5 Ingredients To Help Your Security Team Perform at Enterprise Scale

respond

Every enterprise needs a Cyber Security Program. But not every organization has the resources nor the inclination to build a robust Security Operations Center. Leveraging new security technologies and implementing proven security basics enables enterprise scale Security Operations without big budgets and large teams of security resources.

Here are 5 ingredients to managing a successful security program – without an enterprise sized budget

1. Focus and Prioritize Security Data →
2. Understand Your Environment and Know What Matters →
3. Leverage Machine Automation →
4. Keep it Simple – Applications, not Platforms →
5. Demonstrate Success with Metrics →

1.

Focus and Prioritize Security Data

Not all security alert sources are created equal. The multitude of security sensors and data types is continuously expanding and it's easy to get overwhelmed by the avalanche of data. At times, it feels like if you're not monitoring everything, why are you monitoring? In reality though, certain alerting technologies provide better indications of compromise than others. When considering coverage, start in terms of network and endpoint visibility.

For network visibility, many turn to Network Intrusion Detection and Prevention technologies. You may already have these deployed or may have Unified Threat Management (UTM) devices deployed where this module can be enabled. If you do not have this option, there are no cost, open-source solutions such as Suricata and Snort that can be downloaded and used to provide network security visibility. For endpoints, you likely have already deployed technologies that aid you in monitoring systems. Endpoint Protection Platforms, such as traditional and next-gen antivirus vendors, enable monitoring for malware.

Additional technologies such as web filtering and Endpoint Detection and Response (EDR) software can further aid in identification of breaches, but are not required to provide monitoring for the majority of security use cases. Effective security monitoring is not defined by the number of log sources collected, rather by the continued monitoring and analysis of valuable security alerts.

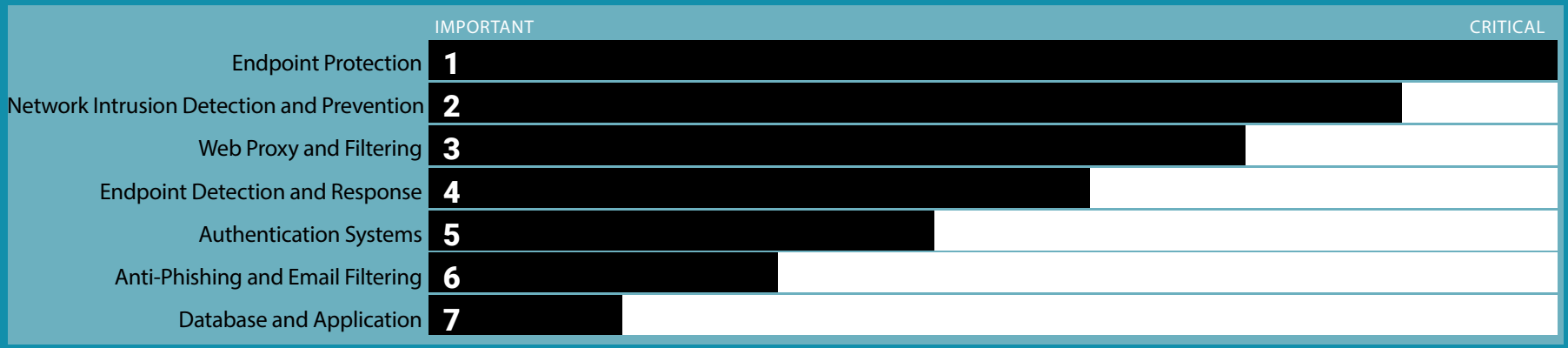
Network Intrusion Solutions
(also called IDS/IPS)

- Cisco FirePower
- Fortinet FortiGate
- Palo Alto Networks
- Snort
- Suricata
- Trend Micro TippingPoint

Malware Detection

- SymantecEndpointProtection
- Microsoft Security Essentials

Priotitize security data sources



2.

Understand Your Environment and Know What Matters

Security alerts can provide evidence of a possible compromise, but what is the potential impact? Even the best security analysts struggle to make good escalation decisions if they don't understand their environment and what is important to the organization. High-value assets and accounts observed in alerts certainly makes the alerts worthier of analysis and can increase the likelihood of an actual attack. Similarly, vulnerability data and intelligence aids in understanding what could be an attack and what is likely not an attack.

To determine the potential impact for an alert, it must be analyzed in context:

- Critical and high-value systems – including IT infrastructure, business generating systems, IT administration systems, and executive workstations
- Vulnerabilities present in the environment for each system, especially those that could be used in an attack to compromise an asset
- Critical and high-value accounts – including IT services accounts, IT administration accounts, executives, and others with high-level privileges that could be leveraged in an attack
- External intelligence – including geo-location data and threat intelligence such as suspicious IP addresses, domains, URLs and hashes
- Internal Intelligence (see sidebar)

Context is unique to an organization and difficult to manage across many clients, this single factor is why many security teams become disillusioned with their MSSP.

