Next Generation SOCs – New Processes Enhance Cybersecurity

The Demands on SOCs are Increasing

The Security Operations Center (SOC) is the first line of defense against cyber attacks. They are charged with defending the business against the many new and more virulent attacks that occur all day, every day. And the pressure on the SOC is increasing.

Their work is more important, as the cost of data breaches are now substantial. The Ponemon Institute's "2017 Cost of Data Breach Study" says the average cost of an incursion is $3.62 million. The study also says larger breaches are occurring, with the average breach impacting more than 24,000 records. And with new regulations such as the EU's General Data Protection Requirement (GDPR) putting stiff financial penalties on breaches of personal data, the cost of a breach can have material impact on the financial results of the firm. This trend toward increasingly onerous statutory demands will continue, as the U.S. is now considering the Data Privacy Act, which will bring more scrutiny and accompanying penalties for breaches involving personal data in the U.S.[1]

1 "2017 Cost of Data Breach Study: United States," IBM Security and Ponemon Institute, June 2017.

TechTarget | Custom Media
WHITE PAPER

The demands on the SOC due to the expansive variety of threats has created a number of pain points that are identified in the recent Vanson Bourne study, "Stay Ahead of Cyber-Crime," sponsored by Juniper Networks. For example, 43 percent of the respondents in this survey believe that attacks are evolving faster than security tools, and 35 percent see skills shortages in their SOCs. This data makes it abundantly clear that the SOC has to raise its game and develop new approaches and processes that will enable the group to continue to protect the organization.[2]

And, of course, attackers are becoming more technically sophisticated, constantly exploiting new attack vectors, and for-profit or government sponsored hacking teams are constantly adding new skills. It is worth noting that with the increasing number of social and spoofing attacks, these attackers are adding behaviorists and specialists who have psychology skills to find new ways to get users to click on links or engage with fake emails or websites that start the attack process. This is part of the hackers' embrace of a long-term view of their targets, demonstrated by the growth of advanced persistent threats (APTs) that continually attack a single target. And defenses are becoming less effective. The availability of demo or evaluation versions of many cyber-security tools allows attackers to evaluate and find ways around common defenses. Aided by stealthier attack methods, the job for the security engineers and analysts becomes more difficult without next-generation security products.

The Next-Generation SOC

Current shortcomings

Defining the next-generation SOC starts with identifying some of the current issues that need attention and prevent the SOC team from upping their game. There are a number of fundamental improvements that must occur. Alert fatigue is a common and vexing problem. False positives waste SecOps staff time, and when there is an overly large number of alerts, it becomes more probable that staff will miss an actual threat. This problem is often exacerbated by many different security tools/products/services, each creating their own alert stream.

The second relatively common problem is poor triage methods. When this process is manually driven by the judgement of a senior SOC engineer, it becomes dependent on the existing knowledge of one or a few specific individuals. This is not a strong process. A far better approach is to use a consistent structure for triage that is informed by the latest threat intelligence data.

The last important change from current to next-generation SOCs is to remove the task of integrating data from multiple low-level security tools to gain a complete picture. The genesis of this problem was the past practice of deploying a new security tool for each new threat. The next-generation SOC demands a highly integrated set of tools that provides greater insight and faster response.

The Next-Generation SOC – Faster and Proactive

Two critical demands form the vision for the next-generation SOC. The first is the need to find threats and intrusions much faster to stop the lateral spread of threats and limit or stop damage. The second is to move from a purely reactive defensive stance to a more proactive approach that is typified by the new process of threat hunting. These two requirements help identify more detailed capabilities that must be in the next-generation SOC. The most important of these include:

- **Use of threat and artificial intelligence –** Enhancing security activities with external intelligence about threats and infusing internal systems with AI provides the ability to substantively change and improve SOC operations. Additional intelligence will reduce the time to identify real threats and breaches, eliminating many false positives while using a better understanding of the threat landscape to ascertain if new attacks are occurring.

2 "Stay Ahead of Cyber-Crime," Juniper Networks and Vanson Bourne, 2018

Threat intelligence from both internal and external sources is a must-have, and many external threat databases are constantly updated with global information. Choosing a solution that has AI-enabled "learning" is quite important, as this functionality will deliver better protection every day going forward.

