INFORMATION SECURITY

VULNERABILITY ASSESSMENT AND TESTING

THREAT INTELLIGENCE

BURTELSON CORPORATION

Burtelson

EXECUTIVE SUMMARY

Burtelson information security vulnerability assessment and testing services are complete and customized to meet the unique needs of clients. Key components of Burtelson vulnerability assessment include cyber intelligence, threat analysis, and vulnerability testing. Burtelson intelligence analyses are among the most popular among a variety of healthcare clients.

This paper summarizes the complete aspect of Burtelson's cyber intelligence strategy points. Collectively, this summary provides clients with information on superior intelligence analyses, threat mitigation, lower costs and patient confidence. From a broader standpoint, the security assessment services are coming together to deliver industry-leading healthcare security intelligence analysis. This paper will address both of these aspects of Burtelson's internal and external strategy.

Burtelson Cyber Threat Intelligence

Strategic Functionality

At a strategic level, threat intelligence spotlights the exposure a healthcare organization has to particular threats and allows those threats to be considered in relation to current and future financial risks, reputational risks, and continuity of operations. Types of strategic threat intelligence include threat assessments, intelligence summaries, and adversary profiles or assessments.

Rule number one: Know your enemy. Threats to healthcare organizations are relentless, and they come in all shapes and sizes and from all directions. We focus on both internal and external sources to create the most accurate threat profile, and rank the value of the sources of threat intelligence. If you utilize a Security Information Event Management (SIEM) approach, you're a great starting point. Raw sources of internal network data come in the form of event logs, DNS logs, firewall logs, among others, and are present in your SIEM. Having knowledge of prior incident response engagements is very helpful in leveraging more evolved threat awareness based on internal sources. Retaining malware used, packet capture and netflow can be valuable intelligence sources.

In addition to internal sources, we look to external intelligence sources. We start by collecting information on threat indicators from security researcher and vendor blogs, as well as publicly available reputation and block lists.

Threat intelligence accuracy is based on the number of false positive alerts or actions obtained from the threat intelligence. The lower the number, the more accurate the intelligence. Confidence ratings or certainty scoring may help in assessing the potential for false positives. Accuracy is also contextual. When context correctly links the operational and strategic aspects of a threat, the activity can be accurately attributed and the motives and capabilities of the adversary can be assessed. Inaccurate context results in incident-response efforts that are misdirected, and strategic defenses that are misaligned with real threats.

DUE TO THE EVER-INCREASING VOLUME OF CYBERATTACKS AND REGULATORY PRESSURES ON HEALTHCARE ORGANIZATIONS AND PRACTICES, THERE IS AN INCREASED NEED FOR BETTER CYBER INTELLIGENCE STRATEGY AND DEPLOYMENT.

ALERTING AND BLOCKING

This is the basic use case for leveraging threat intelligence. Use tactical feeds of threat intelligence-derived indicators to block malicious activity at firewalls or other gateway security devices. Detection for indicators of compromise (IOC) can be deployed as alerts in SIEMs, as signatures on IDS/IPS, or host-based signatures on configurable endpoint protection products.

CONTEXTUAL ALERTING AND SIGNATURE MANAGEMENT

Alerts with context provided by threat intelligence are useful in determining the severity and validity of alerts. Both host- and network-based detection signatures are made more useful in context from threat intelligence by providing confidence, priority, and appropriate next steps based on an adversary's known tactics, techniques, and procedures.

INCIDENT RESPONSE

Threat intelligence directly supports incident-response processes by placing observed IOCs into context. This helps responders determine where to look next to observe an ongoing intrusion. Threat intelligence can also drive the prioritization of ongoing investigations based on knowledge of the adversaries involved.

THE FIRST STEP

We get started by understanding your organization's specific needs for threat intelligence. This first step is perhaps the most difficult. Your organization should be asking this question again and again, as your needs, budget, and risk posture evolves.