world utilizing strategies such as the "known bad" approach that focuses on signs that can be detected to stop an attack, including a hash or an indicator of compromise.

2. Threat intelligence isn't just a list of bad IPs. It includes detailed threat actor profiles, attack mechanisms, and instructions on how to respond to a threat.

3. It's constantly evolving and providing information on existing and emerging threats.

4. Its main goal is to better equip organizations in the fight against global threats.

Using a combination of automated and manual techniques, threat intelligence data is gathered from all over the internet. This data is then processed by dedicated research teams who analyze and validate the information before publishing it in the form of strategic or tactical threat intelligence.

Strategic threat intelligence is intended primarily for human consumption, and it guides strategic security decisions, such as deciding which areas of cybersecurity to focus on, and how to launch employee awareness programs for the latest threats.

Tactical threat intelligence is most commonly published in the form of threat feeds, and it's generally interpreted by one or more security solutions. It is more useful on a day-to-day basis, as it helps organizations detect and fight security incidents in their networks. Some popular threat feeds include AlienVault OTX, FireEye iSIGHT Threat Intelligence, and Webroot BrightCloud Threat Intelligence.

An effective SIEM solution can enable you to use threat intelligence in the following ways:

1. **Add custom threat feeds:**
SIEM solutions process threat intelligence from trusted sources, and some even give you the option to add custom feeds that your organization subscribes to independently. Because many threat feeds are specific to an industry or certain types of threats, custom feeds may make more sense for your organization.

2. **Give a comprehensive view of your network:**
   Knowledge about global threats does you no good if you can't use it within the context of your own network. With a comprehensive view of all devices and applications in your network, a SIEM can notify you if malicious entities are detected on any system in your network.

3. **Reduce the number of integrations:**
   SIEM solutions provide the required functions from a single console with provisions for smooth integration where required. Once a security incident is detected, you can thoroughly investigate, manage, and respond to it. This helps expedite the incident resolution process, ensuring that your organization remains secure from any threat.

Detecting threats intelligently: Two use cases

Here are two use cases where you can use threat intelligence in a SIEM solution to protect your organization from threats.

Use case 1:

Communication with callback servers

Sometimes, an infected system may come under the control of an external server, also known as a command-and-control (C2 or C&C) server. The C2 server can then use this system to extract sensitive data or infect other critical servers in your network.

SIEMs that leverage threat intelligence constantly scan outgoing traffic logs from your network and capture communications being sent to these types of servers. You can then launch an investigation to find out how and when the system was infected, and you can check for other potentially infected systems that have had contact with this C2 server.

Use case 2:

SQL injection attempts from malicious sources

Attackers may exploit vulnerabilities in your web server and inject malicious SQL code to retrieve confidential business records from your databases. To avoid such data breaches, the threat intelligence capability in your SIEM allows you to keep an eye on all incoming connections to your web servers and flag any malicious IPs or domains. In this way, you can contain the loss of important data, and identify and fix vulnerabilities in your web server.

Chapter 6: Hardening your cloud security

The cloud is quickly replacing traditional on-premises data centers, but the trade-off is that you rely much more heavily on cloud providers to handle the security of your hardware. Even so, due to the shared responsibility model in cloud computing, you cannot completely leave security management to cloud vendors alone. Enterprises also have to take proactive measures against cyberattackers targeting their network.

Here are just six simple yet effective steps to harden cloud infrastructure security:

1. **Detect cloud misconfigurations:**
   Cloud misconfigurations are arguably the leading cause of data breaches that take place in the cloud. A misconfiguration occurs when a security admin sets up cloud services improperly or specifies settings that do not provide adequate security for the data stored in the cloud. For example, a common S3 bucket misconfiguration is to make it publicly accessible. This means other users on the web with AWS accounts can access the sensitive data stored in your S3 bucket. A single misconfiguration such as this can cause a massive data breach and lead to non-compliance. Regular, comprehensive security audits of cloud infrastructure help detect security misconfigurations and rectify them immediately before adversaries exploit them.

2. **Perform penetration testing:**
   It's always better for you to hack yourself before an attacker does it for you. You should evaluate the security of your cloud infrastructure by simulating a cyberattack. This can reveal vulnerabilities and enable you to grasp your organization's security maturity. An organization with an ethical hacker on its team can run these simulations and test the performance of their security controls. Enterprises have also been known to hire ethical hackers on an ad hoc basis when they want to test out security configurations.

3. **Gain visibility into all cloud activity:**
   Most organizations around the world have adopted a multi-cloud strategy wherein they use cloud services from multiple vendors. This allows them to distribute their assets, data, applications, and storage across multiple hosting environments.
   While a multi-cloud strategy does have benefits, it also makes it harder for you to monitor what's happening across the cloud at any point in time. An effective security information and event management (SIEM) solution that centralizes the information garnered from all cloud platforms and then alerts security analysts in the event of a mishap is critical. Anomaly detection techniques should also be used to observe any abnormal activities performed by users on any host.

Figure 6-1 shows how an effective SIEM solution like ManageEngine Log360 can provide you with critical information about what's happening in your cloud infrastructure.

