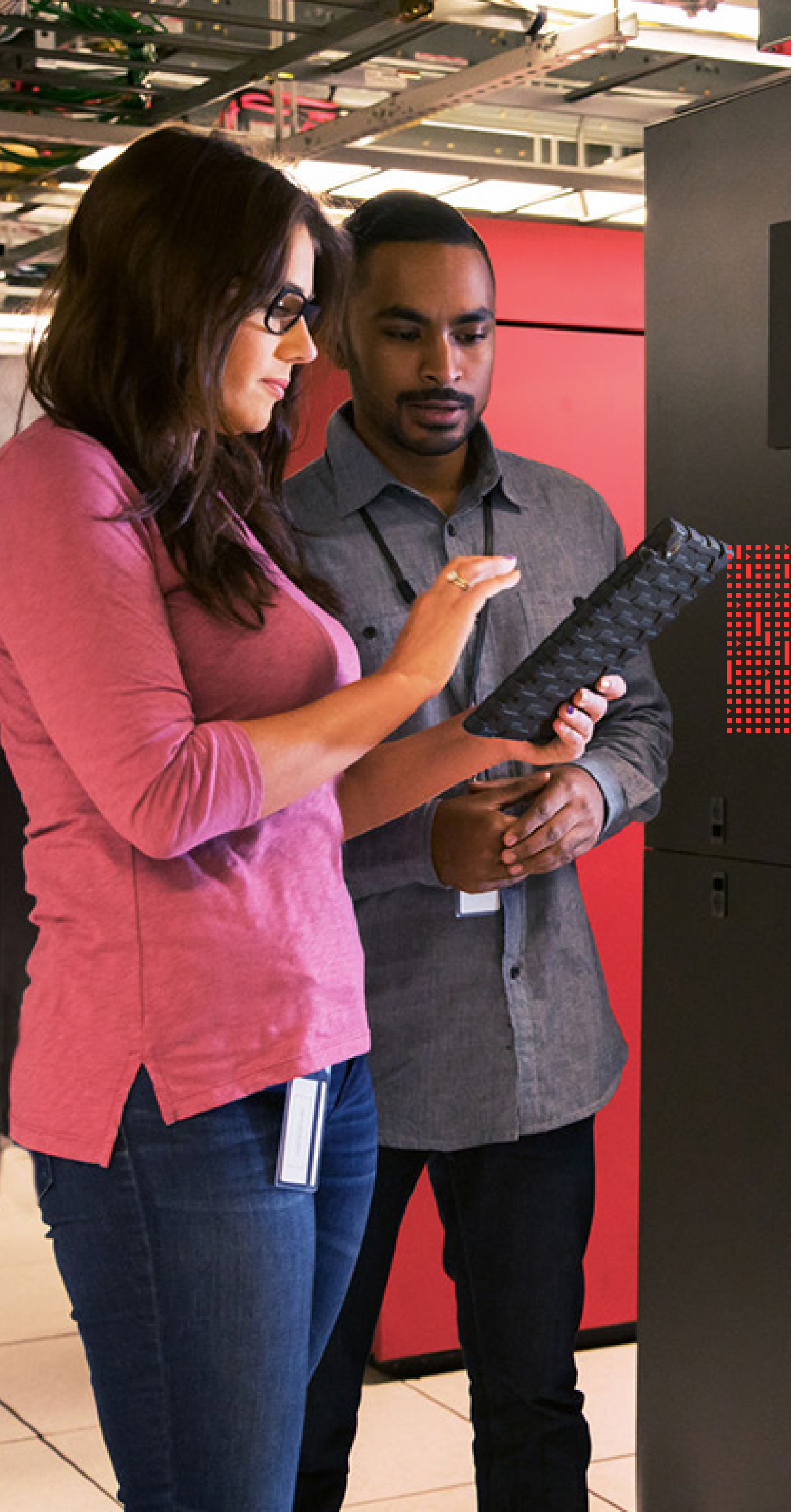
graylog

OPTIMIZING SIEM WITH LOG MANAGEMENT

```
                     :33:20 -0800     230.208.239.28     hriley6u       134.102.154.238
2016-11-02 16:23:43 -0800     206.109.204.72     wwoods6c       235.243.22.90
2016-11-02 22:21:52 -0800     63.14.148.248      kbishop6r      Log events: 203.8
2017-01-02 10:06:11 -0800     185.67.8.223       ahowell6n      Log events: 203.8
2016-11-13 11:01:25 -0800     59.29.50.63        abishop7z      c:\Windows\Temp\p
2016-11-16 02:53:23 -0800     70.159.214.117     llong4w        95.88.12.95
