WHITE PAPER

FireEye®

Taking Control of Security Operations

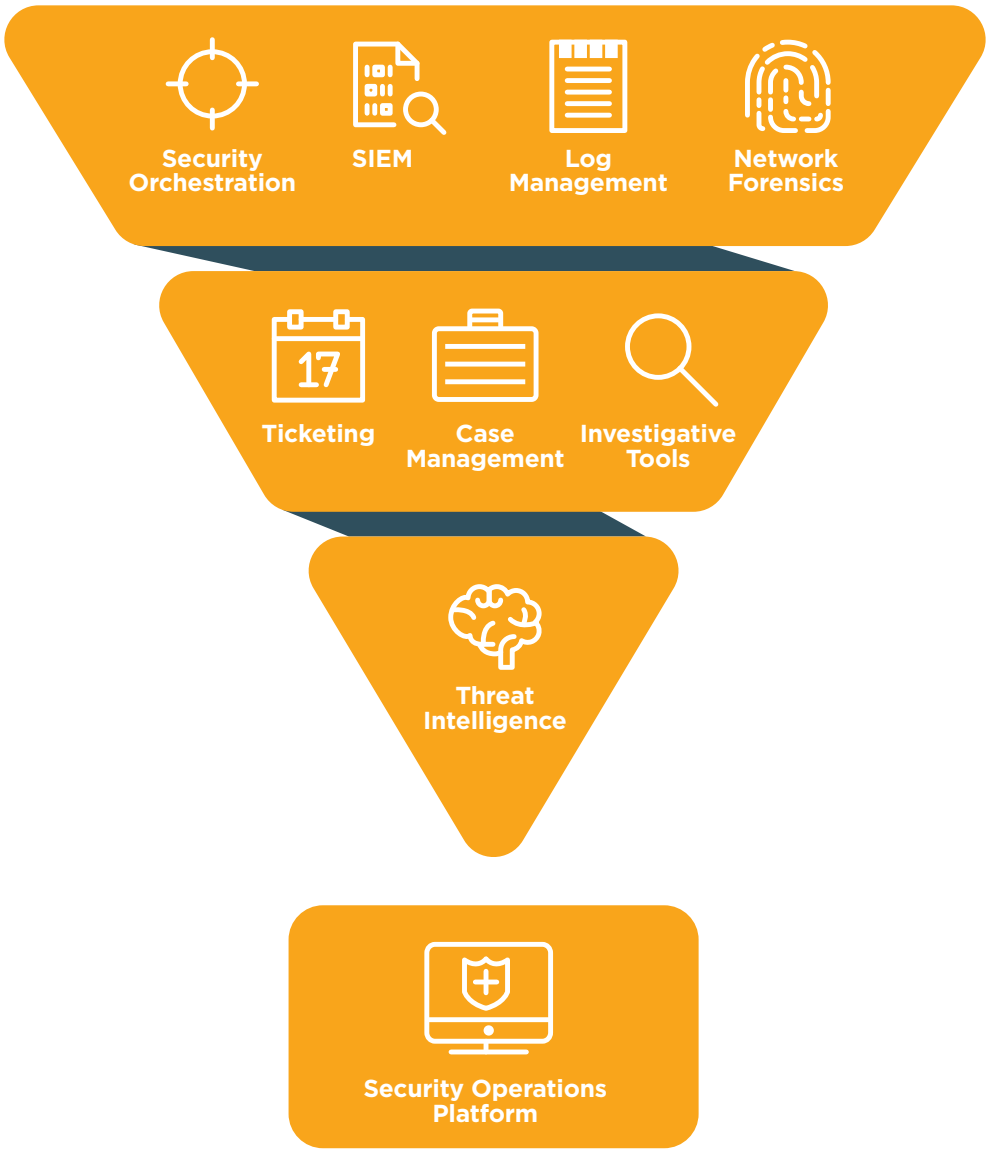
Making unified security accessible to every company

A New Way Of Thinking About Security Operations

In an environment where new threats appear almost daily, many companies are making the smart choice to invest more money and effort into improving their security posture. Their reasoning is simple: If an organization — big or small — has what attackers are after, whether it's information, money or simply disruption, sooner or later it will become a target. The burden of building an effective security ecosystem is particularly heavy for companies that have limited resources. They're exposed to the same level of risk as top enterprises, but lack the same level of funding and human capital.

Financial limitations aside, buying a new appliance or subscribing to a service rarely yields the improvement that companies seek. Adding point products often leads to more complexity, additional headcount, error-prone manual work and potentially greater exposure to risk if new security measures are not implemented correctly. Newer products have been surprisingly slow to address these acute, well-known customer needs.

Fortunately, a more holistic approach to cyber security is emerging.