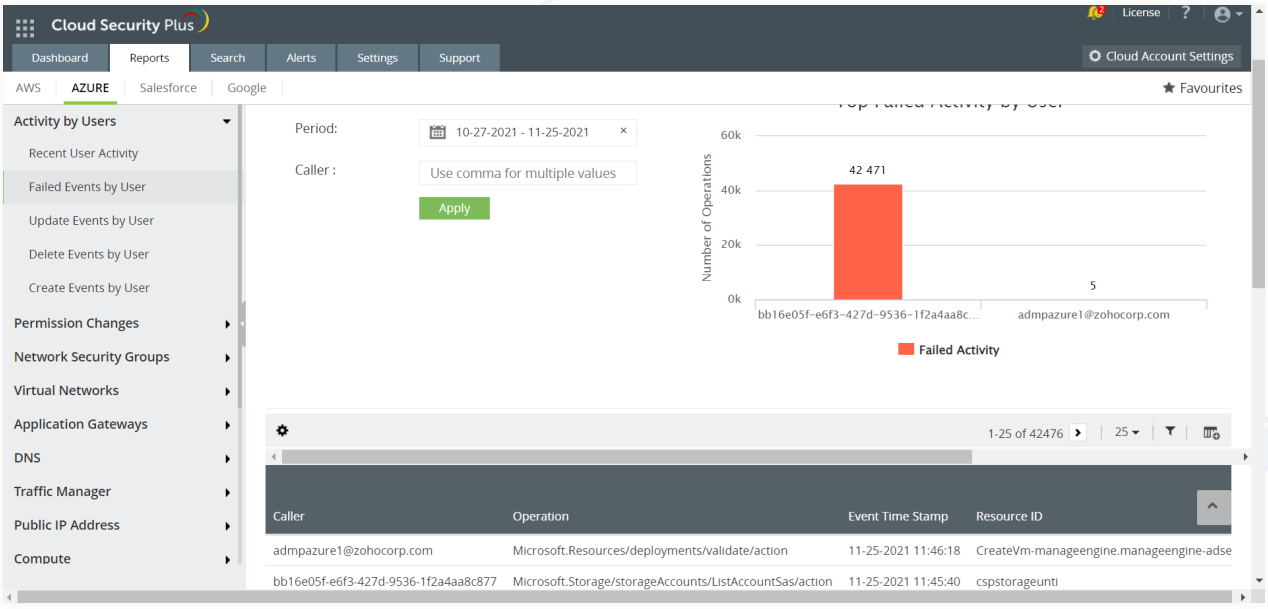


Figure 6-1: Monitoring cloud infrastructures on one console in your SIEM solution

4. **Minimize risk with strong authentication and authorization:**
Implement tight identity and access management controls to ensure that only authorized people have access to resources in the network. The principle of least privilege should be followed, and the Zero Trust security model, which recognizes trust as a vulnerability, should also be put into practice. Just-enough access, just-in-time access, and multi-factor authentication should also be implemented to enhance security.

   Adaptive authentication is a new development that works by creating a profile for each user with a calculation of their risk score. Depending on the risk score, the user may be required to provide additional credentials or, conversely, allowed to use fewer credentials. This allows for more enhanced security. For example, if a user logs in from an unregistered device or from a new geographical location, their risk score automatically increases and they are presented with additional authentication mechanisms to prove their identity.

5. **Introduce a cloud access security broker:**
A cloud access security broker (CASB) is a policy control and cloud visibility mechanism that sits between the cloud service users and the cloud applications. This software monitors all the activities that users do in the cloud and also enforces security policies. The CASB could either be an on-premises deployment or a SaaS application. A CASB can help a company monitor all user activity in the cloud. When a CASB is integrated with a SIEM solution, a security analyst can get deeper context surrounding a user's cloud activity for an investigation.

6. **Train your employees to make security a priority:**
   Employees should regularly be trained to make sure they don't fall victim to an account compromise. It may be necessary to train your employees at least once every six months.

Benefits of a CASB-integrated SIEM solution

The analyst firm Gartner first defined the phrase "cloud access security broker," or CASB, in 2012. It has become a well-known and well-adopted technology for cyberdefense. You can think of it as a solution that sits between an organization's users and the various cloud services they access. And because it sits there, a CASB can help you authenticate and authorize users as they attempt to access the cloud, and it can also enable you to identify what flows in and out of the cloud. Your security operations center may be highly reliant on a SIEM solution today; within the next two years, you must ensure that your SIEM either integrates seamlessly with an external CASB or has built-in CASB capabilities.

A CASB should be part of your SIEM for five major reasons: to address the high uptake of cloud applications, to correlate events that happen in different parts of the network, to prevent data leaks, to provide visibility into shadow IT, and to offer visibility into identity and access management (IAM).

1. **Addressing the high uptake of cloud applications:**
   The average employee uses as many as 30 SaaS cloud applications. On top of that, they use these applications on their own mobile devices. As if this were not enough, most organizations nowadays use a multi-cloud environment with various PaaS and IaaS delivery models. Therefore, you need to have a CASB-enabled SIEM solution that gives visibility into the applications in use and how they are being used. With such a solution, you can also be aware of the level of risk a particular application poses to your organization.

   A SIEM tool without a CASB integration will not give you this visibility into cloud activities. And a standalone CASB will lack the necessary security context provided by events of interest happening in other parts of the network.

2. **Correlating events that happen in different parts of the network:**
   Cyberattacks have become sophisticated in recent times; you have instances of living-off-the-land attacks, cloud malware with initial access in an on-premises server, cloud ransomware and disruptionware, and insider attacks. You need the ability to see patterns and correlate seemingly unrelated events that happen in different parts of the network, and to group them together as a single security incident.