2017-01-08 07:10:02 -0800     160.163.182.160    rmorgan5i      Log events: 203.8
2016-12-18 04:43:35 -0800     15.112.139.10      cmitchell7f    c:\Windows\System
```

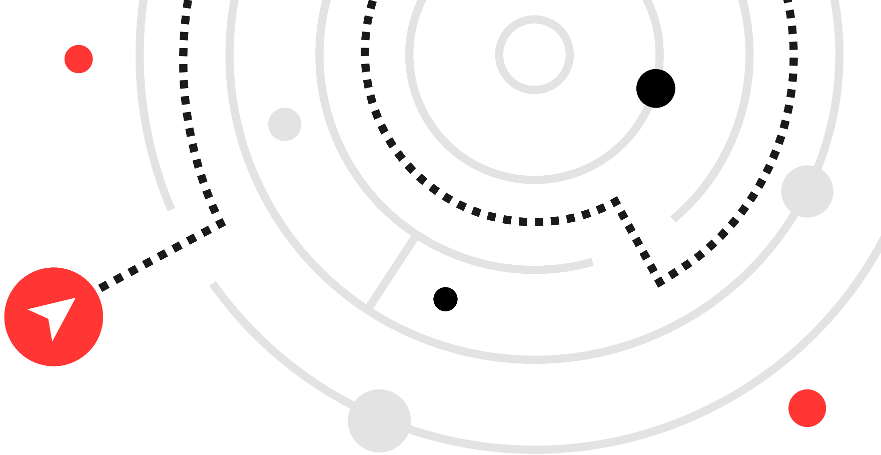
CONTENTS



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.



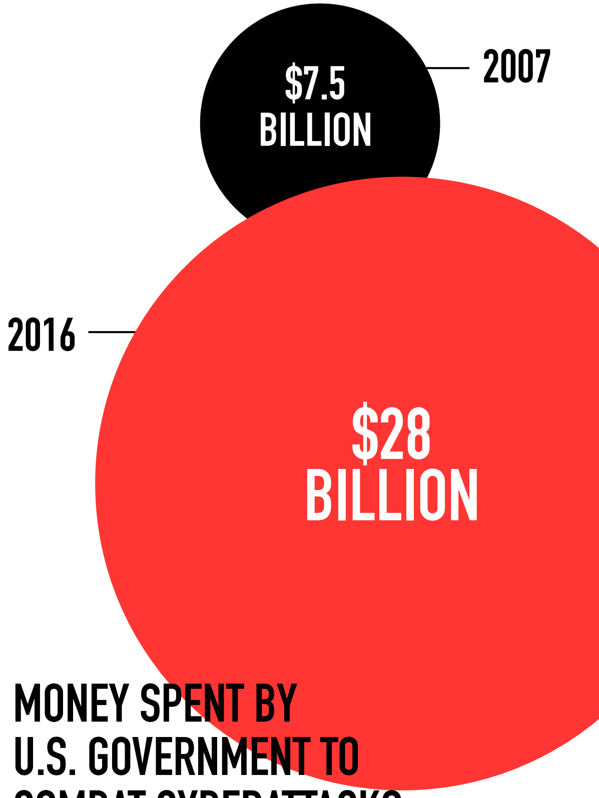
NAVIGATING THE THREAT LANDSCAPE

Today's cyberattacks are complex and effective. 2017's infamous WannaCry ransomware attack found more vulnerable hosts by scanning each infected machine's connected LANs and WANs, automating machine infection and file encryption.