Internal Intelligence

An often overlooked, but incredibly valuable, piece of context is Internal Intelligence derived from observations in your environment. This can take the form of suspicious indicators observed and recorded by an analyst for continued monitoring or can be related to historical patterns observed to understand what is normal for an environment going forward.

Many organizations struggle with understanding and capturing information on their environment for monitoring because it is difficult and time-consuming when performed manually. The advantage you have to make this happen in your organization is software that can automate these tasks for you, which is another ingredient we will discuss next.

3.

Leverage Machine Automation

Manual process is the reason why many organizations struggle with security monitoring. Security monitoring, as it's been defined by the industry in the past, is burdensome with manual engineering and analytics tasks. This may work well for large enterprises with significant time, personnel and funds. More and more organizations are struggling to balance resources and security risk.

Automation has changed the game by eliminating the need to perform many of the manual tasks performed over the last several decades. The following tasks can now be partially or fully automated:

- Collection of security alerts
- Collection of security relevant context
- Analysis of security alerts
- Decision to escalate an alert or not
- Building and prioritization of a security incident
- Notification of a security incident requiring response action

The Right Automation Solution :

Increases security capacity and capability while reducing operating costs — machines move faster and can consider significantly more information when making decisions.

Continually delivers ROI as it rapidly scales your ability to neutralize attacks without risk or the need to build an expensive, or complicated, infrastructure or team.

Levels the playing field — multimillion dollar Security Operations Center (SOC) functionalityisaccessibletoany size organization, at a fraction of the investment.

Automation brings advanced capability to the masses. This is a key ingredient in how to enable continuous and effective security monitoring in your organization. You will want to be careful when selecting automation vendors, as some claim automation that requires significant configuration, as we'll discuss next.

4.

Keep it Simple – Applications, not Platforms

In order for automation to help your organization, it shouldn't add significant work to your already busy workload. Search for applications that are designed to work mostly out-of-the-box and steer clear of platforms that result in significant operating expense. Automation software should simplify processes, not make them more complex.

When evaluating automation software, be wary of:

- Significant configuration and ongoing maintenance – automation software should not take consultants or project plans to setup and operate
- Solutions requiring expertise to operate – automation software should have the expertise built in by experts, not for you to program
- Substantial technology investments – consider what technologies and resources are required to run the software, as this can be very costly in time and money
- Lack of scalability – expect solutions to scale as you grow, you want to futureproof your operation as your company grows

These considerations clarify which automation vendors require just as much time to operate as the value you get out of them.

AI + ML

Artificial intelligence and machine learning are advanced technologies with the potential to rapidly change the face of security operations. Security teams with limited resources will benefit by vendors that offer complete solutions leveraging these technologies.

> "To be undeniably valuable, AI and ML should provide value right out of the box requiring no up-front training or large datasets. Simultaneously, they must also learn on their own as well as with human feedback to improve the quality of decision making. Just as an analyst improves with time and experience, so should AI and ML solutions."
>
> — Steve Dyer, CTO, Respond Software

5.

Demonstrate Success with Metrics

Security metrics is a hot topic (SANS and NIST offer good information on this topic). While compliance is relevant and an important metric for many organizations, we recommend three operational metrics to provide you with optimum visibility into your security programs' performance and a way to track improvements.

Coverage It's important to understand and track what percentage of your environment has enough sensor coverage to identify malicious activity. Do you have blind spots? Network and endpoint sensor placement is key to attain good visibility. Choke points for user and server segments are good places for network-based sensors, as well as considering perimeter (external) vs. internal network coverage and multiple office or datacenter locations. Ensuring timely deployment of updated signatures from your security technology vendors is another key aspect of measuring coverage.

Time to Detection Once an organization can detect attacks, the speed of detection is important. Industry statistics vary in providing mean time to detect a breach in environments, ranging from hours to months. The goal is to identify an intrusion before it becomes a significant breach. Automation software, such as the Respond Analyst, can significantly decrease time to detection by vastly improving the chances of identifying a breach from the start.

Time to Resolution This metric will track how long it takes your organization to resolve an incident once identified. The goal is to remediate or mitigate the risk as quickly as possible thereby removing exposure to your organization. Efficiency is critical to limit down time and resume normal business operations. Metrics in this area also expose how well your cross-functional team processes are working.

Learn More

If you'd like to learn more about optimizing your security operations program, please check out our blog at Respond Software. Our security researchers and customer success teams post frequent tips and resources to help make your job easier!

Respond Software

Respond Software delivers Instant ROI to organizations in their battle against cyber crime. With its patent-pending intelligent decision engine, PGO™, Respond Software's product uniquely combines the best of human expert judgement with the scale and consistency of software. This quick-to-implement cyber-security automation software delivers the equivalent of a virtual, best-of-breed analyst team that dramatically increases capacity and improves monitoring and triage capabilities, at a fraction of the cost. Founded in 2016 by security and software industry veterans and backed by leading Silicon Valley venture capital firms, Respond Software is headquartered in Mountain View, CA.

Learn more online	Read our Blog	Request a Demo	Contact Sales

respond