# OPTIMIZING SIEM
## WITH LOG MANAGEMENT

graylog

# TABLE OF CONTENTS

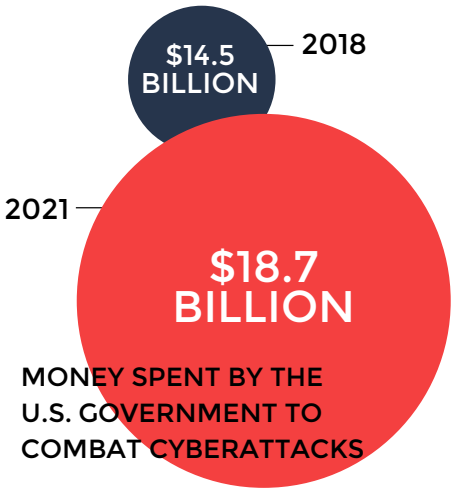
# INTRODUCTION

Security Information and Event Management (SIEM) solutions have typically been focused on alerting organizations of issues that applications and network hardware identify. When those alerts go unheeded or don't deliver next steps on how to mitigate threats, SIEM can become an expensive
and ineffective tool.

In this eBook, we'll explore how to make the most of SIEM with log management tools that enhance capabilities and strengthen security.

# NAVIGATING THE THREAT LANDSCAPE

**Today's cyberattacks are complex and effective. In the most sophisticated nation state cyber attack, IP hopping Nobelium used spear-phishing to prompt user actions on multiple hidden layers of executions, ultimately deploying DLLs that allowed action-on objectives.**




Source: Security Forward

Tmobile's data breach began with an unprotected router as the entry point that was used to hack servers and steal nearly 100 million customers' sensitive data. Though these attackers targeted large organizations, their methods leave businesses of any size at risk.

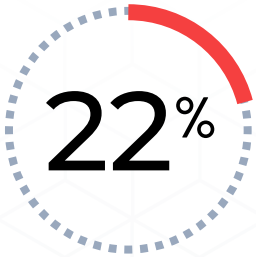
Data breaches occur by various means, so predicting how attackers will exploit vulnerabilities to gain system access proves difficult. For example, circumvention of Crypto.com's 2FA authenication allowed hackers to access 500 wallets, stealing $18M.

**$223.8B**
**EXPECTED GLOBAL SPENDING ON CYBERSECURITY**
Source: Canalys

And Ronin learned to never compromise security standards when they rolled back protocols to allow servers the ability to handle their growing gamership, resulting in the theft of $600M

in cryptocurrencies. Even Business Email Compromise (BEC), a simple attack involving a threat actor posing as a business contact requesting money and/or sensitive data, is as effective as it is common.

Managed Security Service Providers (MSSPs) can enhance companies' security posture by providing outsourced security monitoring and management for devices and systems including SIEMs. Available around the clock, MSSP services can lessen the need for hiring security experts, simultaneously lowering costs and increasing security.




Network intrusions and data breaches from compromised user credentials

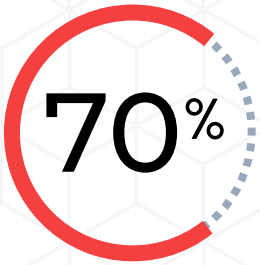
Source: IBM

**Logs, the messages almost every computing device generates, show details on how and when the device was used, as well as attempted and successful logins. Also known as event logs, audit travels, or audit records, logs are typically text-based and may be stored on local or remote servers. A proper log analysis can reveal the nature of threats, from where the attacker targets to methods used in attempting to breach security.**

But, whether via MSSP or not, the traditional approach of using SIEM to bridge systems and logs and monitor their data in one place doesn't fully identify an entire threat or provide remediation tactics. More widespread visibility is needed to act on the information SIEMs do provide.

To this end, organizations and MSSPs are now rounding out their SIEM approach with log management products that collect, process, analyze, and visualize data surrounding a suspected threat.

Organizations using only SIEM could be missing some valuable information, since SIEM-only vendors often adhere to a pricing model that restricts the level of log detail that an organization can collect. Working with this constraint is not only expensive, but also extends vulnerability as threat investigators must wait longer to correlate and search.