Uber's data breach began in a GitHub repository that attackers used to gain login credentials, leading them to user data they held for ransom. 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, a third-party vendor was responsible for a server misconfiguration that led to a major Verizon breach.

And a weak encryption algorithm caused a leak of approximately 28 million user records for Taringa, a social network based in Argentina. 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.



MONEY SPENT BY U.S. GOVERNMENT TO COMBAT CYBERATTACKS

Source: The Best VPN

NETWORK INTRUSIONS AND DATA BREACHES FROM COMPROMISED USER CREDENTIALS

Source: Microsoft

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.

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.

ABOUT LOGS

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.

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.

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.

CYBERATTACK FACTS

1 IN 131

EMAILS CONTAIN MALWARE

Source: Symantec

$3.8M

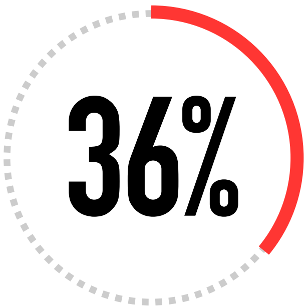
DATA BREACH COST FOR THE AVERAGE COMPANY

Source: Microsoft

230K

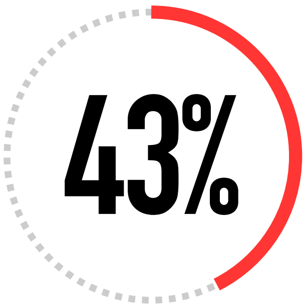
NEW MALWARE SAMPLES PRODUCED EACH DAY

Source: Panda Security



INCREASE IN RANSOMWARE IN 2017

Source: Symantec



AMOUNT OF ATTACKS AIMED AT SMALL BUSINESSES

Source: Small Business Trends

THE STATE OF SIEM

The typical SIEM approach hasn't allowed for deep analysis of identified issues, though recent SIEM products have included new features:

