Security Operations Center as-a-Service

Choosing the Right Security Vendor

Synopsis

One of the biggest misconceptions in the technology marketplace are Managed Service Providers (MSPs) who believe they can build a Security Operations Center (SOC) and begin providing Managed Security Services (MSS) to their clientele. After all, it seems like it would be a natural progression to add a few network security devices into their Network Operations Center (NOC) and rebranding it as a Security Operations Center (SOC) but nothing could be further from the truth.

Understanding the Difference Between a SOC and NOC

The roles of a SOC and a NOC are not subtly but fundamentally different. The SOC and NOC are responsible for identifying, investigating, prioritizing, escalating and resolving issues, but the types of issues and impact they have are considerably different.

A NOC handles incidents and alerts that affect performance and availability. The NOC's job is to meet service level agreements (SLAs) and manage incidents in a way that reduces downtime, so it focuses on availability and performance.

A SOC focuses on incidents and alerts that affect the security of information assets and its main role is to protect intellectual property and sensitive customer data – a focus on security.

While both a SOC and NOC are critically important to any organization, combining them into one entity and having them each handle the other's duties can spell disaster – because their approaches are so different and skill sets required to manage are distinctive.

A NOC analyst must be proficient in network, application and systems engineering, while SOC analysts require security engineering skills.

Last but not least, the very nature of the adversaries that each group tackles are different. The SOC focuses on "intelligent adversaries" while the NOC deals with naturally occurring system events.

SOC Challenges and How Inceptus Addresses Them

Staffing

One of the most significant issues in building and maintaining a SOC are a lack of cyber experts. A 2016 report from Cisco (1) predicted that there would be a shortfall of 1.5 million cybersecurity job openings and that figure was only going to get bigger with cybercrime outpacing the talent shortage. Cybersecurity Ventures (2) predicts there will be 3.5 million job openings globally by 2021. The challenge is, and has been, recruiting and retaining cyber professionals. The challenge is even larger when trying to recruit or retain high level experts, like Tier 2, 3, or 4 experts. MSPs who wish to get into the security game have to compete for this talent from other security companies and government organizations.

Inceptus recruits heavily from the armed forces, government agencies, and other security companies. Experts in the cybersecurity industry are highly respected and revered and there are only a couple of degrees of separation between who knows who. Cybersecurity professionals flock to companies and organizations who possess these experts because they want to learn from people who have had years of experience dealing with some of the most sophisticated attacks. MSPs generally do not have this type of talent and try to grow it organically. Inceptus employs some of the most respected cyber experts in the industry.

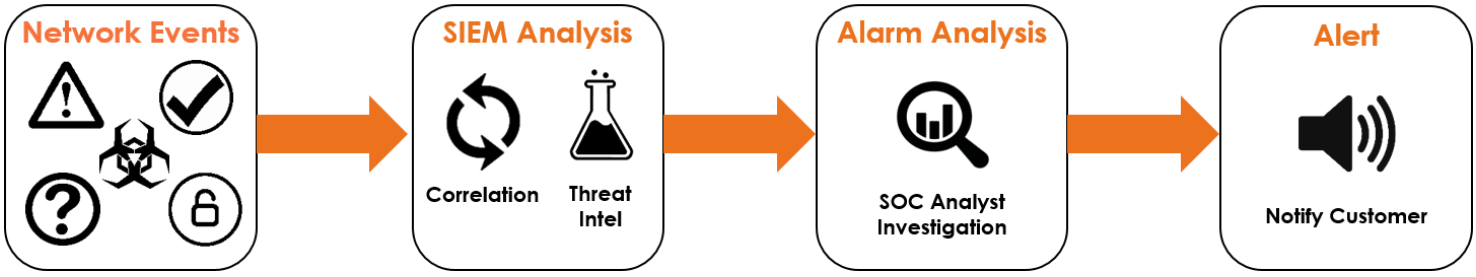
1. https://learningnetwork.cisco.com/blogs/talking-tech-with-cisco/2016/10/26/getting-started-in-a-cybersecurity-career