   A CASB-integrated SIEM solution will enable you to see malicious activities in both on-premises and cloud environments.

3. **Preventing data leaks:**
With the advent of cloud apps, there is a substantial risk of both intended and unintended data leaks. For example, an employee in the marketing department may use an app called Font Candy to create vibrant typography. However, this app may be unsanctioned within the organization, and the employee may have private contact details and classified information stored within it. In such a scenario, you need the ability to manage unauthorized uploads of sensitive data and prevent data leaks. With a CASB, you can also enforce cloud security policies and controls to prevent data from being transferred over the internet.

A CASB-integrated SIEM tool will enable you to see all this information on the same console as the rest of the important security information.

4. **Providing visibility into shadow IT:**
Nowadays, most organizations have a list of sanctioned cloud apps that employees can use if they wish. These applications could have become sanctioned after the organization deemed them to be secure and effective for employee productivity. The sanctioned applications are either owned or controlled by the organization. On the other hand, you can also have shadow applications that are outside the ownership or control of IT organizations. Shadow applications may have vulnerabilities and loopholes that could be exploited by attackers.

A CASB will give you the ability to discover shadow applications and the top users who access these applications. A CASB-integrated SIEM tool will allow you to see this information along with other activities the user may have done on the network. This way, you can get the complete picture of possible malicious activities.

5. **Offering visibility into IAM:**
According to Erik Wahlstrom, research director at Gartner, "Organizations shouldn't replace their IAM programs with CASBs, but rather intersect the two for increased governance and access control of cloud applications." A CASB can provide better IAM through ways such as adaptive authentication and user-based risk analysis.

By bringing this capability within SIEM, you will get to see the risky behavior of users in a single console and also use playbooks and workflows to respond to these threats.

Chapter 7: Acing cyber forensics

Cyber forensics involves backtracking an attack to assess the damage and predict if any further harm can be caused. This chapter will walk you through conducting a cyber forensic investigation.

Here's a simple example of how you can use log forensics to understand the intricacies of what occurred during an attack. Assume an alert has been generated by your SIEM tool to let you know that an important file has been modified by a user. Since this is an important file, you check if the user has the privileges to perform such an action. What strikes you as odd is that although the user has the permission to make such modifications, a person in that particular role has no duties that relate to the file that has been modified.

In such a case, you might wonder if the user has been recently added to the access control list with the required permissions. You then look for logs that indicate Event ID 4670, which corresponds to permissions on an object being changed. These logs will reveal who made changes to the access control list. This is a rather simplified version of log forensics.

Querying log files for specific events

Log file analysis is a tedious process because of the large volume of logs generated by all devices across the network. Even if you've configured your audit policies to skim off "noise" during log collection, you're still going to have terabytes of data to process. So the obvious challenge is this: How do you look for an event of interest? As much as this is a needle-in-a-haystack problem, you can query to look for particular events in log files. You can specify how you want log files to be returned and in what order you want them presented.

A great way to search for specific events from terabytes of log data is to use Elasticsearch. This offers you an easy way to search and analyze large data volumes. A good SIEM solution can assist in aggregating your log data, and help you look for specific events using Elasticsearch. Log360 allows you to aggregate your logs and use Elasticsearch to retrieve specific events, and it uses intuitive visuals to display the analytics. Figure 7-1 shows how Elasticsearch is done in Log360.