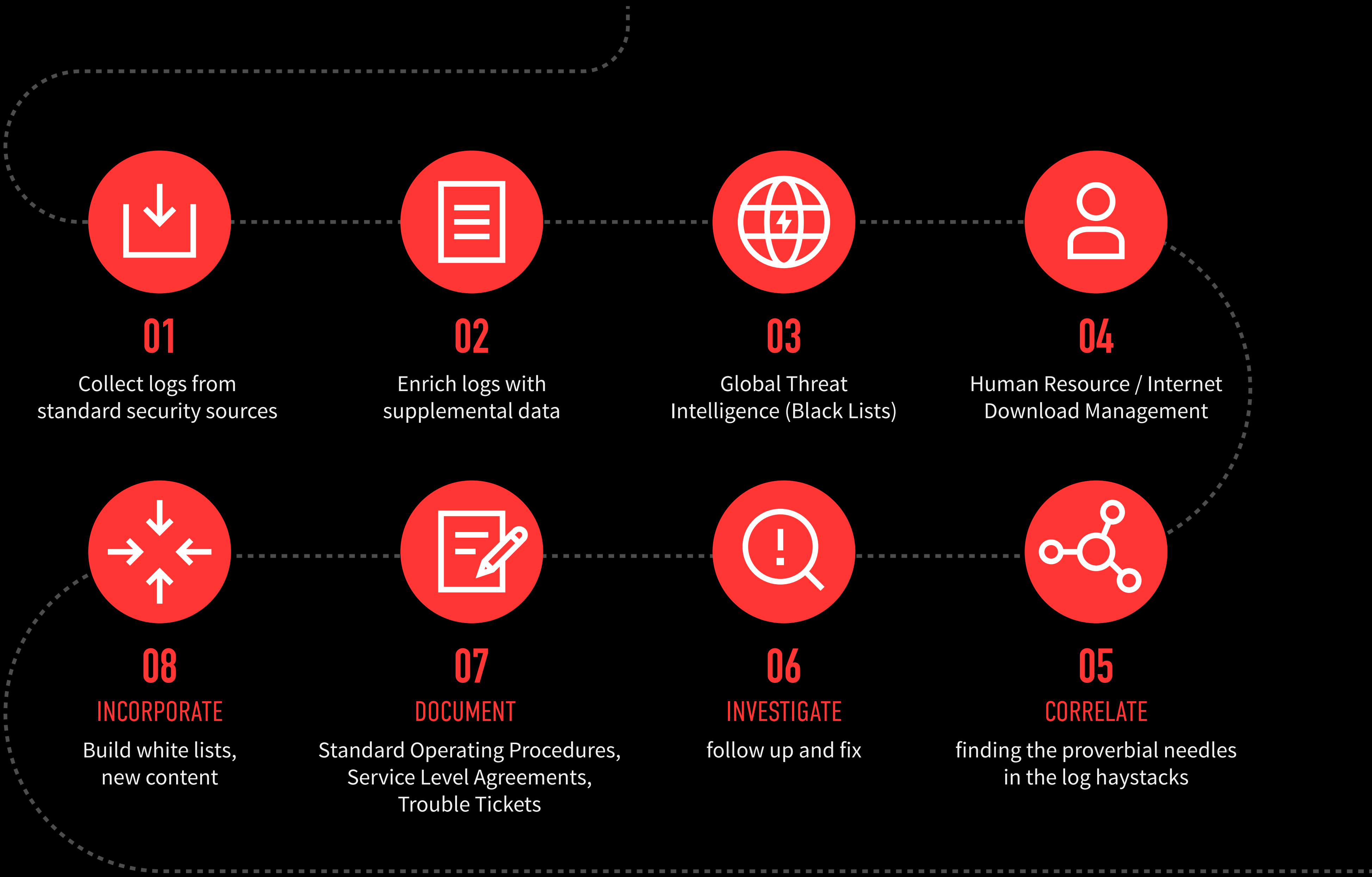
- Real-time monitoring
- Correlation of events
- Parsing and log normalization
- Anomaly detection
- Long-term log storage
- Reporting

These emerging SIEM products now collect logs across security/network devices, Microsoft's Active Directory, operating systems, databases, servers, and applications. 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



01
Collect logs from standard security sources

02
Enrich logs with supplemental data

03
Global Threat Intelligence (Black Lists)

04
Human Resource / Internet Download Management

05
CORRELATE
finding the proverbial needles in the log haystacks

06
INVESTIGATE
follow up and fix

07
DOCUMENT
Standard Operating Procedures, Service Level Agreements, Trouble Tickets

08
INCORPORATE
Build white lists, new content

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 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

TYPICAL TARGET FEEDS:

