Cybraics Identifies Critical Misconfigurations Prior to Vulnerability Disclosure

Challenges

- Many medical devices are maintained by device manufacturers, making it difficult for the healthcare provider to update and enforce policies
- Adversaries are often aware of vulnerabilities before vendors disclose them

Existing Security Tools:

- IDS/IPS, Threat Intelligence, SIEM, Advanced Threat Detection

Results

- Mitigation of a vulnerability before an exploit was leveraged by an adversary

Background

The healthcare provider has a dedicated security operations team and has implemented several advanced security measures; including an IDS/IPS, Threat Intelligence, SIEM, Advanced Threat Detection software. They also utilize the services of an MSSP.

What We Found:

The nLighten platform implements multiple unique, proprietary analytics, including network behavioral analytics that identifies anomalous behavior in the traffic patterns of IT and OT networks. In this case, a graph analytic, EdgeX, identified a server involved in abnormal behavior – contacting external hosts differently from other devices. Our artificial intelligence (AI) analyst, Janus, highlighted it for further investigation. The server was a network-based management device that administers all patient bedside devices. The existing security tools and 3rd party MSSP were incapable of alerting the healthcare provider's security team that the management device was also contacting thousands of domains across the internet and that the NBNS protocol was traversing the firewall. Even worse, many of these domains host malware distribution sites.

Janus, our AI analyst, alerted the security team of the anomaly and we advised the customer that their bedside management server was connecting to external hosts using a NetBios protocol. They then took immediate action to reconfigure the server and disable the traffic. One week later, Microsoft released a critical patch for this exploit, identified as BadTunnel, which allows attackers who receive NBNS packets to conduct a man-in-the-middle attack on network traffic. The nLighten platform helped the healthcare provider avoid a potential HIPAA compliance violation, and more importantly, circumvented a catastrophic event should an adversary gain control of the bedside devices.

Result:

Beyond detecting active threats against an organization, the nLighten platform identifies misconfigurations and network hygiene issues. Traditional signature-based systems, SIEMS, and threat detection tools that rely on sandboxing, as used by this healthcare provider, may miss these types of misconfigurations. nLighten is changing the legacy security mindset by fortifying the IT ecosystem with AI-based security analytics.

Copyright © 2017 Cybraics, Inc. All rights reserved.