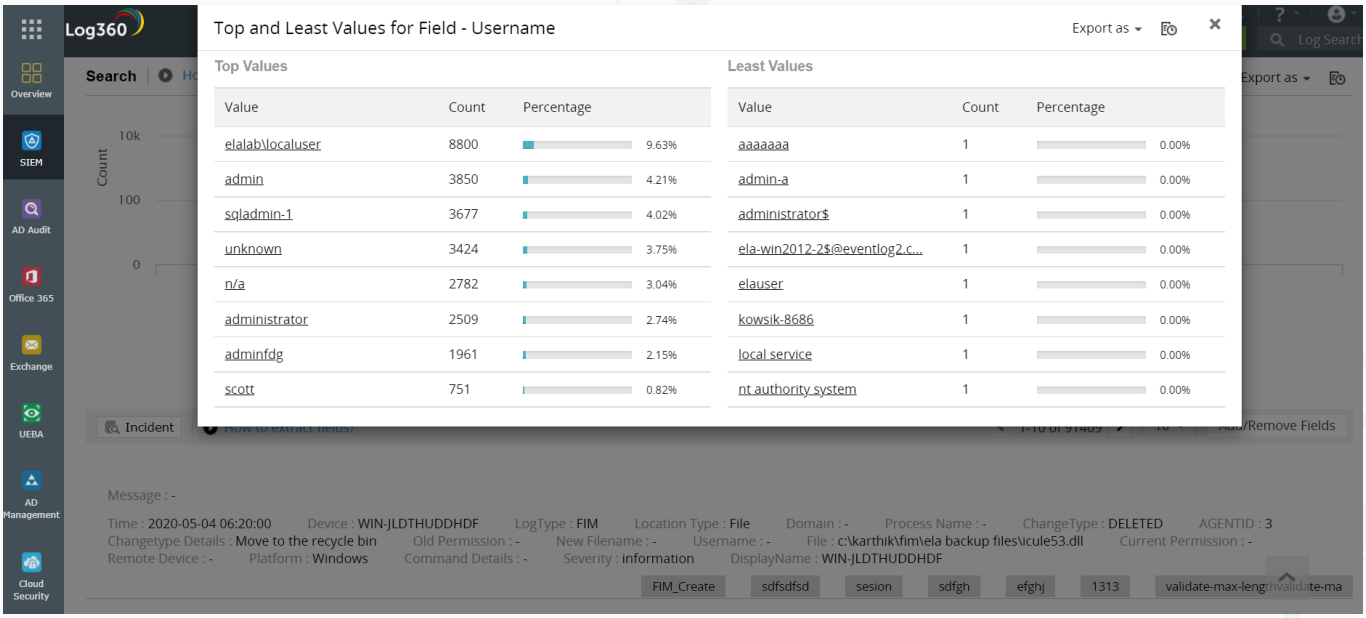


Figure 7-1: Log search engine of Log360

Three hacks to get log forensics right

1. **Check threat intelligence feed:**
   You can supplement your forensics with industry-specific threat intelligence feeds that add context to your network activities. For example, you can get threat intelligence feeds on a malicious IP address that attempted to infiltrate your network. Your threat intelligence feed can provide context on the IP address with historical information, such as any past attacks associated with the IP address that were carried out on other organizations in your sector. This can help you understand what attackers might be attempting to do on your network.

2. **Design alert templates:**
   You can save a search query for future use. You may also wish to save your searches as alerts so you get notified whenever your search conditions are satisfied. This will help cut down on your repetitive tasks.

3. **Visualizing the root cause :**
   Visually representing the sequence of events that led to an alert makes it easy for any analyst to understand the entire pathway of a security incident.

Chapter 8: Complying with regulatory mandates

Periodic audits are conducted to ensure that compliance mandates are followed. It's important for companies to ace these audits to avoid penalties and other major consequences that could disrupt business. Compliance mandates ensure organizations are meeting the minimum requirements to safeguard against security threats.

Popular Compliance mandates

Here are three popular compliance mandates that are in effect around the world:

HIPAA:

This is a US federal law that constitutes privacy laws, breach notification laws, and security laws that protect health information of patients and empowers them with the right to be informed on the disclosure of their information to a third party.

PCI:

PCI DSS is a set of laws that regulate the way credit card information is stored, processed, and transmitted. These regulatory laws improve account security throughout the transaction process. They specify data encryption requirements; protection requirements for cardholder data; and maintenance requirements for firewalls, antiviruse solutions, and other security solutions.

GDPR:

The GDPR is a set of rules that aim to empower EU citizens with more control over their personal data. The GDPR mandates that businesses collect information legally and have the prescribed protection in place to safeguard information from being misused.

Subverting any of these mandates can lead to exorbitant penalties and even jail time. GDPR non-compliance in the UK in 2018 were set to a maximum fine of £17.5 million or 4% of the organization's annual global turnover—whichever is greater—for infringement. For PCI DSS non compliance, fines usually vary from $5,000 to $100,000 per month until the merchant achieves compliance.

It's safe to say no organization wants to spend revenue paying off fines. This is why compliance management is a serious issue that requires attention.

Before getting started on handling compliance within your organization, you need to consider:

1. The domain your organization functions within and the laws or mandates that govern that industry.

2. The existing IT security framework you've got in place and if it is scalable to a growing organization.

3. The technological complexities in your network that will affect your operations, such as access to servers or the location of important network assets.

We also recommend a thorough risk assessment, which is a good way to determine what dangers your organization faces. Risk assessment will help you calculate costs you might have to pay in case of a security incident in your company, both in terms of penalties and losses due to operation interruption. A risk assessment will also help you prioritize what immediate and crippling threats need the most care, so you can invest in the right security solution.

You should also invest in a compliance management solution that can do most of the work for you. Most SIEM solutions offer a variety of IT security controls with in-depth reporting that is mapped to compliance laws that you fall under.

Log360 offers in depth reports to check and prove compliance with the GDPR, PCI DSS, HIPAA, SOX, CCPA, and more. These compliance reports can be customized to suit the internal needs of your company. Keeping in mind the potential for future IT compliance regulations, the solution also offers custom compliance reports, too. Figure 8-1 shows the different compliance-related reports available in Log360.