Rise in Data Breaches Globally in late 2022

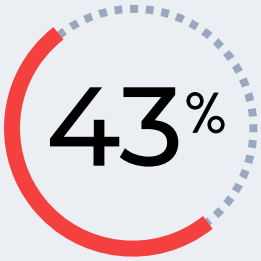
Source: Infosecurity Magazine

# CYBERATTACK FACTS

**69%**
MALWARE DELIVERED BY EMAIL
Source: HP Wolf Security Report


INCREASE IN CYBERATTACKS IN 2022
Source: Forbes

**$9.4M**
DATA BREACH COST FOR THE AVERAGE COMPANY
Source: IBM




AMOUNT OF ATTACKS AIMED AT SMALL BUSINESSES
Source: Fobes

**316K**
NEW MALWARE SAMPLES PRODUCED EACH DAY
Source: Atlas VPN

THE WORLD WILL NEED TO CYBER PROTECT
**200 ZETTABYTES**
OF DATA BY 2025.
Source: CyberSecurityVentures.com

GLOBAL CYBERCRIME DAMAGE PREDICTED TO HIT
**$10.5T**
ANNUALLY BY 2025.
Source: CyberSecurityVentures.com

# ABOUT LOGS

Log management solutions allow organizations to conduct further incident investigation and deeper analysis on SIEM alert details. By capturing all types of log and event data in one central location, these solutions provide granular search capabilities and actionable remediation steps.

# THE STATE OF SIEM

The typical SIEM approach hasn't allowed for deep analysis of identified issues. though modern SIEMs typically include.

- **Real-time monitoring**
- **Correlation of events**
- **Parsing and log normalization**
- **Anomaly detection**
- **Long-term log storage**
- **Reporting**
- **SOAR integration**

With a growing focus on providing products and services as a closed ecosystem, SIEM solutions are becoming more complex and time-consuming to manage. Users may become overwhelmed by receiving too many notifications and reviewing false positives, ultimately leading to ignored alerts.

In the end, organizations may find themselves susceptible to threats while paying for a solution they don't effectively use. Organizations that want to avoid this situation need to choose a scalable log management tool that fits their needs in price and performance to complement their SIEM product.

**In the end, organizations may find themselves susceptible to threats while paying for a solution they don't effectively use.**

# THE PATH TO SIEM SUCCESS


Source: Accuvant

# IT BANDWIDTH

**IT teams tend to be staffed rather lean for the large realm of responsibility they have. They must implement tools to help them log and monitor their network and oversee these processes alone.**

IT teams need to be trained in using SIEM solutions to get the most out of them, yet these teams are often so small that only one member becomes the SIEM expert, leading to a single point of failure when a threat looms.

To further complicate the IT issue, because of cost constraints and problems with operating at scale, SIEMs tend to be licensed to capture only a subset of data to be monitored. When SIEM data is limited, you don't get a complete picture of threats and vulnerabilities. This is especially problematic now that SIEMs typically include Anomaly Detection ML/AI, which needsa complete picture to determine what is "typical" behavior and what is anomalous.

This need for a wide scope applies to threat intelligence feeds also. These feeds help organizations learn from others' past security incidents via third-party streams of threat patterns and artifacts that are automatically updated when new threats emerge. The streams target intelligence feeds to get their data. A target feed scope should be wide enough to let SIEM deliver meaningful insights. If the feed scope is too narrow, the SIEM doesn't see enough to recognize if your systems are truly at risk. Yet even a wide target feed scope doesn't provide the complete threat picture either, as IT teams still lack next steps for remediation.

An uneven ratio of IT tasks to workers plus SIEMs that aren't pulling their weight equals an unclear vision of system vulnerabilities and potential threats. With a shortage of

## TYPICAL TARGET FEEDS:

- **IPs and firewalls**
- **Endpoints**
- **Active directory**
- **Operating systems**

security resources, MSSPs have become popular solutions. MSSPs overseeing SIEM could ease burdens for IT teams, but SIEM customers would still receive alerts with no remediation plans.

Though helpful, MSSPs don't address the lack of specific and detailed information necessary to investigate and remediate threats that SIEMs typically don't provide.

## TARGET FEEDS TO SIEM

Malicious activity from Domains, Hashes, and IPs

# HOW GRAYLOG HELPS

## For security and compliance purposes, organizations tend to store logs with the intent of reviewing them later as they prepare for or react to a security incident.

Although logs can help identify security weaknesses, when massive amounts of logs are generated daily, there is simply too much information to review, letting threats slip by. This scenario is when adding a log management solution to SIEM becomes vital.

Log management alone doesn't provide real-time insights on your network security, but when SIEM and log management are combined, you gain more information for SIEM to monitor.