- **Automation of processes –** As the speed issue has come to the fore, automation has become the critical technology for reducing the cycle time for many of the processes and tasks completed within the SOC. Gaining speed is more important than ever, as the ability to find and remediate threats faster is the best way to reduce the impact of any breach. This is particularly important when there is a virulent threat. Further, increasing the level of automation also makes it possible for existing SOC staff to accomplish more with the same level of staffing and resources. However, not all automation is the same. The better solutions have automation capabilities that are both autonomous and support enhanced human decision-making. Both approaches have value in specific scenarios.
- **Threat hunting –** Threat hunting is the process of proactively and iteratively searching an organization's networks for threats that have not been discovered by other existing security solutions. This is the key to moving from reactive to proactive security, a critical distinction of next-generation SOCs. Typically a team is put in place to find these threats, as well as those with the intent, capability, and opportunity to do harm to the company. As might be expected, new tools and products are necessary to accomplish this, and these tools should have substantial levels of automation to increase the effectiveness of threat hunting.
- **Unification of security tools into a single platform –** SOCs can no longer be burdened with unique and non-integrated security tools. Integration is essential to simplify SOC operations and reduce wasted time. In addition, when the combined capabilities of many tools and intelligent solutions are combined, security posture will improve. From a tactical perspective, a broad integrated tool set will also provide better triangulation to identify and remediate threats.

How Juniper Delivers for the Next-Generation SOC

Juniper Networks provides a range of cybersecurity products and services that are essential building blocks for enabling next-generation SOCs. The Juniper ATP appliance provides an integration platform that allows logs from multiple sources to be centrally analyzed. This provides a more comprehensive perspective for identifying threats with one solution. And the integration capabilities are enhanced with open APIs that allow for the integration of third-party threat intelligence data that results in a stronger threat intelligence database for identifying new or emerging threats.

One of the most attractive capabilities that Juniper provides for next-generations SOCs is application behavior visibility in addition to network visibility. With broader application visibility, the SOC can identify more than just network threats and infestations, and that provides an additional layer of cyber-defense that many other solutions just don't offer.

Key Takeaways

The pressure and demands on SOCs continue to increase each and every day as technically competent and well-funded attackers create new and virulent malware and exploits. Many organizations are now updating their SOC to provide protection from the latest threats.

However, unlike other advances in the SOC, today's upgrades are changing fundamental processes and approaches. Increased use of automation and intelligence

is the primary driver of this change. The goal is to save SOC staff time by automating tasks and to incorporate new sources of intelligence to support both the automated and manual processes. These improvements to defensive posture are also being enhanced by the first wave of offensive cyber-security tactics around threat hunting. Rather than waiting until an exploit shows itself, next-generation SOCs are actively scanning and evaluating the network, "hunting" for exploits and malware that may have penetrated the perimeter defenses.

Juniper Connected Security is a complete portfolio of security solutions that help enable the next-generation SOC. The company has more than two decades of experience providing network solutions and security. The latest generation of products delivers for the most advanced SOCs.

For more information, please go to https://www.juniper.net/us/en/solutions/security/

About Juniper

Since its founding over 20 years ago, Juniper has been committed to bringing simplicity to networking, including the security and safety of information that flows through the network.

That is why Juniper introduced the Juniper Advanced Threat Prevention Appliance (JATP), which works with the security products you already have to improve productivity of both analysts and responders.

JATP can detect advanced malware in 30 seconds, fueled by threat behavior analytics and machine learning. It integrates seamlessly with existing security architecture and provides unmatched protection against advanced threats targeting your organization. It is the only solution certified by ICSA Labs to provide 100% detection of advanced threats.

JATP combines advanced threat detection with consolidated security analytics across all infrastructure and offers one-touch threat mitigation to streamline security and SecOps. With JATP, you protect on-premises and cloud-based assets, email and data, and gain a deeper insight into compromised users and endpoints.

To find out more, visit Juniper at **https://www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/**