Nsight

Accelerating Digital Transformation

CASE STUDY

SentinelOne EDR Implementation: AI-Driven Threat Detection for a Global Manufacturer

Introduction

A global cleaning products manufacturer with over 6,000 employees operating across North America, Latin America, Europe, the Middle East, Africa, and Asia Pacific sought to overhaul their cybersecurity infrastructure. To protect critical systems from advanced threats, the company partnered with Nsight-Inc for the SentinelOne EDR implementation.

This project focused on enhancing their EndpointDetection and Response (EDR) capabilities, providing AI-driven threat detection and real-time protection across their distributed environments.

Project Objectives:

The client needed a robust security solution to protect their endpoints and infrastructure.

Their main goal was to implement scalable endpoint security solutions to provide real-time protection and automate responses to potential threats. Ensuring that the new EDR solution covered both on-premise systems and cloud environments was essential for safeguarding their global operations.

The client required a solution capable of continuously monitoring and protecting thousands of endpoints in multiple regions. This included addressing potential vulnerabilities across various infrastructure layers, integrating AI-driven threat detection, and automating responses to threats as they arise.

Pain Points: Challenges Faced by the Client's IS Team

Deployment Challenges

The client's Information Security (IS) team initially encountered challenges during the SentinelOne EDR implementation, particularly deploying agents on their numerous endpoints. Ensuring these sensors were configured correctly and functioning across various environments required meticulous planning and execution. Nsight-Inc had to address several technical barriers, including ensuring that all SentinelOne agents were healthy after deployment.

Technical Focus:
Nsight-Inc overcame deployment challenges by implementing the following steps:

Developed a structured rollout plan tailored to the client's large-scale, distributed environment, ensuring smooth execution across multiple regions.

Automated the agent deployment process, reducing manual intervention using automation tools to install SentinelOne agents on thousands of endpoints quickly and efficiently.

Conducted rigorous testing at each stage to verify that all sensors were installed, configured, and communicated correctly with the SentinelOne platform.

Minimized the risk of configuration errors and network issues by automating checks during deployment, allowing for faster identification and resolution of potential problems.

Enabled ongoing monitoring to track deployment progress and sensor health, ensuring all endpoints were protected without unnecessary delays or downtime.

False Positive Alarms

Frequent false positive alerts overwhelmed the client's IS team, disrupting their security operations. These false alarms diverted attention from actual threats and led to inefficiencies in the security operations center (SOC).

Technical Focus:
Nsight-Inc worked with the client to fine-tune SentinelOne's detection algorithms, reducing false positives and enhancing threat detection accuracy. By refining the detection thresholds and leveraging AI-driven threat detection, SentinelOne was able to differentiate between legitimate threats and benign activities.

Lack of Automation for Agent Upgrades

The client's previous endpoint security system lacked automation for upgrading security agents, requiring time-consuming manual updates. This delayed critical security patches and exposed systems to potential vulnerabilities.

Technical Focus:

Nsight-Inc automated upgrading endpoint agents using SentinelOne's built-in tools. This streamlined the update process, ensuring all agents remained up-to-date with the latest security patches without requiring manual intervention.

Nsight-Inc's Approach: Implementing AI-Driven Threat Detection with SentinelOne

SentinelOne EDR: The Chosen Solution

SentinelOne was chosen for its comprehensive Endpoint Detection and Response (EDR) features, which include AI-driven threat detection, Deep Visibility, Extended EDR, and 24/7 SOC support. The platform's ability to integrate real-time protection across both on-premises and cloud environments made it ideal for the client's requirements.

Technical Focus:

SentinelOne's AI capabilities aligned perfectly with the client's need for proactive threat detection and automated response mechanisms. The AI-driven system continually learns from threat patterns, protecting the client against new and evolving cyber threats.

Proof of Concept (POC) and Deployment Strategy

Nsight-Inc conducted an on-site Proof of Concept (POC) to evaluate SentinelOne's performance. The POC compared SentinelOne's capabilities against other EDR solutions, focusing on detection accuracy, response time, and ease of deployment. SentinelOne outperformed other tools in threat detection speed and the ability to handle large-scale deployments.

Technical Focus:

During the Proof of Concept (POC) phase, Nsight-Inc conducted a detailed evaluation of SentinelOne's EDR capabilities to ensure the solution could meet the client's stringent security, operational efficiency, and scalability requirements. Key metrics used to evaluate SentinelOne's effectiveness included:

Detection Accuracy:

Nsight-Inc measured SentinelOne's ability to accurately detect and classify threats, focusing on both known and unknown malware. The platform's AI-driven threat detection capabilities were tested against various attack vectors, including ransomware, fileless attacks, and advanced persistent threats (APTs).

- SentinelOne's performance was benchmarked against standards, ensuring it could accurately identify malicious activity without missing critical threats.

False Positives:

The number of false positive alerts was a critical metric, as excessive false alarms could overwhelm the client's security team. Nsight-Inc closely monitored how frequently SentinelOne triggered false positives during the POC. By analyzing and fine-tuning detection algorithms, Nsight-Inc was able to reduce the occurrence of false positives, ensuring the client's security team only received actionable alerts, thereby enhancing operational efficiency.

Response Times:

Another key metric was response time—the speed at which SentinelOne could detect, contain, and remediate threats. Nsight-Inc tested how quickly the platform could isolate infected endpoints, neutralize malware, and restore systems to their original state. Real-time protection capabilities were also tested, ensuring that SentinelOne could respond immediately to active threats without manual intervention, reducing the risk of a prolonged breach.

Resource Utilization:

Nsight-Inc evaluated SentinelOne's impact on system performance, including CPU and memory usage during idle and active states. The goal was to ensure the platform provided robust protection without negatively impacting endpoint performance or productivity.