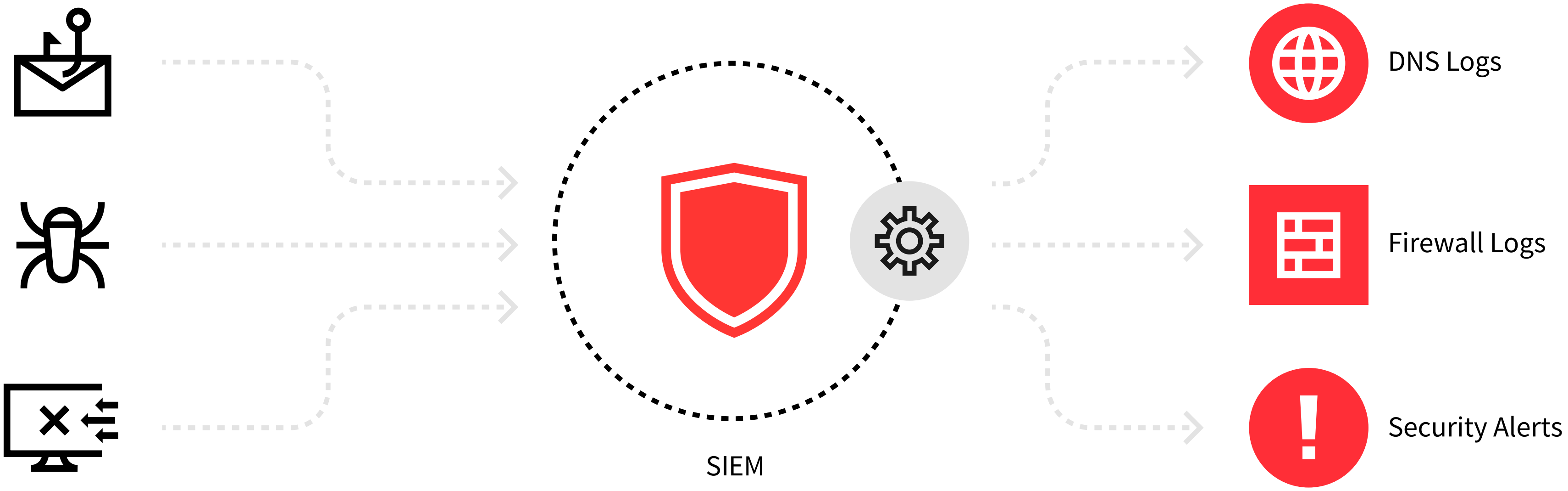
- IPS and firewalls
- Endpoints
- Active Directory
- Operating systems

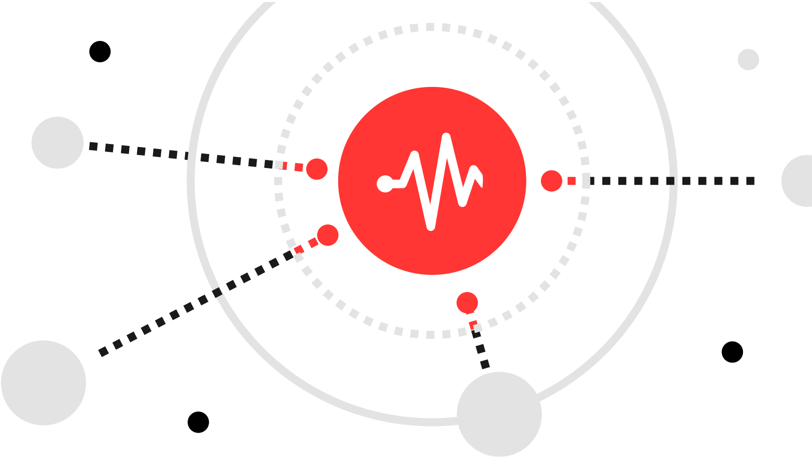
and potential threats. With a shortage of security resources, MSSPs have become popular solutions. MSSPs overseeing SIEM could ease burdens for IT teams, but SIEM customers would still receive alerts with no remediation plans.

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:

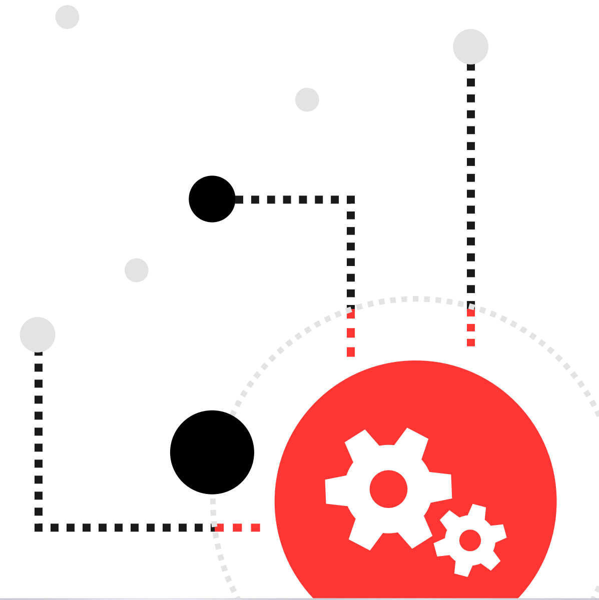
- Begin threat investigation with complete data
- Analyze deeper to learn threat origin and path
- Inform remediation tactics
- Fortify network security against future threats

