SENTINELONE AUTONOMOUS CYBERSECURITY ANNOUNCEMENTS

STEVE MCDOWELL, CHIEF ANALYST
10/17/24

CONTEXT

SentinelOne unveiled several announcements at its recent OneCon 2024 customer event, which bring the company closer to delivering on its vision of making the Autonomous Security Operations Center (SOC) a reality.

The company's new and updated offerings bring enhanced security automation, data integration, and AI-driven threat response:

1. **Singularity Hyperautomation**: A no-code automation solution that allows for custom workflows and automates tasks like ransomware mitigation and asset compliance monitoring. It integrates with various tools to enhance SOC operations.

2. **Singularity AI SIEM**: A cloud-native AI-powered SIEM that ingests data from the security ecosystem for real-time threat detection and automated response.

3. **Purple AI Updates**: New capabilities are provided to automate alert triage, threat hunting, and investigations, reducing alert fatigue and improving response times. It uses generative AI to guide analysts and initiate autonomous investigations.

4. **Ultraviolet Family of Security Models**: Specialized LLMs designed for cybersecurity offer enhanced detection and reasoning capabilities optimized for security tasks.

Let's take a look at each.

SINGULARITY HYPER-AUTOMATION

Singularity Hyperautomation is SentinelOne's advanced automation solution for streamlining and enhancing security workflows within SOCs. It enables the no-code, drag-and-drop automation of various security tasks and processes.

Key features of Singularity Hyperautomation include:

1. **No-Code Automation**: Users can create custom workflows using a visual, drag-and-drop interface without needing programming skills. This simplifies the automation of routine security tasks, such as ransomware mitigation, asset compliance monitoring, and responses to suspicious activity or insider threats.
2. **Over 100 Integrations**: The platform offers out-of-the-box integrations with more than 100 security and IT tools, including seamless integration with other SentinelOne products, like endpoint, cloud, identity, and AI SIEM, for a unified response.
3. **Workflow Customization**: Users can build workflows tailored to their unique security needs, leveraging data from any source, using no-code access to APIs.
4. **Intelligent Automation Suggestions**: Singularity Hyperautomation suggests automation options during investigations based on peer-driven insights. This capability helps SOC teams automate repetitive and time-consuming tasks.
5. **Automated Playbook Generation**: In conjunction with SentinelOne's Purple AI, the platform can automatically generate playbooks based on real-world data and insights for responding to incidents.

SINGULARITY AI SIEM

Singularity AI SIEM is SentinelOne's cloud-native, AI-powered Security Information and Event Management (SIEM) system. Its key features include:

1. **AI and Automation-Powered**: Singularity AI SIEM uses AI and automation to enhance threat detection, investigation, and response processes, enabling real-time detection of threats on streaming data.
2. **No-Index Architecture**: Unlike traditional SIEMs that rely on indexing data for searches, Singularity AI SIEM uses a no-index approach. According to SentinelOne, this enables faster data access and eliminates

the need for pre-indexing, which speeds up the investigation process and reduces storage costs.

3. **Scalable Data Lake**: The system is built on the Singularity Data Lake, offering always-on storage for real-time data access. It allows seamless ingestion, storage, and querying of large volumes of structured and unstructured data across the enterprise.

4. **Open Ecosystem**: Singularity AI SIEM is built with an open architecture, allowing integration with a wide range of third-party security tools and IT systems. It supports the Open Cybersecurity Schema Framework (OCSF), enabling it to ingest data from SentinelOne's native solutions (endpoint, cloud, and identity security) and external sources. This capability provides SOCs with expanded visibility across their entire environment.

5. **Automated Workflow Integration**: The system facilitates the automation of workflows across different security tools and processes. It works with SentinelOne's Purple AI to provide real-time, AI-assisted threat hunting, automated alert triage, and machine-speed protection.

6. **Real-Time Detection and Response**: Singularity AI SIEM supports the immediate detection of threats and anomalies in real-time by processing data streams as they are ingested, reducing the time needed for threat identification and response.

7. **AI-Assisted Investigation and Threat Hunting**: Singularity AI SIEM integrates with SentinelOne's Purple AI generative AI-driven assistance for analysts. It can automatically translate natural language queries into structured investigations, summarize security logs, and guide analysts through the investigation process.