2. https://cybersecurityventures.com/jobs/

inceptus

40,930,176 Events | 3,089 Alarms Analyzed | 4 Alerts Issued

Feb 2, 2019 – May 2, 2019

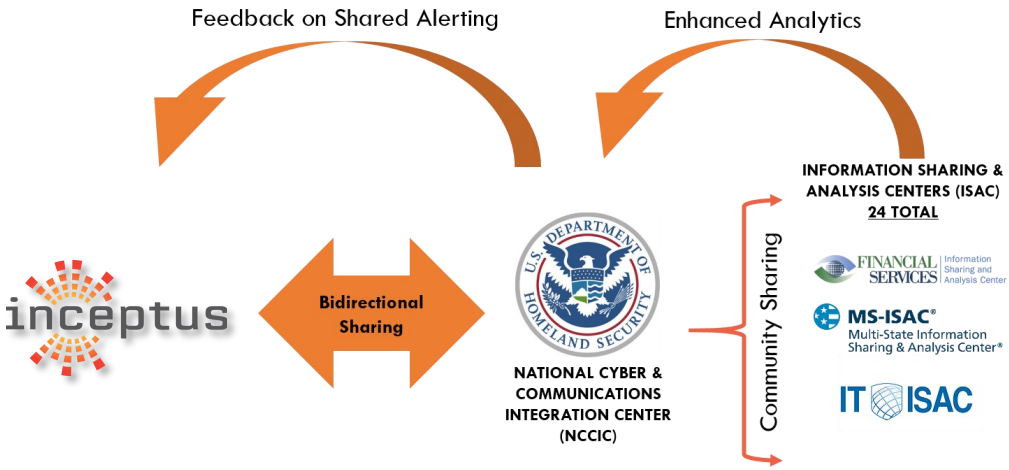


Alerts Efficiency

Inefficient alerting in one of the major reasons SOCs fail. An example would be getting too many false positives and not getting relevant alerts. Reasons this happen vary but the more common ones are:

- Not understanding what the alert means. To the untrained analyst, a group of alerts may be meaningless but to a seasoned analyst, they could collectively represent a major cyber attack
- Not properly training and tuning the security devices to the behavior of the client's network. Organizational networks behave differently from one another just like a business runs different from one another. No two organizational networks are alike. Organizations are configured differently, use different applications, perform different functions, and allow/ disallow users access to different areas and applications on the network.
- Not employing tools to quickly identify, investigate, and notify on true positives. Many MSPs who decide to provide MSSP services find out quickly that there is a lot of orchestration, automation, and workflow processes that take place in the background to be able to notify quickly.
- Not utilizing threat intelligence correctly or at all. Threat Intelligence is the key to identifying malicious software, IP addresses, websites, signatures, intelligence, etc. but if not used correctly or misinterpreted, it is ineffective. Many MSPs do not have the talent to ensure threat intelligence is correctly correlating to alert on True Positives.

The Co-Founders of Inceptus have years of experience building and operating SOCs, understanding and defining data analytics, and direct involvement in some of the most sophisticated nation state attacks on both commercial and government organizations. Inceptus understands that networks and user behaviors are always changing, to the training and tuning of security devices happens continuously. Inceptus not only focuses on the "what just happened?" but also the "why it just happened?" as well, making threat intelligence a key part of our service.



inceptus

Processes and Procedures

Developing, implementing, and maintaining processes and procedures are instrumental to running a successful SOC. The ability to create a replication of routine processes is a major efficiency issue for many SOC teams where hundreds of processes in itself, can be challenging. Although MSPs are also heavily focused on processes and procedures, they are quite different because rather than focusing on assets, SOC processes and procedures focus primarily on incident handling and alerting.

Processes, Policies, and Procedures are an integral part of any organization's cybersecurity program. Imagine if your organization is hit with a cyber breach but there is not an Incident Response Plan in place. Your company will lose valuable remediation and mitigation time because no one knows what to do or what their role is. Inceptus focuses heavily on Policies and Procedures because they can preempt a cyberattack if followed, and can assist in recovery efforts if your organization experiences a cyber breach.

The Technology

If an MSP has not had extensive experience with security devices, e.g. Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS), Security Information and Event Managers (SIEMs), etc., they quickly discover they are way over their heads. These devices are not like routers, switches , and servers. They are more complex in the sense they require hours of training and tuning to get to the "True Positives'. Simply dropping these devices into a client network without an intimate understanding of how they work has proven disastrous for many MSPs. Many of the effects they experience after they move to becoming an MSSP are:

- Finding out the level of support from their vendors is not the same experience they get from their networking vendors
- Not realizing the configuration and change management of security devices requires an even more precise skillsets which there is already a lack of in the marketplace
- A false reliance on the technology to provide them everything they need with untrained personnel

Inceptus only provides cybersecurity services. We spend countless hours vetting security vendors and training our employees to ensure we understand what the right security technologies are for our clients. We not only train our analysts to detect and alert on "True Positives", but we train them to spot havioral anomalies as well. Something that can only be learned from years of experience.

Summary

The cost to build a world-class Security Operations Center can exceed millions of dollars. At the start many MSPs feel that the cost to build is only a small effort and an incremental fee to their existing service offerings. Inceptus has met with many MSPs that have tried, and subsequently scrapped the idea after spending a lot of money, time, and resources. Cybersecurity is the only technology that has an adversary which requires a specific skillset to stop them. Inceptus possesses those skillsets. You wouldn't trust your Maserati to get fixed by a mechanic who only knows how to work on Fords. Why would you trust your security with a company who doesn't really understand security?

Inceptus, LLC

4825 Coronado Pkwy., Suite 1
Cape Coral, FL 33904

Phone: 239-673-8130
Email: info@inceptussecure.com

www.inceptussecure.com

#UnderOurProtection