ISE® SOUTHEAST EXECUTIVE FORUM

Nominee Showcase Presentation

H. Lee Moffitt Cancer Center & Research Institute

Creating a SOC with the perfect fit

Hugh Percy, MSIS, CISSP

Supervisor, Cyber Security Operations

Company Overview

- Mission: To Contribute to the Prevention and Cure of Cancer
- > 5000 total workforce
- > 1B annual revenue
- 30 year birthday this year
- Non-profit Cancer Care and Research Institute
- International Cancer Care Center
  - 6th on the top cancer hospitals in the Nation – 2017 U.S. News & World Report
  - Florida's only NCI designated comprehensive care facility

Presentation Overview

- The Cyber hack/attack event - Not “if”, but “when
- Preparing for the known is hard enough, but what about the unknown?
- Expand your capability – get bold and proactive
- A Security Operations Center (SOC) – a modern world requirement

SOC – Phase One

Two phased Project Phase One

Our SOC is being built in phases and operates on the premise that the more we monitor our environment, the better we know what our normal operating environment consists of. When something falls outside the norm, it gives us the opportunity to catch an unwanted or damaging event before it can cause major impacts.

A successful SOC operation is only attained by collaboration between all teams of IT.

Performance Monitoring

A SOC is solely focused on incidents that are cyber related; attacks, intrusions, threat incidents, etc, that are identified, analyzed and mitigated. Our SOC has been created to handle not only cyber but also integrated the purpose of a Network Operations Center (NOC). A traditional NOC's function is to monitor infrastructure for events that require attention so as to avoid degradation in services.

Cyber Security Monitoring

By correlating business-relevant information against available technical data, the SOC can produce security industry trends that can enable the business to improve decision-making, risk management, compliance and business continuity.

Case Study - Hospital #3

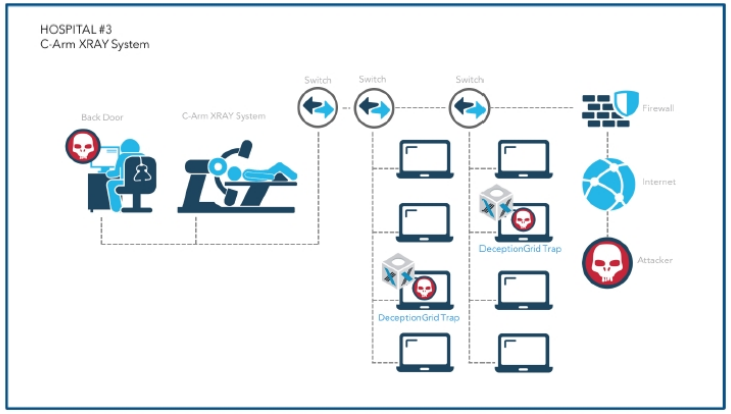
Hospital #3:

Vendor D - X-Ray machine

Overview

Our client is a top 200 global hospital that was evaluating advanced threat detection solutions. They had interest in evaluating deception technology and already had in place a funded cyber defense architecture. They had intrusion detection, firewalls, and endpoint security in place.

The hospital had a small but sharp IT and security operations team. They had considerable experience in cyber security in past employment and were using their current technology consistent with best practices. They had no knowledge of any attacker presence within their networks.



Healthcare - State of the Union

Healthcare is one of the largest individual markets within the United States with annual expenditures that consume approximately 17.5 percent of the gross domestic product in the United States. The ecosystem that provides healthcare in the U.S. includes approximately 900,000 physicians spread across over 225,000 practices. In addition, there are over 2,700,000 registered nurses, physician's assistants and medical administrative staff that support these hospitals and physician practices.

There are other key facilities necessary for the delivery of important healthcare services. This includes over 5,500 hospitals that support these healthcare providers directly. There are

organizations: Excellus BlueCross BlueShield, 10 million records compromised; Premera Blu Cross, 11 million records affected; and Anther Blue Cross, with 78.8 million sensitive patient records compromised. Recent events since th original MEDJACK report continue to show th acceleration of attacker activity within healthcare in 2016 after reported incidents dropped slightly in 2015.

During the first few months of 2016, the healthcare industry experienced a increased number of cyber threats that struck numerous hospitals across North America and around the globe. Some of these hospitals are listed in Table 1 - North American Hospitals Impacted by Cyber Attackers in 2016. All of these attacks were

Operational Turn out/Results

The implementation of a Security Operations Center (SOC) has already produced some impressive results.

- Since go-live, (first week of July):
  - Handled 800 events and generated 586 IT service tickets
  - Preemptively prevented around 231 performance downtimes. These tickets allowed our infrastructure, server and application teams to work issues ahead of a major problem.
  - Handled 10 Major downtime incidents
  - Handled 2 Major Cyber security events

Lessons Learned/Best Practices

- Do not attempt to cover all events
- Identify critical assets
- Establish a clear communication plan and level of escalation

Phase two

Sometime within the next few months, the SOC will be operating 24/7/365.

Expanding this coverage by leveraging 3rd-party Security Operation Center offerings

Phase One has allowed us to detail what we need to do to move forward with a Hybrid SOC.

Thank you and Questions

Questions?

Contact Info:

- Hugh Percy
  Supervisor Cyber Security Operations
  Hugh.Percy@moffitt.org

- Dave Summitt
  Chief Information Security Officer (CISO)
  Dave.Summitt@moffitt.org