IoC Management

MOBILIZING THREAT REMEDIATION

VERITI

SUMMARY

Mobilizing threat remediation is crucial to maintaining a proactive security stance. Veriti's IoC Management solution simplifies the integration and management of threat intelligence feeds, ensuring that all IP addresses, file hashes, domains, and URLs are consistently updated across the security environment. Additionally, Veriti facilitates cross-sharing of intelligence between vendors, ensuring that if one vendor identifies a threat, it is enforced across all others and enriched with more indicators that are implemented in other layers of security. By automating the detection and propagation of indicators of compromise (IoC), Veriti helps organizations stay ahead of attackers and reduce the workload on security analysts.

CHALLENGE

Organizations face several challenges in managing IoCs. Security tools often require manual updates, which is time-consuming and prone to human error. Identifying and responding to zero-day attacks is critical yet challenging without automated processes. Security analysts are overwhelmed with the volume of threat intelligence and alerts, leading to delays in threat detection and response. Additionally, ensuring a coordinated response across different security tools and solutions can be difficult, reducing the effectiveness of threat remediation efforts. Adding to this challenge is that the Security Operations Center (SOC) often does not have direct access to security controls, which are managed by other teams. This can lead to internal politics that delay the response to threats. The "lifetime of an IoC" without automation and cross-collaboration is typically very short, meaning that without these elements, the response is often too late to be effective.

SOLUTION

Veriti's IoC Management solution addresses these challenges with a comprehensive, automated approach. It enables the easy addition and management of threat intelligence feeds, automatically pushing updates to security tools to maintain synchronization across the environment. The solution identifies zero-day indicators of attack from any vector and mobilizes threat remediation across the security stack automatically. Automated detection and analysis of known attacks from organizational traffic reduce the workload on security analysts. Just-in-time response capabilities allow swift action against zero-day attacks by identifying, validating, and distributing attack indicators across security solutions, effectively stopping additional attack attempts. The solution ensures a consistent and coordinated response to zero-day attacks, improving the efficiency and effectiveness of security event handling.

In reality, when an analyst wants to enforce an IoC, it's not a matter of "if" other teams will review it, but "when." Veriti addresses this by taking the specific part of "ownership of enforcement" and giving it to the SOC. This reduces the load on the security teams responsible for enforcement, ensuring a more streamlined and timely response to threats. The solution ensures a consistent and coordinated response to zero-day attacks, improving the efficiency and effectiveness of security event handling.

STOP ATTACKERS DEAD IN THEIR TRACKS WITH EFFICIENT IOC MANAGEMENT

CHALLENGE

- Manual Updates
- Zero-Day Threats
- Analyst Overload
- Fragmented Response

VERITI'S APPROACH

- Automated Integration
- Zero-Day Remediation
- Automated Root-Cause Analysis
- Just-in-Time Response
- Cross-Stack Coordination

RESULTS

- Enhanced Security Posture
- Reduced Analyst Workload
- Faster Response Times
- Consistent Protection
- Proactive Threat Management

RESULTS

By automating the integration and propagation of IoCs, organizations can stay ahead of attackers and minimize vulnerabilities, enhancing their security posture. Automated detection and analysis reduce the burden on security analysts, allowing them to focus on more strategic tasks. With just-in-time response capabilities, organizations can minimize mean time to detect and react (MTTD/MTTR), ensuring threats are addressed promptly. Cross-stack coordination ensures that all security tools are updated with the latest threat intelligence, providing a unified defense against attacks. A notable example of Veriti's impact is seen with a company during the emergence of a critical vulnerability, Veriti's proactive exposure assessment and remediation capabilities were crucial. Despite the company not having patched their systems, Veriti automatically blocked an exploitation attempt, showcasing the effectiveness of its IoC management.