EXTENDING A SECURITY TEAM THROUGH SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

InquisIT, LLC. | 14900 Bogle Drive, Suite 203 | Chantilly, VA 20151
Info@inquisitllc.com | www.inquisitllc.com |

WHAT ISSUES ARE SECURITY TEAMS ENCOUNTERING?

Companies and organizations around the globe are struggling to keep up with the demands of trying to stay afloat in a sea of security incidents while still actively hunting for threats and extend security in their network.

Every day, multiple upon multiple tickets flow into security organizations. This constant onslaught of cybersecurity incidents has left many organizations trying to play catch up while still actively hunting and advancing security.

When combining the factors listed here in addion to the many complicated issues of dealing with cybersecurity, this allows attackers to gain further footholds and maneuver latterly throughout environments.

Hence, the reason for **Security Information and Event Management (SIEM)** tools. These tools can alleviate most issues that occur from an overworked, understaffed, and any fallen behind team.

LACK OF WORKFORCE & TIME

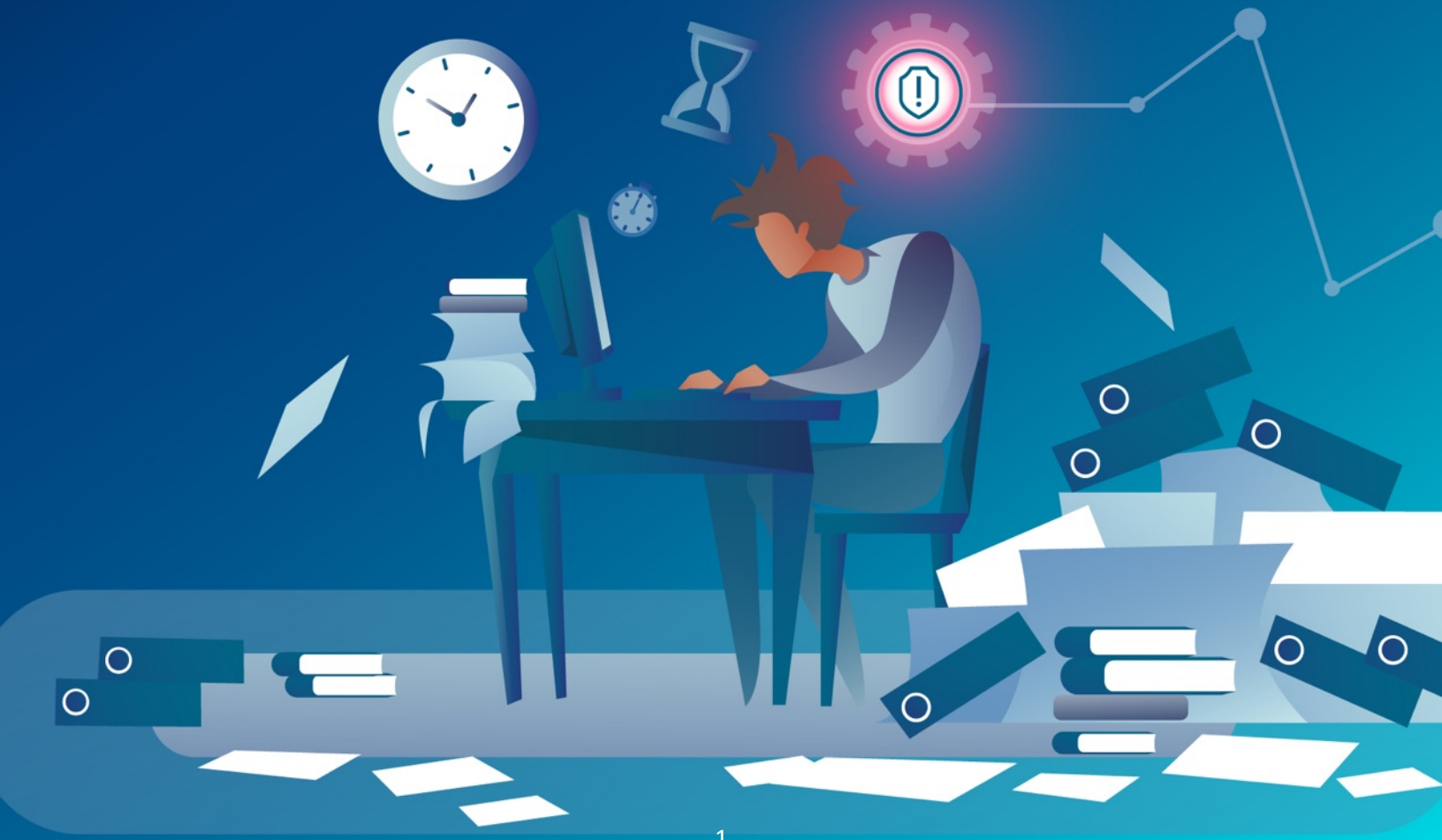
On average, a security incident, based on industry data, takes approximately 8 hours to complete from start to finish. Even if there are multiple highly skilled incident handlers on your team who can handle juggling multiple incidents, on average, they will most likely be able to handle approximately 2-3 full incidents a day.

