Automate the Advanced Analysis of Malicious & Suspicious Files

SentinelOne & CodeHunter Joint Solution Brief

Market Challenges

Enhancing Threat Protection Against Advanced Malware Threats

As the volume and complexity of malware continues to grow, security teams are overwhelmed with alert fatigue and increased false positives, leaving little time and resources to spend on complex threat detection and analysis. Threat actors persist, evolving their attacks to evade current security solutions using tactics like those you see in "hunter-seeker" malware.

Identifying and analyzing complex threats requires highly specialized analysts, time, and luck. Even when a potential threat is identified, the current generation of cybersecurity technology is unable to provide in-depth actionable intelligence without weeks, or months of manual analysis. That's often too little, too late.

Joint Solution Highlights

- Enhance threat detection
- Improve response time
- Reduce false positives
- Actionable intelligence
- Streamline security operations

Joint Solution

As threats evolve, organizations need solutions that have been built to keep up with emerging and advanced threats. Combining SentinelOne's endpoint protection capabilities with CodeHunter's malware-hunting platform's advanced threat analysis enhances the detection of unknown and sophisticated malware threats. Together, SentinelOne and CodeHunter detects, analyzes, and provides actionable intelligence on even the most complex malware threats at speed and at scale.

Integration Benefits

- **Enhance Threat Detection:** Combining SentinelOne's endpoint protection capabilities with CodeHunter's malware-hunting platform's advanced threat analysis enhances the detection of unknown and sophisticated malware threats.
- **Improve Response Time:** By automating the analysis process, the integration significantly reduces the time it takes to identify and respond to new malware threats, mitigating potential damage quickly.
- **Reduce False Positives:** The combined solution reduces false positives by providing more accurate and detailed analysis of suspicious files and activities.
- **Actionable Intelligence:** The integration provides actionable intelligence that assists organizations in taking proactive measures to protect their systems and data before they are impacted by malware.
- **Streamline Security Operations:** Integrating the two platforms streamlines security operations by providing a unified view of threats and automated response capabilities, reducing the dependency on manual efforts.

How It Works

The SentinelOne and CodeHunter integration enables automatic transmission of unknown malware threats that require advanced analysis.

When a malware threat is classified by SentinelOne as “Malicious” or “Suspicious”, the integration automatically sends these incidents to CodeHunter for instant, in-depth analysis. Unknown, zero-day, multi-part, and custom malware threats are analyzed at the binary-code level, and remediation intelligence is automatically generated. This eliminates the extended, typically manual, process of malware reverse engineering and provides the SOC actionable insights to immediately secure the endpoint.

Solution Use Cases

Automatically Identify Unknown Malware Threats in Minutes

CodeHunter identifies malware threats that are invisible to traditional security measures and provides actionable threat insights and guidance for security teams. CodeHunter automates the malware reverse engineering process, detecting and analyzing threats at the binary-code level. Security teams get immediate intelligence on otherwise undetected threat vectors missed by other security solutions, allowing them to focus on remediation and minimizing vulnerabilities.

Maximum Protection Against Emerging Threats via Seamless Integration

Customers rely on the expertise of SentinelOne and CodeHunter to detect and analyze malicious threats, offering clear guidance for remediation.

Integrating the two platforms streamlines security operations, providing a unified view of threats and automated response capabilities in minutes, reducing the need for manual efforts. The combined solution provides comprehensive protection against a wide range of malware threats, including zero-day and polymorphic malware.

Conclusion

Together, SentinelOne and CodeHunter enable security teams to automate the labor and time-intensive malware reverse-engineering process so they can keep up with the volume and sophistication of today’s threat landscape. Teams can focus on remediation, increase incident response time, and reduce vulnerabilities.

About Partners

SentinelOne | CODEHUNTER

SentinelOne (NYSE:S) is a global leader in AI-powered security. SentinelOne’s Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with speed, accuracy, and simplicity.

CodeHunter is a complete malware-hunting solution that automatically identifies, analyzes, and provides intelligence on the most advanced malware threats lurking inside and outside of your environment, just waiting to do damage. Our cloud-based technology identifies zero-day, multi-part, and custom malware threats invisible to existing security measures.

> *The SentinelOne and CodeHunter partnership is helping us streamline the path from threat detection to remediation. This seamless integration accelerates unknown malware identification and analysis, ensuring a swift response to cyber threats, and enhancing our overall cybersecurity posture.*

CISO
Major Systems Integrator

CODEHUNTER