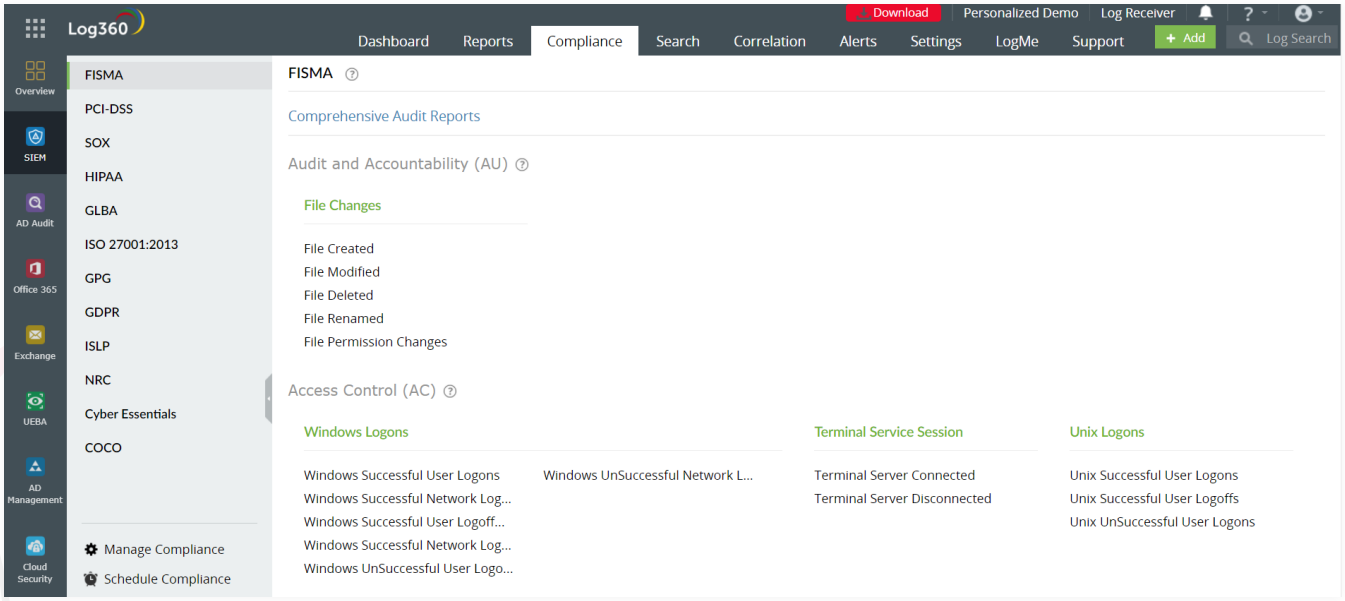


Figure 8-1: Analyzing compliance with Log360

Chapter 9: Sharpening your incident response

So you've collected your logs and centralized them. You've set up threat feeds and defined the kind of events that you want to be alerted to. What's next? Logically, the next step is incident response. Your incident response plan is all the more better if it's automated.

Automating your incident response

An automated incident response plan helps contain the damage while you're trying to figure out the specifics of the threat and how to mitigate it. Automating your incident response will help decrease your mean time to respond (MTTR). Your MTTR measures the average time it takes to control and remediate a threat.

Establishing a low MTTR translates into less damage for you to handle in the long run. When a threat or malicious entity is allowed to ferment within your network for a long period, it can cause even more damage to your network resources and can be catastrophic.

Decreasing the MTTR

Here are eight steps to set up automated incident responses using your SIEM solution. Following these solutions can enable you to decrease your MTTR.

1. **Log events:**
   Set up alerts in your SIEM solution so that you get notified about indicators of compromise. Whenever a user performs activities that go against your rules, you should get an email or SMS about it. Furthermore, this event should also be visible on your alerts dashboard.

2. **Categorize alerts:**
   Each alert should be classified as "Critical," "Trouble," or "Attention" and should be color coded. This will help you prioritize alerts.

3. **Add alerts to an incident:**
   On numerous occasions, there could be multiple alerts; however your analysis will show that these alerts are part of a single attack. In these cases, you should be able to add multiple alerts into one incident. For example, you may wish to treat occurrences of lateral movement and privilege escalation as one incident.

4. **Assign incidents to analysts:**
   Your SIEM solution should allow you to make use of assignment rules to automatically assign the incident to a security analyst.

5. **Track incident status:**
   You should be able to track the status of the incident at any time. You should know if the incident is "open," "closed," or "in progress."

6. **Incident investigation and diagnosis:**
   You should be able to see details such as the incident creation time, the incident age, the hosts and users involved, suspects in the incident, and processes that were run as part of the incident. You should also be able to collate all the evidence and notes about the incident in one place so that you can make informed decisions on how to respond. This will also help you collaborate with other analysts and perform log forensics more effectively.

7. **Respond with automated workflows:**
   Ideally, you do not want any delay in taking action after you receive a notification through email or SMS. This is where automated workflows will help. These will serve as the first response before you step in to take further action. Automated workflows can enable you to log off a user, disable a user, shut down a system, execute a script to change a firewall rule, and more.

8. **Integrate with ticketing systems:**
   Your SIEM solution should integrate seamlessly with popular third-party ticketing tools. The incident can then be managed within the console of your ticketing tool.

Responding with workflows

Here are two real-life scenarios where you can use response workflows.

Example 1:

Defend against insider threats

A malicious insider can physically access a critical server and extract files on a removable device. To mitigate this, you can set up an alert to notify you when a USB device is plugged in to this server during non-work hours. However, an alert alone may not suffice; after all, it takes just a few minutes to copy files. You should have a built-in workflow that can block the USB port on this device and notify you of the status. With this workflow in place, employees won't be able to take confidential information and you can investigate the incident at your convenience.

Example 2:

Disable compromised systems on your network

When an incident occurs, the first step of the investigation is to review your device logs, as all network activity leaves a log trail. Sometimes, attackers gain entry to a network by compromising a legitimate user account. They may then delete logs from the machines they breach to escape detection or hide their continued presence in the network.

You can set up alerts to identify when security logs are cleared from a machine. In these cases, it may be too late to undo the damage already done, but you can prevent any further malicious activity. Create a built-in workflow to log off and disable the compromised user account, effectively cutting off the attacker from your network.

Three tricks to get your incident response right

1. Not every alert needs to be reflected as a separate security incident. Identify related alerts and add them into one security incident. This will help you manage threats efficiently.

2. Store all information about a security incident, because this information might be required for future analysis. The duration you store it for depends on the requirements of your business.

3. Set up advanced reporting for different job profiles. You can start with:

   - **Analyst reports:**
     Number of incidents, types of incidents, and time taken to detect and respond to them.