Scalability:

The client required a solution capable of scaling across thousands of endpoints in various geographic regions. Nsight-Inc tested SentinelOne's ability to scale seamlessly while maintaining consistent performance, monitoring how the platform handled increased workloads without degradation in detection accuracy or response speed.This ensured the solution would effectively safeguard the client's global operations with AI-driven threat detection and real-time protection.

Learn how our SentinelOne implementation services can enhance security operations.

Technical Implementation: Deploying SentinelOne Across On-Prem and Cloud Environments

Deployment Across All Environments

Nsight-Inc successfully deployed SentinelOne agents across the client's on-premise and cloud environments, providing comprehensive endpoint coverage. The deployment included configuring SentinelOne sensors on all critical infrastructure and endpoints to ensure real-time monitoring and threat response capabilities.

Technical Focus:

Nsight-Inc followed a step-by-step deployment strategy, piloting the agents in isolated environments before scaling up to cover all endpoints. Configuring security policies and setting up automation for incident response were integral parts of the deployment process. Automated policies were implemented to trigger responses to various threat levels, ensuring rapid remediation of detected threats.

AI-Driven Threat Detection and Automation

SentinelOne’s AI-driven threat detection capabilities were essential in detecting sophisticated threats with minimal manual intervention. The AI continuously monitored endpoint behavior to detect abnormal activities, such as unusual file modifications or network communication patterns, which could indicate a security breach.

Key Benefits of SentinelOne EDR: Real-Time Protection and SOC Support

Real-Time Protection and 24/7 SOC Support

With SentinelOne’s real-time protection and 24/7 SOCsupport, the client experienced continuous monitoring and immediate responses to detected threats. The platform ensured that potential threats were addressed in real-time, reducing the risk of data breaches or system compromise.

Technical Focus:

Real-time monitoring enabled continuous visibility into all endpoints, ensuring potential threats were detected and addressed immediately, reducing the risk of prolonged exposure.

Improved detection rates:

Integrating AI-driven threat detection allowed the system to identify and classify emerging threats quickly, significantly increasing threat detection accuracy.

Reduced response times:

By automating threat responses, such as isolating compromised endpoints and initiating remediation processes, SentinelOne reduced the time it took to neutralize threats, ensuring minimal impact on operations.

Proactive threat management:

Real-time monitoring allowed the client's security team to stay ahead of potential threats, preventing attacks before they could cause significant damage.

Marketing Focus:

24/7 security framework:

Real-time monitoring allowed the client's security team to stay ahead of potential threats, preventing attacks before they could cause significant damage.

Peace of mind:

For enterprises facing an increasingly complex cyber threat landscape, this always-on security framework ensured their systems were always protected, reducing the burden on internal security teams and giving leadership confidence in their cybersecurity defenses.

Reduced operational overhead:

With automated processes and real-time monitoring, companies benefit from enhanced security without needing constant manual intervention, allowing them to focus on core business functions.

Enhanced Endpoint Security and Centralized Management

SentinelOne’s central management console allowed the client’s IT team to manage all endpoints from a single interface. This streamlined security operations, making monitoring endpoint activity, detecting potential threats, and managing incident response actions easier.

Technical Focus:

Simplified Endpoint Discovery:

Centralized control lets the IT team quickly discover and manage all endpoints from a single interface, ensuring no devices are overlooked. This enhances visibility into the entire network, enabling faster identification of new or unprotected devices

Streamlined Monitoring:

Security teams can track device health and activity in real time with all endpoints monitored through a unified console.
This reduces the complexity of managing multiple tools and systems, leading to more efficient security operations.

Efficient Threat Detection:

Centralized control improves detection by providing a consolidated view of all potential threats across the network. This makes it easier to spot patterns of suspicious activity and respond more quickly to detected threats.

Automated Remediation:

The centralized platform enables automatic threat response actions, such as isolating infected endpoints and applying patches directly from the console. This minimizes downtime and accelerates remediation efforts, ensuring security issues are addressed promptly and effectively.

AI-Driven Detection for Evolving Threats

SentinelOne’s AI-driven detection capabilities empowered the client to stay ahead of evolving threats. The AI constantly improved its detection models, allowing for quicker identification of new threats and reducing the number of false positives.

Technical Focus:

Enhanced Threat Detection Accuracy:

By leveraging AI-driven threat detection, the system could analyze large volumes of endpoint data in real-time, improving its ability to accurately identify known and unknown threats.

This advanced detection capability minimized the risk of missing critical security incidents.

Adaptive Machine Learning Models:

SentinelOne's machine learning algorithms continuously learned from past incidents, refining their detection models to become more precise. This adaptive approach allowed the system to identify evolving and sophisticated threats better, improving detection accuracy.

Significant Reduction in False Positives:

Fine-tuning the detection algorithms and adjusting sensitivity thresholds helped dramatically reduce the number of false positives. This ensured that the security team received fewer unnecessary alerts, allowing them to focus on genuine threats and improving overall operational efficiency.

Conclusion: Future-Proofing Cybersecurity with SentinelOne EDR

Long-Term Security Solution

Nsight-Inc successfully implemented a scalable, AI-powered Endpoint Detection and Response solution that was aligned with the client's long-term security goals. The SentinelOne EDR implementation addressed immediate security concerns and positioned the client for future success in a constantly evolving threat landscape.

Technical Focus:

The combination of AI-driven threat detection, automated response actions, and SOC support provided a resilient cybersecurity framework capable of adapting to new challenges, ensuring the client's systems remain secure well into the future.

Secure your organization with AI-powered EDR solutions today.

Contact Us

for a tailored cybersecurity strategy.

✉ marketing@nsight-inc.com

4633 Old Ironside Drive Suite 306 Santa Clara, CA - 95054