CYREN BY DATA443

Leveraging Threat Intelligence to Improve MTTR and Support Decision Making in the SOC

Solution Brief

Business Challenge

With more than 90% of enterprise breaches starting with a single email, security operations (SOC) teams are constantly locked in a battle to protect their enterprise against evolving email-borne adversarial tactics. The SOC relies on data to inform their decisions – typically including multiple threat intelligence feeds (free and premium) as well as in house intelligence. Threat intelligence is intended to provide contextual and actionable insights that improve threat detection and response efficiency by prioritizing threats that require immediate attention. But not all threat intelligence feeds are equal. Free threat feeds often acquire their "data" from the same source and may not always be timely or high quality. Low quality, improperly operationalized intelligence provides limited value and can often increase a security analyst's workload, resulting in overwhelmed security teams and increased organizational vulnerability.

Solution Benefits

- Increased awareness of new and emerging email-borne threats
- Actionable, contextual intelligence to make timely, meaningful decisions
- Improved efficacy of threat response

Challenges Solved by Threat Intelligence

Lack of Visibility - Expensive security investments are effective in stopping known, existing threats being delivered via email. But what about new and emerging threats? Effectively protecting the enterprise from a rapidly evolving threat landscape is a challenge that many enterprises face today. Organizations lack the context to understand the impact of emerging threats and the visibility needed to identify them, leaving the organization vulnerable.

Lack of Timely Intelligence - With attacker Tactics, Techniques, and Procedures (TTPs) constantly evolving, time is of the essence when responding to and containing threats. If not operationalized in time, threat intelligence can quickly become stale and leave your organization susceptible to rapidly changing attacks orchestrated by opportunistic attackers.

Improving Accuracy of Threat Detection and Response - Intelligence providers often purchase information from similar sources before packaging and selling them as intelligence feeds. As enterprise SOCs subscribe to multiple threat intelligence feeds (free and premium), they may often face challenges with the accuracy of their threat detections, due to their mixed quality. Valuable information can often be buried within mountains of old information or false positives. This can lead to missed detection opportunities, reducing the effectiveness of their security investments.

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

DATA443

4000 Sancar Way, Suite 400
Research Triangle, NC 27709

Website: www.data443.com
Email: info@data443.com

US: +1 919 526 1070
UK: +44 203 7693 700

Leveraging Threat Intelligence to Improve MTTR and Support Decision Making in the SOC

Solution Brief

Cyren Threat InDepth

Cyren Threat InDepth is contextualized, correlated threat intelligence that allows security teams and security executives to gain a comprehensive and multi-dimensional view of evolving email-borne threats and make meaningful decisions to combat them. This high-fidelity, actionable intelligence is gathered by analyzing and processing billions of daily transactions across email content, suspicious files, and web traffic to provide unique, timely insights faster than other vendors. Threat InDepth is available to enterprises as – Phishing & Fraud URL Intelligence, Malware URL Intelligence, Malware File Intelligence, and IP Reputation Intelligence.

Threat InDepth Benefits

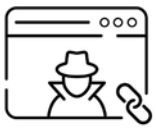
1. Unique Visibility to Protect Against Known & Emerging Threats: Cyren GlobalView™ Threat Intelligence Cloud processes billions of transactions a day to identify security threats across email, file and web, providing Cyren the earliest possible indication of new, emerging email-borne threats. Cyren's proprietary threat engines analyze and correlate this information providing valuable context (available as Threat InDepth Intelligence) to security teams allowing them to affect faster detection and response. By combining human intelligence and advanced algorithms, Threat InDepth allows analysts to detect new and emerging threats hiding in plain sight, ensuring early detection and remediation.

2. Accelerate Threat Detection & Incident Response: Analysts are constantly engaged in a battle to protect their enterprise against evolving attacker TTPs. Timely, contextualized threat intelligence empowers security teams to make smart and meaningful decisions. By analyzing billions of emails daily, Cyren threat engines are able to uniquely identify and correlate IOCs faster than other security vendors. Threat InDepth leverages this information and provides security teams with timely, actionable insights they need to rapidly identify, prioritize, and respond to threats and reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

3. Improve Value of Security Measurements: By operationalizing intelligence in a timely manner across their security investments, enterprises can ensure and maintain a comprehensive security posture. Threat InDepth provides security teams with correlated, contextual, and timely intelligence faster than other vendors. By ingesting these high-fidelity insights, security tools can improve the effectiveness of their detections providing teams with a multi-dimensional view of the threat landscape. This allows organizations to ensure and maintain a comprehensive and proactive defensive posture.

IP Reputation Intelligence

Phishing & Fraud URL Intelligence



Malware URL Intelligence

Malware File Intelligence

DATA443

4000 Sancar Way, Suite 400
Research Triangle, NC 27709

Website: www.data443.com
Email: info@data443.com

US: +1 919 526 1070
UK: +44 203 7693 700