   - **SOC manager report:**
     Number of incidents handled by analysts along with the average time to detect and respond to threats by analysts.

   - **CISO level report:**
     Analysis of how incidents have impacted the business; where more automation can be implemented.

Chapter 10: Popular cybersecurity frameworks: ATT&CK and NIST

Two frameworks that managed to clear up our foggy lenses when it came to cybersecurity were ATT&CK and NIST. ATT&CK's database of tactics and techniques combined with NIST's framework to assess the security posture create a formidable defense against known threats.

Having a SIEM solution that can map events on your network to ATT&CK's tactics or techniques and implement suitable workflows to deal with them puts you at a place where your SOC team can confidently defend your network. If your SIEM solution can map your security configurations against NIST's requirements as well, you can fortify your organization's security.

An overview of MITRE ATT&CK

ATT&CK's fascinating way of charting out an attacker's objective and methods and matching it with appropriate mitigation strategies makes this framework a trailblazer in helping companies understand the adversarial mindset. Today, ATT&CK has been universally adopted by companies to understand what attacks they're up against and the vulnerabilities that might exist on their networks. Through ATT&CK, they can also infer the kind of security solutions they might need. The ATT&CK framework's foundation is built on publicly-accessible research on cyberattack techniques, threat intelligence on attacks, and reports of security incidents.

The MITRE ATT&CK framework is a matrix that presents the tactics of a cyberattack, the "why" (rows in the matrix), and the techniques of a cyberattack, the "how" (columns in the matrix). For every technique, it also lists sub-techniques. Sub-techniques describe techniques in a more explicit way. Finally, the framework lists procedures that are examples of the techniques and sub-techniques as observed in the real world.

Tactics in the MITRE ATT&CK framework
There are 12 tactics in the framework. These are:

1. **Initial Access:**
   Gaining entry into a network through common techniques like phishing or exploiting external remote services.

2. **Execution:**
   Executing malicious code on the victim's system that allows the attacker to control the system remotely.

3. **Persistence:**
   Leveraging the presence of the malicious entity and striving to maintain its foothold in the network, the attacker attempts to apply techniques like changing configurations or credentials to cut off legitimate users from having access to the network.

4. **Privilege Escalation:**
   Gaining higher-level permissions to escalate privileges.

5. **Defense Evasion:**
   Gaining access to trusted software and existing tools on the system to mask the malware being circulated in the system and hide their own footprints.

6. **Credential Access:**
   Using nifty tools like keystroke capturing or keylogging software to steal credentials of users.

7. **Discovery:**
   Discovering vulnerable points on the network that can be exploited. This could involve discovering a list of accounts and their status in the environment, or scrutinizing trust relationships between multiple domains on the same network that could be exploited.

8. **Lateral Movement:**
   Pivoting through multiple systems using legitimate credentials or exploiting existing remote sessions to move within the organization's network.

9. **Collection:**
   Gathering data of interest to the adversary's goal, like accessing data in cloud storage.

10. **Command and Control (C&C):**
    Communicating with compromised systems on the network in order to execute malicious tasks. The attacker could use application and web protocols to blend malicious commands into regular traffic, making it difficult to detect communication between the attacker and the victim's system.

11. **Exfiltration:**
    Stealing data through automated procedures and packaging the data being exfiltrated to avoid detection. This data is usually compressed, encrypted, and exfiltrated over an alternative protocol rather than the existing C&C channel.

12. **Impact:**
    Disrupting the availability or compromising the integrity of data by manipulating business and operational processes.

Techniques

Each tactic could be accomplished by an adversary through a myriad of ways, and these are called techniques. For example, initial access could be accomplished through 10 different techniques.

Sub-techniques

Sub-techniques are a more granular description of a technique. For example, the account manipulation technique has four different associated sub-techniques.

MITRE ATT&CK and SIEM

If your SIEM solution is able to leverage the MITRE ATT&CK framework and knowledge base, it will make your security defense tighter. Within your SIEM solution, you will be able to see possible occurrences of techniques or tactics executed by adversaries. You can also get alerts if specific techniques are observed, and you can add these alerts into a single incident for efficient management.

Figure 10-1 shows an example of a possible initial access by an adversary as reported by the ATT&CK module of Log360.