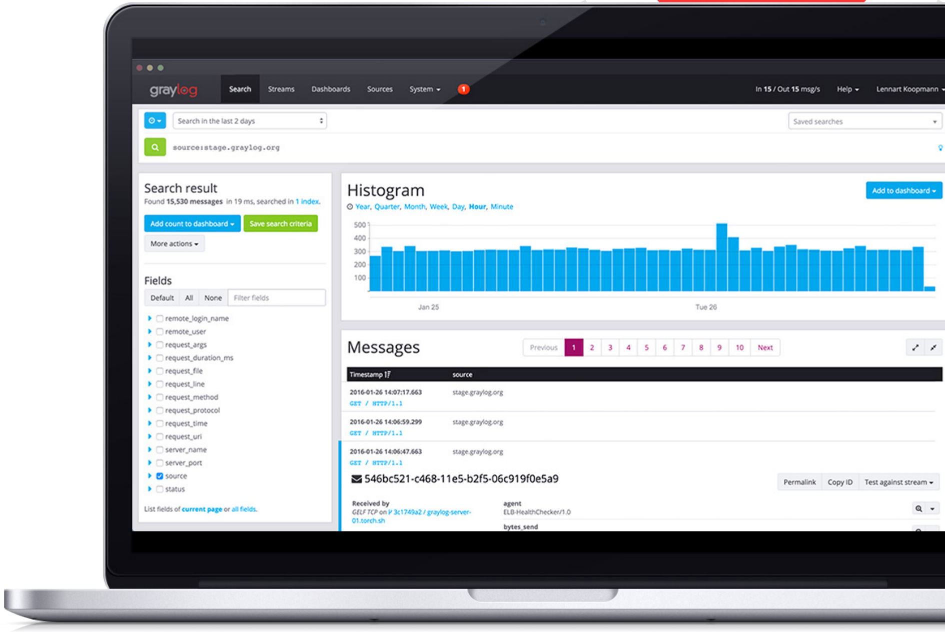
WHEN SIEM AND LOG MANAGEMENT ARE COMBINED, YOU GAIN MORE INFORMATION FOR SIEM TO MONITOR.

Powerful granular search capabilities provide the exact combination of data necessary to examine threats. The unified Graylog 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 from one screen. Eliminating the need to jump from screen to screen is significantly more efficient, saving considerable time and ending frustration.

Graylog is built for a new wave of data explorers and threat hunters. 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'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.

Finally, the design of Graylog's data storage and retrieval architecture inherently allows for multi-threaded and distributed search across the environment. Each search uses multiple processors and multiple buffers on a single machine, then multiplies that threaded search across the number of participating nodes in the cluster. This approach gives much faster results, which is crucial when investigating threats that could turn into major cyber incidents.





Search in the last 2 days

```
source:stage.graylog.org
```

Search result

Found 15,530 messages in 19 ms, searched in 1 index.

Fields

- ☐ remote_login_name
- ☐ remote_user
- ☐ request_args
- ☐ request_duration_ms
- ☐ request_file
- ☐ request_line
- ☐ request_method
- ☐ request_protocol
- ☐ request_time
- ☐ request_uri
- ☐ server_name
- ☐ server_port
- ☑ source
- ☐ status

List fields of current page or all fields.