WORKLOAD

Incident handlers already have copious amounts of work on their desk. Incident handlers have almost no time throughout their day to read, join conferences, or listen to new attack methods that are starting to occur across their industry. Thus, they can fall behind on new advanced methods that attackers are utilizing.

CUT BACKS ON SKILLED TECHNICIANS

Organizations everywhere are cutting back on the number of skilled technicians that they can employ. This forces more work and less research time for all of the current individuals inside of any organizations' information security department.



WHAT IS A SIEM?

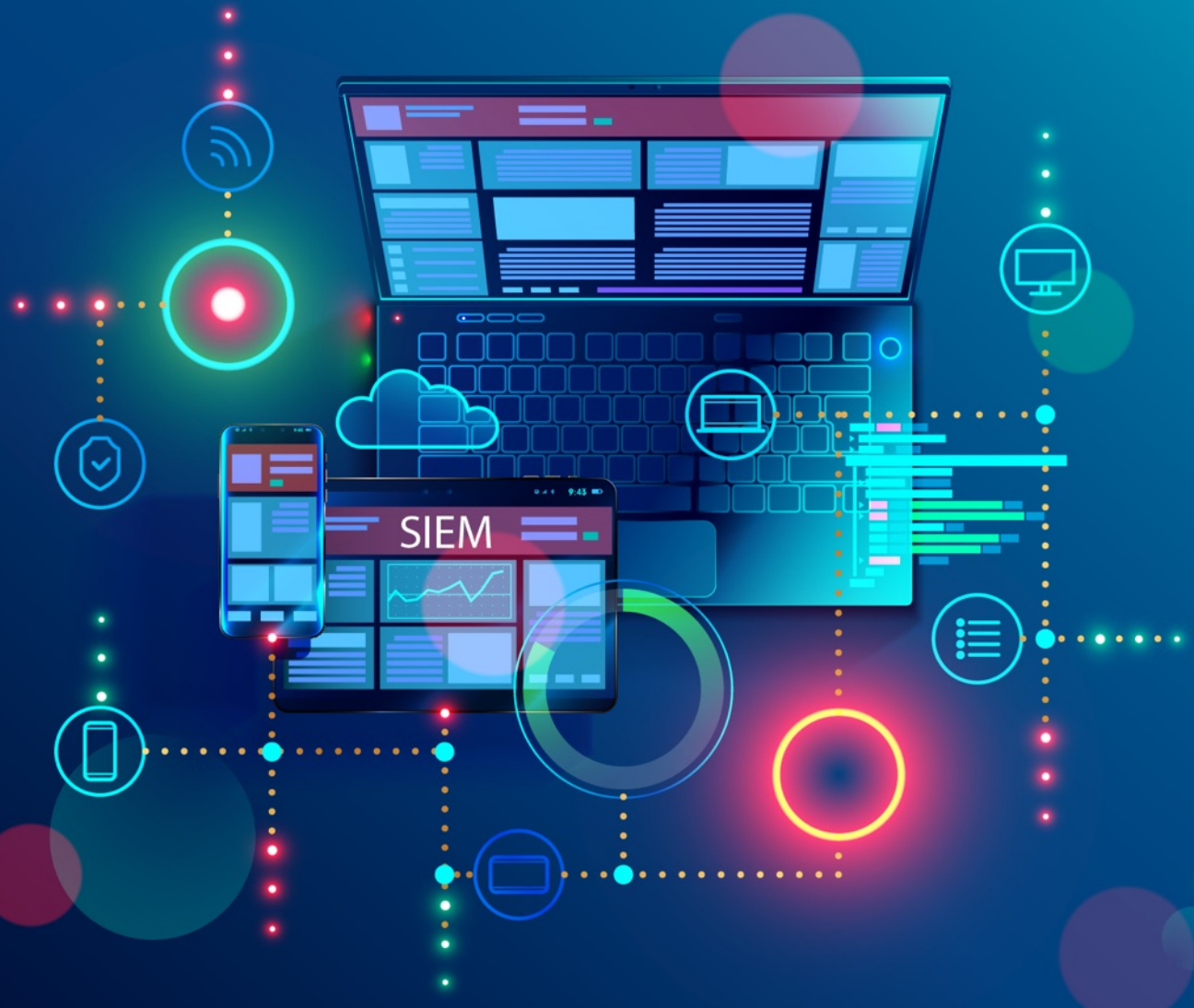
A Security Information and Event Management (SIEM) tool is a master tool in any information security department's arsenal. A general overview of how a SIEM works is that the device receives information from all systems on the environment. Then, it combines all of this information into a story, which can alert and provide all of this information to incident handlers in near real-time.