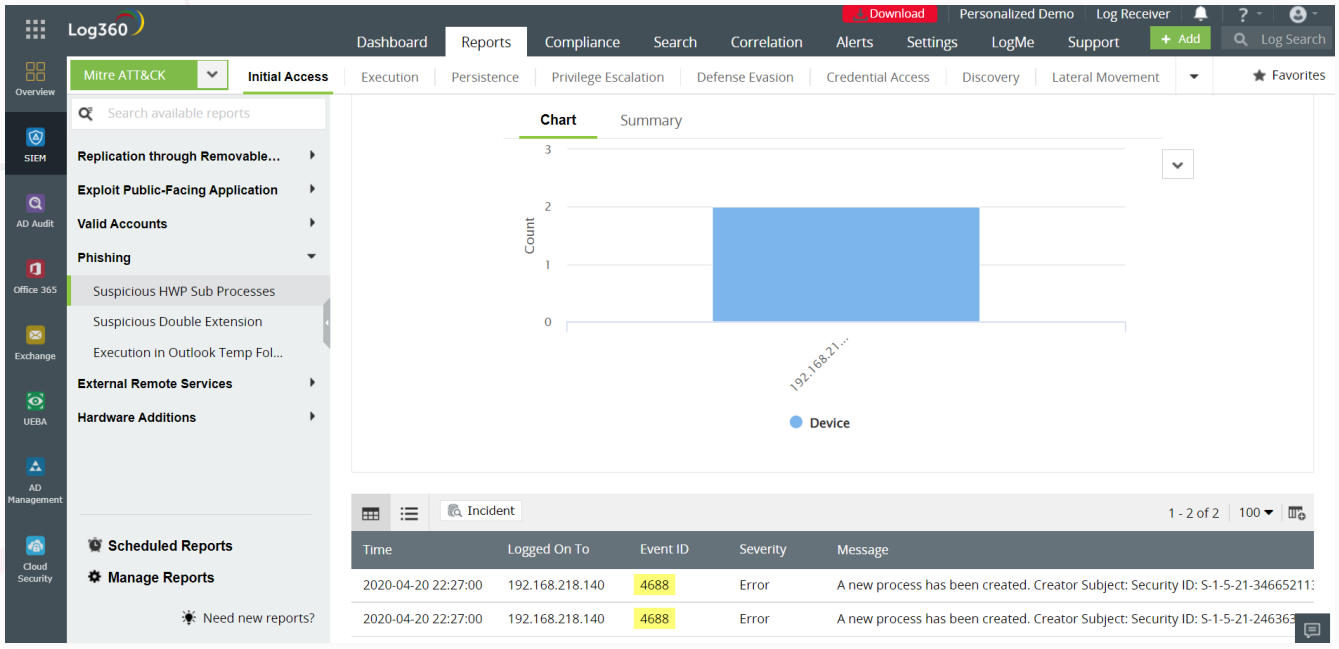


Figure 10-1: Detecting initial access from the phishing technique with ATT&CK reports in Log360

The NIST Cybersecurity Framework in brief

NIST aims to blend industry standards (like FISMA and HIPAA) and best practices (such as risk assessments and asset identification) to help organizations reduce cybersecurity risks. It helps organizations develop a proactive strategy that categorizes assets that need to be protected and helps reduce the risks to these assets. It also advises organizations on the best ways to respond and recover from cyberattacks in case they do happen.

There are three components in the NIST Cybersecurity Framework:

1. **The framework core:**
   This component instructs how to implement uniform defense techniques and comply with industry standards.

2. **Framework implementation tiers:**
   This NIST component helps organizations assess their security maturity level, referred to as implementation tiers, based on the following factors:
   i) What kind of cybersecurity activities does the organization engage in to mitigate possible risks?
   ii) Are cybersecurity activities and defense techniques uniformly implemented across the organization?
   iii) How does the organization participate and contribute to the overall cybersecurity ecosystem?

3. **Framework profile:**
   This component helps organizations define and align their security outcomes, like revisions of the security policy and improvements to the security design, with the associated risks (identified at the "core" stage) and the security maturity level they're currently at (identified in the "implementation tier" stage). Organizations can set this as a "current profile" and then create "target profiles" to determine the maturity levels they aspire to be at.

Making ATT&CK and NIST work for you

The key thing to remember is that a blend of these two frameworks is what will help you strengthen your cyberdefenses. ATT&CK is most useful when your SOC team is running simulations, penetration testing your network, and developing defenses accordingly. This framework is the ultimate reference manual you'll need to equip your red and blue teams. Following this blueprint will help your SOC teams understand what vulnerabilities to fix.

The NIST Cybersecurity Framework's attributes supplement the defense strategy you've started building using ATT&CK. NIST's guidelines are presented as a checklist that you can use to assess your security posture. When you're building a full-fledged defense strategy, you can start by using NIST's assessment checklist to evaluate your security standing and understand issues on your network. You can then delve into understanding how loopholes in your network can be exploited by using ATT&CK.

Chapter 11: Tips from security analysts

As we wrote this book, we spoke to three security analysts who started their careers in cybersecurity within the last five years. They shared with us their journey along with some tips that you might find useful. These are a mix of both general career tips and specific tips on how to get the most out of your SIEM solution.

Conversation with Sanjay Palanivel, SOC analyst at TATA Consultancy Services

1. **Tell us how you got started in cybersecurity.**

   I started in cybersecurity by learning about networking and getting my CCNA certification.

2. **How can cybersecurity analysts or SOC analysts in the beginning of their careers become more effective at their jobs?**

   Learning the art of identifying false positive alerts and addressing incidents based on priority makes for an effective SOC analyst.

3. **What is your daily routine as a security analyst?**

   My daily routine is to analyze abnormal user behavior, detect activities on endpoints, and check for new threats for the day. I also need to check up on my SIEM solution and make sure it's fetching data from all sources.

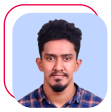
4. **What metrics are important to measure the effectiveness of a SOC?**

   The important metrics of the effective SOC are:

   - Maintaining infrastructure health.
   - Early detection and response to the threat.
   - Maintaining SLAs without any breaches.

5. **How do you foresee the evolution of cyberdefense strategies?**

   Automation replaces manual monitoring of the security monitoring for the events and it will produce a report on this. It will direct the alerts to the incident responder. Moreover, we will see even startups start to hire SOC analysts for their protection against cyberthreats.



Conversation with Nathersha S, IAM analyst at Vanguard Logistics Services

1. Tell us how you got started in cybersecurity.

I started in cybersecurity by getting certified in CompTIA, CCNA, CEH, and ITIL 4. I also found free certifications such as Microsoft Azure Fundamentals and Aviatrix Certified Network Associate valuable.