UPDATES TO PURPLE AI

SentinelOne introduced several new capabilities to Purple AI, its generative AI-powered cybersecurity assistant. These updates enhance the platform's ability to automate security functions, reduce alert fatigue, and streamline investigations for SOC teams.

The new features include:

1. **Auto-Alert Triage**: This new functionality automates the process of prioritizing security alerts. Purple AI uses Global Alert Analysis, which leverages insights from thousands of anonymized alerts, to better

determine true positives that require immediate attention. By surfacing the most critical "Alerts to Investigate," this feature helps reduce alert fatigue and allows security teams to focus on the most critical risks.

2. **Auto-Investigations**: Purple AI can now autonomously conduct investigations. Once an alert is prioritized, Purple AI compiles a list of investigation steps, executes them automatically, and generates a recommended verdict. This feature handles most investigative work, preserving investigative evidence in an auditable investigation notebook for future reference and compliance.

3. **Generative AI-Enhanced Workflow**: Purple AI is expanding its natural language queries. It can now summarize event logs, identify indicators of compromise (IoCs), and guide analysts through threat-hunting activities.

4. **Collaboration and Reporting**: Purple AI's investigation notebooks facilitate collaboration among SOC teams, allowing analysts to collaborate on investigations with shared insights. The notebooks also provide a detailed, auditable trail of the investigation process, reducing the time required to produce reports and improving post-incident analysis.

ULTRAVIOLET FAMILY OF SECURITY MODELS

The Ultraviolet Family of Security Models is SentinelOne's proprietary set of large language and multimodal models designed explicitly for cybersecurity use cases. Key features of the Ultraviolet models include:

1. **Cybersecurity-Specific Focus**: The Ultraviolet models are optimized for cybersecurity tasks, offering enhanced capabilities in understanding and reasoning about security problems. This includes detection efficacy by considering more contextual data in real-time.

2. **Specialized for Security Use Cases**: The models can handle security-specific workloads and challenges, such as identifying anomalies in network traffic, recognizing patterns of insider threats, and detecting advanced persistent threats (APTs).

3. **Multimodal and Large Language Models**: The Ultraviolet family includes both LLMs and multimodal models. These models can process and integrate various data types to provide a holistic understanding of security events.

4. **Improved Efficiency and Autonomy**: The new models, tuned to cybersecurity scenarios, operate efficiently, requiring fewer computational resources.

ANALYSIS

The new offerings and updates help SentinelOne maintain its competitive position in the cybersecurity market. The company is providing its ability to deliver a fully autonomous, AI-powered SOC solution. This should help enterprise customers reduce operational complexity and improve threat response times.

SentinelOne's strength lies in its focus on AI-powered automation and real-time threat detection. The company's Singularity platform integrates AI at multiple layers—across endpoints, cloud, identity security, and SIEM—allowing it to automate many security operations that traditionally require significant human intervention. Its emphasis on autonomous security provides SentinelOne with nice differentiation in a market where manual processes often still dominate.

Relative to competitors like CrowdStrike, which also emphasizes AI and automation, SentinelOne's differentiation comes from its proprietary AI models (such as the Ultraviolet Family of Security Models) designed explicitly for cybersecurity applications. Its domain-focused AI helps in improving threat detection accuracy and reducing false positives, a common challenge in security operations.

Another of the company's strengths is its focus on delivering no-code automation capabilities, as seen in its Singularity Hyperautomation offering. The ease of use and accessibility of no-code development allow SOC teams to build custom workflows without requiring deep technical expertise. This is attractive for organizations looking to implement automation quickly and without extensive overhead.

SentinelOne continues to deliver compelling solutions that keep the company at the forefront of the AI-driven, automated cybersecurity solutions market. The company continues demonstrating innovation in AI, automation, and data integration, setting SentinelOne up to capitalize on the growing demand for smarter, faster, and more autonomous cybersecurity tools.

Enterprises are well-advised to consider SentinelOne solutions as they build out autonomous cybersecurity capabilities.

NAND Research is a technology-focused industry analyst firm providing research, customer content, market and competitive intelligence, and custom deliverables to technology vendors, investors, and end-customer IT organizations.

Contact NAND Research via email at info@nand-research.com or visit our website at nand-research.com.