In more general terms, a SIEM is like a spy, continually listening to crucial pieces of information from everyone around them while taking notes. Then it analyzes the notes received to piece together a larger story of the activities occurring. Once enough information has been received and checked for correctness, the spy reports back to headquarters and provides this information as an alert to its superiors.

In more technical terms, all devices on a network, whether that be cell phones, tablets, printers, fax machines, routers, switches, computers, laptops, servers, or any smart device, all create something called machine data.

This data contains every piece of information that a device or software on any machine is performing every second. All of this data is stored inside of logs, which are saved locally to devices. This data saved inside of these logs is not always structured or easily readable by the human eye.

SIEMs, through the implementation of a local application or other protocol forwarding methods, forwards and ingests this data into the central SIEM console. After ingestion, data is restructured, correlated, extracted, and sorted based on timestamps.



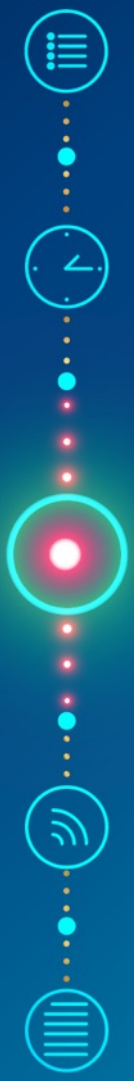
IF A SIEM SEARCH FINDS AN ATTACK

Following ingestion and data transformation, most modern-day SIEMs provide features that allow for automatic and real-time searches to occur. Depending on what tool is being utilized, this could be called rules or correlation searches.

These searches are always updated and contain information about the latest and greatest breaking threats and threat actors' techniques across all industries. These searches run in real-time or near real-time to continually check all incoming logs for malicious activity.

After a search has caught evidence of an attack inside of an environment or hitting the environment, the search or rule can perform several automated actions. These include creating tickets for the incident handlers, sending emails with full log activity of the threat that occurred, or, through multiple APIs, sending automated blocks to different security devices that utilized throughout the network.

Once these alerts and searches send out notifications, the incident handlers can quickly perform the following threat identification process:



Quickly gather all logs from one location.

Analyze the time of attacks.

Understand if this attack is still actively occurring.

Potentially shut down any active connections based on an API or scripts implemented in the SIEM.

Quickly export all data to a report or dashboard to provide senior leadership an overview in a matter of seconds.

HOW CAN A SIEM HELP?

Now that we understand how a SIEM works, there are several benefits through the use of a SIEM inside any organization. Several of these benefits are as follows:

Alleviate Struggles With Understaffed Employees

Through the use of a SIEM tool that is tuned configured and correctly sized for the organization utilizing it. Organizations can improve monitoring and perform threat hunting capabilities that would generally require an entire team to organize and perform. Alleviating the strains of multiple salaries for both the threat hunting individuals and managers and alleviating the issue of trying to find these new threat hunter employees in the middle of a workforce shortage.

Assist in Keeping Threat Knowledge Up To Date

With a SIEM tool, incident handlers and threat hunters don't always have to worry about spending every other minute they are not working, reviewing the latest news, and reports on indicators of compromise. Although they still should, it is not mandatory due to automatic updates and rollouts of new revisions to rules and correlations searches inside of the SIEM. Since all of these rules and searches are pre-configured based on the latest most significant information created from multiple threat feeds. In turn, this can alleviate the stress caused by the lack of time that your incident handlers are encountering by allowing them to focus more clearly on all of the incidents they are already working.

Provide Full Visibility Into Any Environment

Outside of the difficulties that occur from staffing and knowledge, modern-day SIEMs provide immense wealth to the overall visibility and monitoring of the environment they are in, due to their nature. Since SIEMs need to monitor everything to create the bigger picture of attacks, this forces any security engineers working inside of the environment to implement ingestion methods to tap into every device and creates full visibility that was not previously implemented, down to a granular level.

Dashboarding and Reporting

With the ingestion of all data into one central location, all data can transform into dashboards. These dashboards contain information graphs, pictures, trendlines, big number pictures, geographical maps, or any method that is chosen to display any data. This allows log data to be displayed and easily comprehended during meetings or conferences to individuals with any varying level of technical knowledge.

Benefits Outside of the Security Department

SIEMs can also be retrofitted to provide granular information to additional departments outside of the security team as well. Since all systems generate log data, application teams, sales teams, or human resources departments, receive massive benefits from a SIEM solution as well, due to the nature of what a SIEM does on the backend with monitoring and analysis.

Some of these uses cases are the following;

- Monitoring customer-facing applications for errors to quickly correct or handle breaks in a timelier matter.
- Monitoring user traffic on websites to understand where users or customers are navigating to the most.
- Monitoring timestamps on building badge access, for HR to view if employees are accurately filling out their timesheets.
- Monitoring network statistics to understand if any bottlenecks are occurring inside of the environment.

Through the implementation of a SIEM solution in any environment, security teams can multiply their efforts to discover any level of malicious activity that is potentially threating the organization, along with providing full data and assistance to any team that utilizes devices or technology for their business objective.