SEGRA

How to maximize business security with true holistic monitoring of the IT network

In recent years, cyberattacks and cybercrime have become the most serious threats that organizations face. Industries ranging from banking to healthcare, and organizations of all sizes from schools to public institutions, are up against an ever-growing risk of highly damaging, costly data breaches and other attacks. The number of cyberattacks is on the rise, with tactics now used by attackers becoming more and more advanced.

Faced with multiple threats, organizations need to rethink their cybersecurity response to ensure they have the ability to collect, correlate, and analyze security information from all IT systems within their networks.

This article analyzes some of the key challenges that small and medium businesses (SMBs) in particular face when it comes to protecting their IT infrastructures against cybercrime. After providing an overview of today's most common categories and types of cyberattacks, we will look at some of the main limitations of traditional "perimeter defenses" such as firewalls and antivirus software. We then discuss the different approaches to cybersecurity that organizations can adopt, analyzing the key differences between a DIY, in-house approach and a Security Operations Center as a Service (SOCaaS) solution, one of the most powerful, flexible and affordable cybersecurity tools now available.

Faced with multiple threats, organizations need to rethink their cybersecurity response to ensure they have the ability to collect, correlate, and analyze security information from all IT systems within their networks.

The most common cyber threats

Cyberattacks can take many forms and are increasing both in number and sophistication. The number of data breaches in the U.S. rose from 157 in 2005 to just under 1,500 in 2019, with nearly 165 million records exposed[i]. According to analyst firm Raconteur, the average cost of cyberattacks (per organization) reached $27.4 million in 2018[ii]. But what does a cyber threat actually look like today?

There are two main categories of cyberattacks[iii]:

- **Un-targeted**, meaning the attackers indiscriminately target as many devices, services or users as possible.
- **Targeted**, meaning they target specific organizations.

Attacks in both categories can involve a range of tactics, including:

- **Hacking**, which defines any unauthorized access to data stored on a computer network without permission.
- **Ransomware**, which involves disseminating disk-encrypting extortion malware.
- **Phishing**, which means sending emails to large numbers of people, normally asking for sensitive information (such as bank details) or linking to a fake website.
- **Data leakage**, which defines any unauthorized transmission of data from within an organization to an external recipient.
- **Internal threats**, which come from people within the organization and can be either malicious or unintentional.
- **Brute force threats**, which involve attempting to access password protected information.

- **Advanced persistent threats**, which are carried out by a stealthy computer network gaining unauthorized access to a computer network and going undetected for extended periods of time.

Relying on firewalls and antivirus software is no longer enough to protect an organization against all these threats.

Why detecting cyber threats is so challenging

Until recently, most cyberattacks came from outside the organization, meaning perimeter defenses like firewalls or antivirus software were normally enough to stop them. But today, we see how attacks can originate virtually anywhere, including inside an organization's network. Malware can, for example, infiltrate the network through email attachments, banner ads or fake websites. Connected, Internet of Things (IoT)-enabled devices can also be vectors of cyber threats. Many sensors and smart devices are not designed with cybersecurity in mind and, therefore, can be vulnerable to cybercrime, putting an organization's entire network at risk. Intrusion detection and prevention systems (IDS/IPS) often aren't enough to protect a network against threats of this kind.

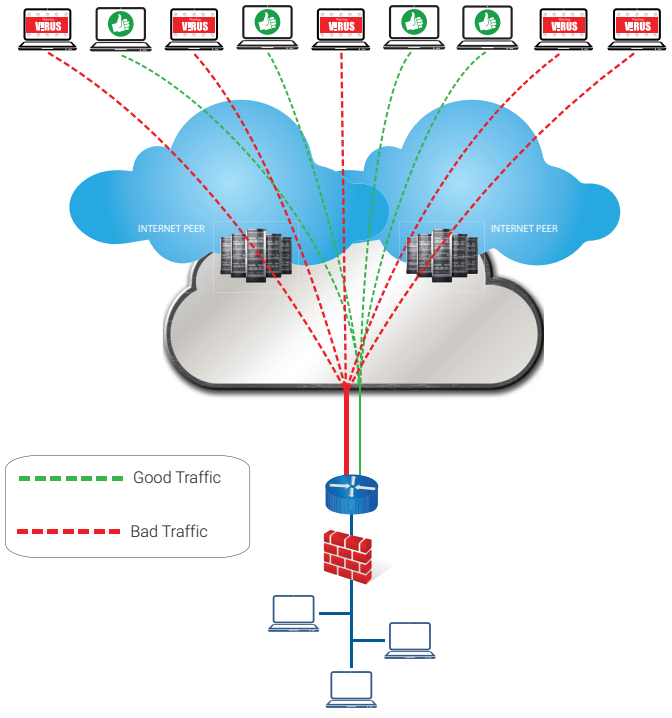

Image 1: Example of a DDoS attack in progress.