With their combined capabilities, you can do even more:

- **Begin threat investigation with complete data**
- **Analyze deeper to learn threat origin and path**
- **Inform remediation tactics**
- **Fortify network security against future threats**
- **Meet a longer list of compliance requirements with a single tool**
- **Quickly respond to audit requests**

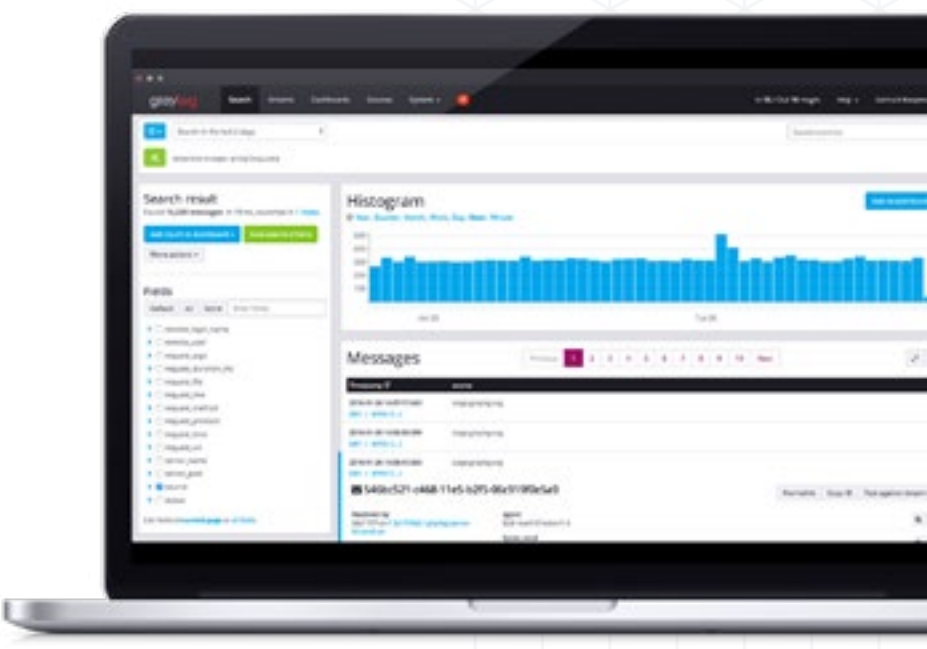
Powerful granular search capabilities provide the exact combination of data necessary to examine threats. The unified Graylog Security interface immediately gives users relevant views of their data so that any analyst can aggregate data from multiple sources, initiate a search across multiple parameters, analyze the data, visualize the data, and report on and save that search, with no system administrators or tool-specific training all

When SIEM and log management are combined, you gain more information for SIEM to monitor.

from one screen. Eliminating the need to jump from screen to screen is significantly more efficient, saving considerable time and ending frustration.

Graylog Security is built for a new wave of data explorers and threat hunters with a focus on providing our users the best analyst experience available today. Users are generally not sure of the extent or breadth of an issue prior to the investigation, but Graylog allows users to explore data without having a complete plan prior to engaging in the search. The power of Graylog Security's search lies in its ability to expand and reveal more information. It delves deeper into search results, exploring data further to find the right answers.

In addition to providing industry-leading threat hunting and incident investigation capabilities, Graylog Security provides in-app access to a number of helpful tools like Sigma Rules and threat intelligence feeds. The Sigma Rules open source repository contains over 2500 alert rules for near-instant improvement to your security monitoring, while threat intelligence feeds make it easy to see if you are dealing with a known bad-actor from a simple right click on a key data point.



# CONCLUSION

A SIEM's goal is to alert users to potential threats but can be ineffective without remediation suggestions or intrusive notifications. Paired with the right log management tool, a SIEM can help you understand where and how a threat began, the path it took, what it impacted, and how to fix it. A combination of log management and SIEM can also relieve burdens for IT, as technology enables real-time security analysis, removing the need to learn numerous security products. The sooner IT groups implement these solutions, the better, so organizations get maximum protection with minimum risk.

# GET STARTED TODAY

See **Graylog Security** in action!

# ABOUT GRAYLOG

**Graylog is a game-changing log management and cybersecurity solution** that offers robust, cost-effective ways to protect your organization against cyber threats. Using AI/ML, security analytics, advanced log management, and intelligent alerting, Graylog enables you to stay ahead of threats. Unlike traditional SIEM solutions that are complex and expensive, Graylog is easy to use and affordable, giving you a superior cybersecurity experience.

Graylog also addresses the needs of IT Ops and DevOps teams by offering centralized log management, making it easy to collect, index, and analyze log data from any source. This ensures IT teams can quickly detect and respond to issues, allowing them to deliver better performance and reliability to their users. Whether you're looking for a comprehensive cybersecurity solution or a way to streamline your IT operations, Graylog has the tools you need to succeed.

graylog

www.graylog.org
info@graylog.com