Security Operations Platforms

One innovative response to operational challenges is the security operations platform. Such a platform acts as the mission control for the security operations center (SOC). It is designed to integrate and automate security operations, allowing security teams to stop threats faster while reducing operational costs. But not every solution is created equal.

For example, security information and event management (SIEM) solutions try to reposition themselves as security operations consoles while offering only limited tactical advantages. They will aggregate alert volume without contextual analysis or automation, which creates a bigger problem for SOC analysts.

This white paper examines the essential capabilities of a security platform and offer some points to consider when selecting a security vendor. No innovation spares a CISO from the need to have top technologies, processes and human capital in place. The promise of a security operations platform is that it allows companies to have a unified security operations experience. It heralds a much more efficient, simpler — and ultimately, safer — future for organizations' computer networks.

Visibility

Visibility refers to an organization's ability to detect, alert on and assess the impact of attacks. This includes visibility into the threats an organization faces and the ability to understand, which ones present the greatest risk. Effective security demands visibility; blind spots in infrastructure can lead to major problems.

As the cyber threat landscape evolves, new visibility gaps can emerge in a network. For example, today's organizations need visibility into vendor connection points, subsidiary organizations and other interconnections that didn't exist in the past.

The burgeoning use of cloud infrastructure also introduces vulnerabilities and visibility gaps. Organizations that use a public cloud to run critical business operations and store confidential data, where user credentials and configuration management are difficult to centrally maintain, make their data security more difficult.

To improve visibility, a security operations platform should quickly identify breaches, proactively identify vulnerabilities, and centralize and synthesize security data to anticipate attackers.

Quickly identify that a breach has occurred

Organizations naturally want to prevent attacks. But as cyber attackers become more sophisticated at exploiting both technological and human vulnerabilities, it's inevitable that breaches will occur. The question becomes: How long will those breaches last? The global median time from compromise to discovery (dwell time) remains high at 99 days, allowing threat actors plenty of time to steal sensitive information and even remove evidence of a breach.[1]

A security operations platform should augment prevention with quick detection so that organizations can understand the malware being used, quickly assess exposure and damage and feed that knowledge back into the overall security operations function. In a world where every minute of a breach costs hundreds (or thousands) of dollars, a security operations platform should be able to detect a breach in a matter of minutes, not hours or days.

Make sense of your alert volume

Organizations also need the ability to identify the real threats among huge volumes of alert noise. Of the 17,000 raw malware alerts an organization receives each week, only 19% are considered reliable and only 4% are investigated. Bad alerts are not only noisy; they're also expensive. On average, the time an organization wastes responding to inaccurate and erroneous intelligence can cost $1.27 million annually.[2]

Alerts without the appropriate context make it hard for security analysts to make educated and informed decisions. An effective security operations platform surfaces and analyzes threats and automates alert validation to eliminate false positives. It also allows security teams to prioritize threats hidden in existing alert volume so they can act on them quickly.

Understand and anticipate attacker behavior

The efficacy of traditional signature-based products has fallen sharply in the last few years. This is the best testament to attackers' ability to morph malicious code to avoid signature-based detection approaches. It also signifies their gradual move away from malicious code towards theft of stolen credentials and techniques that don't involve any malicious code at all.[3]

To be effective, a security operations platform needs to recognize threats it's never seen before. It should apply sophisticated analytics that model attacker behavior to subsequently identify that future behavior. To codify behavior in this way, analytics, intelligence and hands on experience from the field must work hand in hand. That's why solutions should offer more than just machine learning or user behavior analytics (UBA) — they should help analysts prioritize threats, isolate them and choose the right remediation tactics.

1 FireEye (2017). M-Trends 2017: A View from the Front Lines.
2 Ponemon Institute (January 2015). The Cost of Malware Containment.
3 Joshua Goldfarb (October 26, 2016). 20 Endpoint Security Questions You Never Thought to Ask.

Response

With media coverage of cyber attacks at an all-time high, even people who don't work in the security industry know that responding to an incident is as important as protecting against it. An efficient and effective process comprises high-quality alerts, a well-prioritized work queue, accurate analysis and seamless case management. While it may appear that a well-functioning workflow doesn't need to be a top priority for an average company, the data proves otherwise. Last year, it took companies an average of 82 days just to contain and remediate an advanced attack.[4]

To improve response, a security operations platform should integrate all security operations, enrich responses with intelligence, provide case management and improve the efficiency of staff.

Integrate all the pieces of security operations

A good platform should allow security teams to pivot from alert to fix sooner. However, response speed is a typically a function of how quickly security teams can make sense of alerts. If alerts come from multiple sources without the benefit of context and correlation, the log source has almost no value. A proper platform will increase response speed by combining log sources and overlaying them with threat intelligence and analytics to surface new threats. When done right, a platform can be much greater than the sum of its parts.

