FIREEYE

THE SIEM THAT CRIED WOLF

Only ONE out of thousands of alerts may matter. But can today's security information and event management (SIEM) products tell a false alarm from a real threat?

Alert Overload

Every day, IT security teams around the world are inundated with an average of 10,000 alerts—far more than they have resources to investigate.[1] What's worse, the SIEM products used to centralize this data are of little help in sorting trivial alerts from important ones.

Few organizations have the resources to chase down every alert, and **responding to each one is impossible**.

10K+
alerts received by most security operations centers daily[1]

"Off"
Most teams turn off auto-blocking to cope

67%
of organizations judge their response rate as ineffective[2]

In a 2013 major attack on Nieman Marcus, 60,000 alerts—a huge number—were related to the breach, but that represented only 1% of the total alert volume for that period.[3]

Danger Rising

A FALSE SENSE OF SECURITY

Security teams often think high alert volumes must mean their tools are catching the worst threats—but in most cases that simply isn't true.

97%
of worldwide security systems have been breached[4]

False positives represent a large share of alerts, resulting in desensitized teams who may view new alerts as a nuisance rather than a warning. Meanwhile only 29% of alerts are investigated—leaving a wide gap for possible threats.[2]

A single security event can trigger hundreds of alerts; a coordinated attack can generate tens of thousands.

A Highly Complex Problem

Which alerts merit attention? The answer isn't so simple. Most cyber security tools don't distinguish between everyday malware and advanced targeted attacks, which play out over multiple steps and require a more sophisticated response.

ADVANCED ATTACKS

1	2	3	4	5	6
INITIAL RECONNAISSANCE	INITIAL COMPROMISE	FOOTHOLD ESTABLISHED	PRIVILEGES ESCALATED	INTERNAL RECONNAISSANCE	MISSION COMPLETE

PREVENTION — Most security solutions focus on detecting and preventing the early phases of an attack.

RESPONSE — If an attack evades early detection and progresses to a later stage, organizations are especially vulnerable.

Advanced targeted attacks can enter an organization as disparate pieces, which later combine to form a malicious executable file.

Teams that can't detect well-orchestrated attacks also fail to filter out trivial alerts, prioritize alerts and consolidate related alerts.

A security operations platform helps teams from prevention to response, revealing how seemingly unrelated activity connects in coordinated attacks.

A New Direction

Traditional SIEMs can aggregate alerts and other security data, but to fight today's advanced attacks, organizations need a more dynamic solution. A **security operations platform** goes beyond a legacy SIEM to deliver complete visibility and help teams take control of incidents—from alert to fix.

	TRADITIONAL SIEM	SECURITY OPS PLATFORM
Advanced SIEM centralizes security data with advanced user behavior analytics to monitor user patterns, detect non-malware-based intrusions, and manage application access	✕	✓
Security orchestration automates tasks such as containing endpoints, blocking IP addresses, and searching against malware databases	✕	✓
Workflow management tools help track work among analysts, manage cases, and automate investigative tasks	✕	✓
Contextual intelligence provides greater visibility and context of threat actors and their tactics, techniques and procedures, helping determine which threats present the biggest risk	✕	✓
Third-party tool integration connects and enhances individual security solutions throughout an organization with the ability to ingest outside events and logs	✕	✓

ONE

To download the full report, visit
www.FireEye.com/next-gen-siem

1 John E. Dunn (May 14, 2014). Average US business fields 10,000 security alerts per day, Damballa analysis finds.
2 Ponemon Institute (March 16, 2016). The State of Malware Detection and Prevention.
3 Bloomberg (February 24, 2014). Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data.
4 FireEye (May 2014). Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model.

FIREEYE