What's required today is greater capability to collect, correlate, analyze and act on cybersecurity threats from all IT systems and networks, enabling rapid detection and remediation. But most organizations simply lack the technology, skills and personnel to implement such comprehensive cyber security strategy. On average, it can take a staggering 205 days before an organization discovers a data breach[iv].

A cyber threat that goes undetected for too long can not only damage an organization due to exposure of sensitive information, data loss and costly downtime - but enterprises in highly regulated industries such as retail, healthcare and finance can also incur hefty fines, in line with the following regulations:

- Payment Card Industry (PCI)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Financial Institutions Examination Council (FFIEC)

What's required today is greater capability to collect, correlate, analyze and act on cybersecurity threats from all IT systems and networks, enabling rapid detection and remediation.

How to respond to cyber threats: the DIY approach

When addressing today's evolving cyberthreat landscape, organizations may weigh the option of building, deploying and maintaining an in-house security operations center. The downside of this "DIY" approach is that it often requires significant capital investment. Some of the key considerations are:

- Costs can be prohibitive and unpredictable, particularly for SMBs lacking security staff or expertise.
- Full deployment can take months if not years.
- The organization can incur additional costs due to recruiting, training and retaining IT security staff.
- Multiple layers of cyber security protections generally involve multiple tools to learn and interfaces to monitor, which can be a resource-intensive process.
- Keeping up to date and ahead of changing threats depends on the organization's ongoing success at planning, budgeting and implementation.

How to respond to cyber threats: the SOCaaS approach

We've seen how organizations today need an all-encompassing cybersecurity solution in addition to traditional perimeter firewall and antivirus software. Unlike the DIY, in-house approach, this way of managing cybersecurity normally involves:

- A holistic approach to protecting the entire IT infrastructure against all forms of cyber threats.
- Real-time alerts to threats and intrusions.
- Predictable, economical costs.
- Access to professionals with expertise and experience.

This is where Segra's SOCaaS offering comes in. The SOCaaS integrates with existing processes to increase visibility, and combines:

- A security operations center (SOC) with an information security team responsible for ongoing monitoring and analysis of an organization's cybersecurity. The SOC is staffed with tier 1 analysts, advanced security engineers, threat hunters and threat intelligence managers.
- A combination of technologies including:
    - Security information event management (SIEM) software to provide holistic security threat detection through collecting, aggregating and analyzing security data from network devices such as firewalls, servers, routers, switches, wireless access points and O365.
    - Additional tools such as artificial intelligence, cross-correlation of events, user behavior analytics and advanced threat intelligence feeds to deliver smart security threat detection and response.

By constantly monitoring all threat detection data, the SOCaaS solution has all the tools required to detect, automate responses and take action to alert customers in real time as soon as abnormal or malicious behavior is detected anywhere in their network.

The SOCaaS provides organizations with immediate analysis of security alerts generated by applications and network hardware, but without the need for capital investment. The service is hosted in a secure and compliant cloud so that it can manage and monitor an organization's critical systems regardless of where they are.

By constantly monitoring all threat detection data, the SOCaaS solution has all the tools required to detect, automate responses and take action to alert customers in real time as soon as abnormal or malicious behavior is detected anywhere in their network.

The benefits of adopting the SOCaaS solution

The SOCaaS solution offers a holistic monitoring of the entire IT network. It can be configured to protect any servers and IoT devices that an organization wishes to monitor. The SIEM dashboard with advanced threat intelligence is designed to work as a multi-tenant portal with co-managed options that allows a high level of interface customization, meeting the needs of customers who wish to maintain a certain degree of control. The SOCaaS can also often be integrated with, and bring greater visibility to, existing security investments.