Histogram

Messages

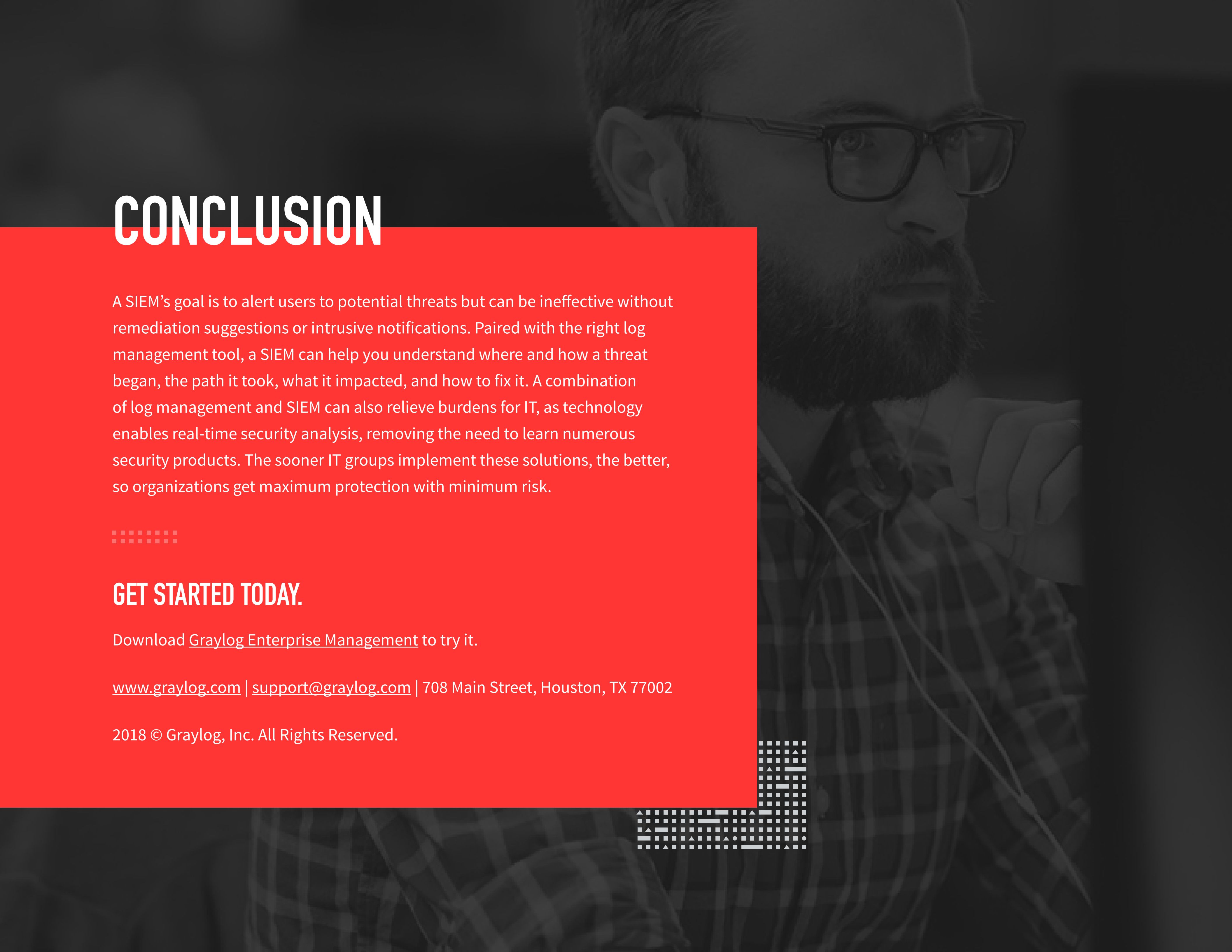
Timestamp	source
2016-01-26 14:07:17.663 GET / HTTP/1.1	stage.graylog.org
2016-01-26 14:06:59.299 GET / HTTP/1.1	stage.graylog.org
2016-01-26 14:06:47.663 GET / HTTP/1.1	stage.graylog.org

546bc521-c468-11e5-b2f5-06c919f0e5a9

Received by
GELF TCP on 3c1749a2 / graylog-server-01.torch.sh

agent
ELB-HealthChecker/1.0

bytes_send



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.

Download Graylog Enterprise Management to try it.

www.graylog.com | support@graylog.com | 708 Main Street, Houston, TX 77002

2018 © Graylog, Inc. All Rights Reserved.