2. How can cybersecurity analysts or SOC analysts in the beginning of their careers become more effective at their jobs?

As a SOC analyst, you should not restrict your learning to the field or role you are placed in. Apart from using the SIEM tools as part of your role, you should explore every bit of how the incident happens. For this, you should have a strong footing in network and security fundamentals and good problem-solving abilities.

Keep learning about new attack vectors that you read about in the news. Find out how they happened.

3. What is your daily routine as a security analyst?

Maintain the overall IT infrastructure, databases of all employees, computers, printers, and devices connected to the office network.

Onboard employees with RACF create mailbox and Active Directory accounts, and provide RDP and VPN access. I also need to provide new users least privilege access and make sure they have the necessary privileges to get their job done.

Off-board employees and revoke and remove their access to accounts, email, and applications based on role-based access management. I also need to do a manual audit of other non-synchronized applications.

4. Can you give your comments about data security?

I would like to refer to authentication, authorization, and accounting here.

Authentication: We need to ensure that each individual has a unique identity for themselves to prove that they are who they claim and can access the requested data. To make this strong, we can have more than one form of authentication: multi-factor authentication or triple-factor authentication to be more secure.

Authorization: Once the user proves their identity, we need to verify whether they have the required level of access and whether their role permits them to access and alter the required information. The system and policies have to adhere to the principle of least privilege. An individual should only have access to the set of resources their role demands. A user should not be granted root privileges or admin privilege until and unless the nature of their job role demands it. This ensures the data can be accessible only to the authenticated and authorized person and other intruders cannot claim access by spamming their identity.

Accounting: You should track the activity of every employee while they are accessing the system resources, network services, and other forms of services. If an employee inputs incorrect login credentials for a while, the system should automatically stop them and block the login, as this could be a brute-force attack. The organization should always audit and check the logs of employees to make sure everything works as per the defined policy.

Logs should be audited frequently to check for anomalous behavior of the system or employees.

5. How do you foresee the evolution of cyberdefense strategies?

Organizations are inviting bug hunters and rewarding them with high bounties. This is proactive security.

More organizations are conducting penetration testing. I think this happens on average once every six months. However, due to the advances of attacks, we need to be more prepared for all possible outcomes and do this once every three months at least.

Conversation with Logeshwaran, IT security analyst at Legato Health Services

1. Tell us how you got started in cybersecurity.

I started my career as a desktop support engineer. I went on to become a systems engineer and then a security analyst.

2. What skills did you need to acquire as you got started in cybersecurity? How did you acquire those skills?

I started in cybersecurity by googling social engineering. I spoke to cybersecurity folks in my company to get an idea about the fundamentals. Analytical skills are essential. You've got to constantly question why and how an incident happened and keep digging deeper.

3. How can cybersecurity analysts or SOC analysts in the beginning of their careers become more effective at their jobs?

To be more effective in cybersecurity, you have to:

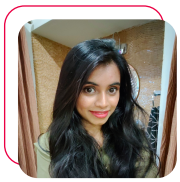
- Learn constantly about emerging threats from sites such as bleepingcomputer.com, tryhackme.com and hackthebox.eu.
- Join a security forum or community, and keep tabs on what others in the domain are saying.
- Never discard alerts even if they happen to be false positives. You need to understand why the alert came through. You will learn with experience to identify false positives.

4. What is your daily routine as a security analyst?

This is my daily routine:

1. Read about new and emerging threats.
2. Check my infrastructure to ensure there is no impact from any new threat.
3. Ensure that we don't run outdated versions of software, as exploits for those will be easily available on the internet.
4. Solve any developer queries, because a secure code means less work.

Author Bio



Tanya Austin:

Tanya is a cybersecurity enthusiast who has authored multiple cybersecurity e-books and articles. She likes to research and write about threat detection tools that empower a security operations center, user and entity behavior analytics, and frameworks such as MITRE ATT&CK that help ramp up an organization's security posture.

Ram Vaidyanathan:

Ram is a cybersecurity expert and evangelist at ManageEngine, a division of Zoho Corporation. As part of his role, he keeps himself updated about the latest techniques attackers use to bring down organizations along with how organizations can defend themselves with the right defense solutions. He speaks at various security conferences and seminars, and interacts with his audiences about Log360, a comprehensive SIEM solution.

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities to detect, investigate and respond to security threats. It brings threat intelligence, machine learning-based anomaly detection, rule-based attack detection, event correlation, log forensics, cloud security monitoring and incident management to address complex security use cases of organizations. Log360 ensures the security of different on-premises, hybrid and cloud network components such as Active Directory, perimeter devices, workstations, databases, business-critical applications, cloud services and more through continuous monitoring.

The user interface is simple to understand and use. With its intuitive dashboards and advanced security analytics capabilities, a security analyst will immediately know if a threat is lurking anywhere in the network. With alerts and contextual responses, they can also resolve the problem before it turns into a major security incident.

For more information about Log360, visit manageengie.com/log-management.

Try Log360 at no cost for 30 days

You can try Log360 at no cost for 30 days in your own network environment, and evaluate its benefits. This is a completely risk-free way to test drive Log360!

Download Log360 at no cost

For a personalized demo, visit manageengine.com/log-management/demo.html.

For a quote, visit manageengine.com/log-management/get-quote.html.