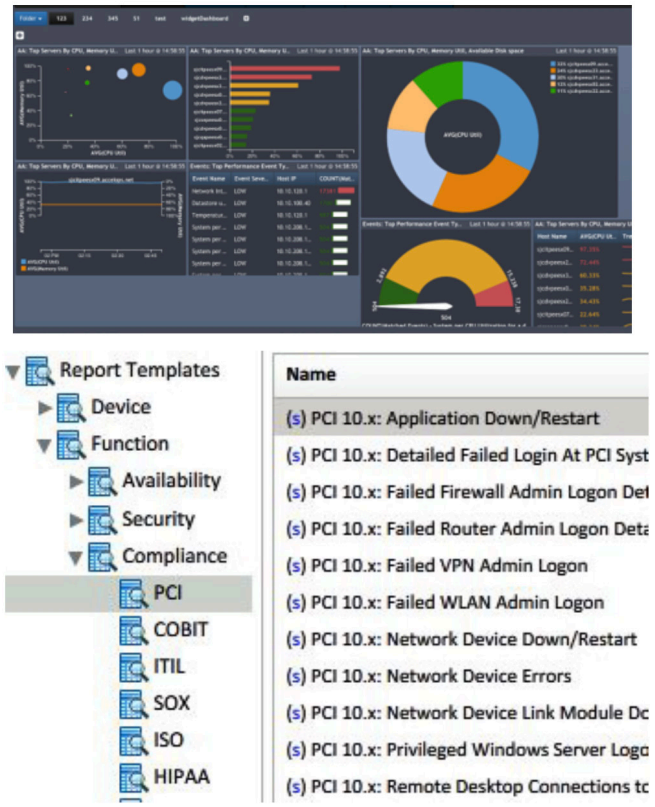

Image 2: The Segra SOCaaS dashboard

Thanks to a dedicated, 100% U.S.-based 24/7/365 SOC team, Segra's SOCaaS solution constantly reviews all alerts in real-time ranging from low to high severity, guaranteeing a 3-minute SLA for all high severity alerts. Sophisticated fine tuning of monitoring and reporting rules means that only actionable alerts are sent to the customer, ensuring near-zero false positives.

In addition, using artificial intelligence and advanced threat intelligence feeds, the SOCaaS builds and refines self-learning behavioral models that detect threat patterns and automate responses with machine learning-derived security information. Security automation and customizable playbooks can orchestrate threat responses and remediations in conjunction with SOC team analysts to improve the efficiency and effectiveness of security operations.

A true cloud-based solution, SOCaaS offers enterprise-grade reliability and the latest feature and threat updates on an ongoing basis. It is fully managed by Segra and comes with turnkey deployment and no local on-premises hardware installation.

The solution's advanced machine learning capability means that the software can learn an organization's environment and activities in a matter of days. For example, SIEM can learn what activity is normal to expect on a Tuesday and what isn't normal on a Tuesday night. Once this baseline is complete, the software platform goes live and alerts begin coming through. The end goal here is to narrow millions of daily alerts and events to just a handful of meaningful alerts that require attention. These include critical information such as incident ID time stamps, source IPs, rules that were triggered and remediation guidance.

With this vital information at hand, an organization is in a much better position to respond to a threat in an effective and timely manner.

Another key benefit of adopting the SOCaaS solution is that its portal enables users to pull from thousands of pre-defined compliance reports and have these generated on a regular basis, including a monthly overview report for C-level executives. In this way, evidence of compliance with key regulations and standards can be gathered in no time.

A true cloud-based solution, SOCaaS offers enterprise-grade reliability and the latest feature and threat updates on an ongoing basis. It is fully managed by Segra and comes with turnkey deployment and no local on-premises hardware installation.

Unlike DIY solutions, costs are entirely transparent and predictable and translate into a monthly fee, based on an OPEX model.

Conclusion

Organizations of all sizes face an unprecedented level of cyber threats both in terms of quantity and sophistication. A holistic approach to cybersecurity is therefore needed, but is often beyond the reach of many SMBs.

Segra's SOCaaS solution enables organizations to gain all the benefits of the world's most powerful and flexible software without the hardware or personnel investment for deployment, management, or maintenance of the system. Segra takes care of all the infrastructure, maintenance, upgrades, patches, capacity planning, backups, and security of the system and platform.

i. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
ii. https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/
iii. https://www.ncsc.gov.uk/information/how-cyber-attacks-work
iv. https://arxiv.org/ftp/arxiv/papers/1901/1901.00699.pdf

For more information, visit: **www.segra.com/socaas.**

SEGRA

833.GO.SEGRA
businesssolutions@segra.com
www.segra.com