Enrich response with intelligence

Reliable, high-fidelity intelligence is an important component of a mature security operations capability. But intelligence won't help if it can't be applied directly to the operational environment. In other words, if it isn't easy to use intelligence to help defend the organization, it's useless. That's why the intelligence from the security platform should always be contextual and relevant, applicable specifically to the organization and the breach it's experiencing and ideally, available on demand should teams need more help for their investigations.

Provide case management

Detection often relies on individual SOC team contributors; investigation and orchestration typically involves multiple team members completing assigned tasks, creating reports and sharing sensitive information. Unfortunately, traditional project management and communication tools are vastly unqualified to coordinate these activities

Augment or enhance the efficiency of staff resources

As threats evolve, organizations are racing to fill cyber security job openings, with demand far outpacing supply. More than 209,000 cyber security jobs in the U.S. are unfilled, and postings are up 74% over the past five years.[5] Even if an organization wants to run security operations 24x7, its budget may not permit an adequately staffed security team. Given most organizations' current resources, it's not a good use of time or money to have analysts processing alerts from conventional security systems. These manual processes are inefficient and error-prone, and if a security operations platform can't automate such repetitive, time-consuming tasks, it puts an organization's security posture and employee engagement at greater risk.

Total Cost of Ownership

Perhaps no other topic gets as much scrutiny in the cyber security industry as total cost of ownership (TCO). Companies like to compare products back-to-back based on price. There's nothing fundamentally wrong with that — even if the products are vastly different. Every dollar they spend on cyber security is a dollar that could be spent on other business priorities and organizations need to evaluate their priorities accordingly.

Given that protecting valuable assets will continue to be a foundational operational expense, a slightly different approach to TCO facilitates a broader, more strategic conversation about cyber security. It offers a more comprehensive view of the costs and benefits that stand behind a security operations platform.

Financial costs

Hardware and software, subscriptions and upgrades, associated costs of deployment and maintenance — these costs typically receive the most scrutiny. But while straightforward at the surface, these costs often hide redundancies and inefficiencies in infrastructure, such as multiple solutions with similar functionality, or disintegrated point products that require excessive maintenance, frequent upgrades and ultimately, longer downtime.

for SOC teams. A security operations platform should equip teams with simple tools that allow them to assign and track tasks, manage the work queue and facilitate knowledge exchange for an efficient resolution.

An effective security operations platform integrates a wide array of capabilities, including network, endpoint and email protection, SIEM and orchestration and log management and forensics. It should also help rationalize costs by offering the option to either integrate existing point products or get rid of them.

4 Ponemon Institute (March 2016). The State of Malware Detection and Prevention.

5 Ariha Setalvad (March 31, 2015). Demand to fill cybersecurity jobs booming.

Operational costs

Expenses don't end when an organization buys appliances or subscribes to services. Operational costs involve attracting and hiring top security talent, training them on products and supporting ongoing operations by allocating time and money to them. For most companies, those expenses are as inevitable as financial costs.

Organizations should carefully choose where to spend their time, because time invariably translates into operational costs. When evaluating security platforms, companies should:

- Seek products that offer broader capabilities to reduce or eliminate the time and costs of training staff on numerous disconnected point products
- Invest in advanced detection capabilities that minimize alert fatigue and detect real threats quickly
- Strengthen orchestration and investigation capabilities so that teams can spend time on the most value-added tasks.

Automation minimizes manual repetitive processes such as alert validation. Too often, security professionals spend 80% of their time on these tasks, which is a common cause of fatigue and churn. By automating such activities, a security operations platform allows these professionals to focus on work that has a much greater impact, such as hunting for threats, preventing threats and — in the unfortunate event of a threat — responding to and resolving the threat.

To handle normal talent attrition, a security operations platform should codify and automate the security team's activities to ensure that best practices stay with the company.

Lastly, service continuity is a major driver of operational costs. Retaining top security talent is as hard as attracting it. Hiring an employee is typically predictable — but losing one isn't, and such a loss can put the continuity of all security efforts at risk. A security platform should equip teams with the right tasks, knowledge and tools for their skill level to keep employee churn to a minimum.

Table 1. Security Operations Platform: Critical Capabilities Checklist

Improves Visibility	
Identifies breaches in minutes	✓
Coalesces and prioritizes the most critical alerts	✓
Anticipates attacker behavior	✓
Accelerates Response	
Integrates the entire infrastructure under a single console	✓
Enriches response with intelligence	✓
Provides case management capabilities	✓
Optimizes Costs	
Streamlines financial investments	✓
Enhances staff efficiency	✓
Ensures service continuity	✓

Conclusion

The security operations platform offers tremendous advantages to many organizations. As with any buying decision, of course, organizations should push their vendors for clarity to ensure that they truly understand the actual capabilities of any proposed solution. Only then will a mature security posture become accessible to everyone, including even those organizations without large, enterprise-sized budgets.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FireEye