SentinelOne

SOLUTION BRIEF

Accelerate Triage and Investigation with Actionable Intelligence

SentinelOne & Recorded Future Joint Solution Brief

Cyber Threat Landscape

The cyber threat landscape is constantly evolving and becoming increasingly complex, with new threats emerging daily. Threat intelligence is essential for organizations to stay one step ahead of cyber threats and protect their systems from potential attacks. However, operationalizing threat intelligence can be a challenging task, as it requires proper integration with the existing security infrastructure and the ability to act quickly upon incoming data. Threat intelligence requires not only an understanding of current threats, but also the ability to anticipate future ones. As new threats and attack vectors emerge, it becomes increasingly difficult for security teams to stay on top without dedicated resources and tools. As a result, it can be difficult for security teams to keep up with all the latest threats and protect their organizations from them.

Malware analysis has become increasingly challenging in recent years due to the emergence of new and sophisticated attack methods. The number of malicious threats continues to grow at an alarming rate, making it more difficult for security teams to keep up and protect their organizations from attack. According to the AV-Test Institute, there are 560,000 new pieces of malware seen every day. This number will likely increase further due to new vulnerabilities and attack techniques being exploited in the wild.

How Extended Detection and Response Can Help

As enterprise networks become more complex and cyberattacks become increasingly sophisticated, organizations are turning to extended detection and response (XDR) solutions to keep their systems secure. XDR platforms are a consolidated security solution that provides automated detection, investigation, and response capabilities across an organization's network. They combine data from multiple sources—such as endpoints, servers, cloud applications—and use advanced analytics to detect suspicious activity or threats. The data collected by the platform is then used to alert security analysts when threats are detected or to trigger automated responses based on pre-defined rules.

With an XDR platform in place, organizations have access to real-time visibility into their networks so they can detect potential threats quickly and efficiently. Additionally, automation streamlines the detection process by providing faster triage and investigation times so that malicious actors can be identified quickly before they can do any damage. By bringing together a strong XDR foundation with unique insight into today's threat actors via threat intelligence and malware analysis, security teams can protect their organizations from a wider range of threats, quickly.

Recorded Future®

INTEGRATION BENEFITS

Accelerated Triage

Automatically enrich endpoint incidents with real-time threat intelligence from over 1 million sources

Seamless Sandboxing

Submit binaries for static and dynamic analysis by Recorded Future Sandbox

Powerful Automation

Automated enrichment and incident handling for evolving threat indicators

Integrated Intelligence & Sandboxing

By leveraging threat intelligence feeds and sandboxing technology, companies can bring evidence-driven context to their extended detection and response (XDR) solutions. This extra layer of understanding can accelerate triage and investigation into suspected malicious cyber activity. Companies implementing XDR solutions benefit from increased visibility and more accurate alerting. The cybersecurity landscape can be heavily impacted by the insights gleaned via contextual threat intelligence input, allowing businesses to make better risk management decisions as they relate to their critical assets.

Joint Solution

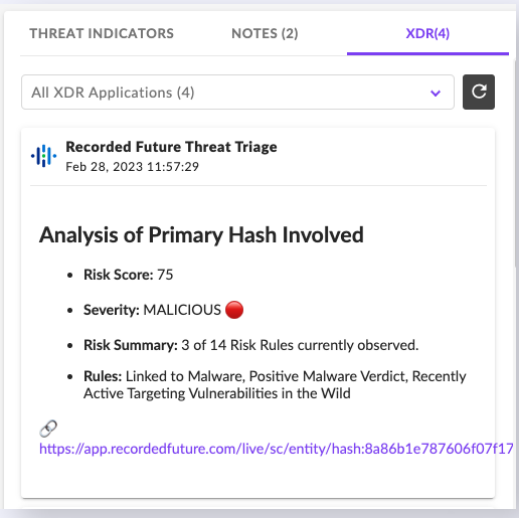
The partnership between SentinelOne Singularity XDR and Recorded Future delivers several advantages for modern organizations looking to improve their cybersecurity posture against emerging threats. This includes enhanced incident detection capabilities that can help security analysts quickly identify any suspicious activity on the network; improved triage processes that allow analysts to prioritize incidents based on severity; hunting capabilities that enable security teams to discover malicious threats buried deep within the network, and powerful automation to empower teams to act faster when it comes to mitigating any potential impact or damage caused by a breach or attack. Moreover, customers also benefit from unified security measures across their entire technology stack — allowing them to better defend their systems against attacks or breaches before they occur.

Recorded Future provides actionable threat intelligence offering detailed analysis into adversary tactics, techniques & procedures (TTPs) and specific insights about malware campaigns targeting particular industries or regions around the world. This information aids security teams by providing them with valuable data about current and possible future attack vectors that can be leveraged by malicious actors - enabling them more time to prepare preventative strategies accordingly before an incident occurs. In addition, Recorded Future also offers detailed assessment capabilities for each malicious file based on attributes like malware families, reputation scores, and risk rules.

> “
>
> Recorded Future’s security intelligence is now available in SentinelOne through a seamless integration on the Singularity XDR Marketplace. This integrated experience allows enterprises to achieve unprecedented levels of protection with SentinelOne’s platform when enriched with the actionable context provided by Recorded Future.
>
> **STUART SOLOMON**
> PRESIDENT,
> RECORDED FUTURE

Use Cases

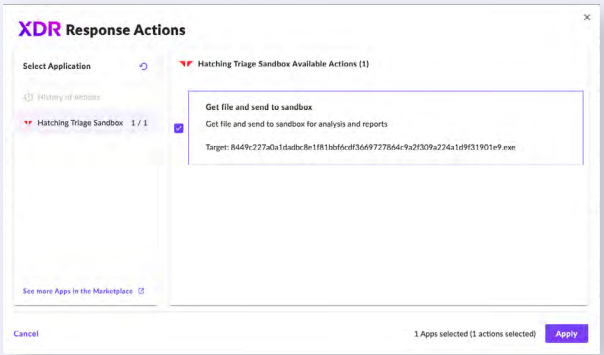
01 | Accelerated Triage



Auto-enrich XDR incidents with real-time threat intelligence from over 1 million sources. When an incident is detected by Singularity XDR, the Recorded Future Threat Triage app enriches the XDR feed with a contextual risk score, malware family, additional indicators, and a link to deeper intelligence in Recorded Future intelligence cards. The added context makes it easier for analysts to assess the incident and relevant IOCs to determine whether it should be escalated for incident response.

02 | Automated Malware Analysis

Using the Recorded Future Sandbox, suspicious or malicious files are automatically or manually sent for additional analysis. The analysis results are added as enrichment in the XDR feed, with a 1-click pivot to deeper results. Recorded Future Sandbox uses a unique architecture to scale Windows, Linux, Android, and macOS analysis capabilities. With automated analysis of file-based threats, analysts can enhance the prioritization of threats for threat hunters and incident responders.



03 | Emerging Threat Tracking

Track indicator risk over time to reopen incidents if observed indicators of compromise rise in risk level. For example, if a threat contains an indicator with a 20/99 risk from Recorded Future, an analyst may close out the incident as a false positive. The Recorded Future Threat Triage app tracks risk scores over time, so if the indicator suddenly becomes a higher risk (above a set threshold) the XDR incident will be reopened for an analyst to re-investigate.

04 | Proactive Threat Hunting

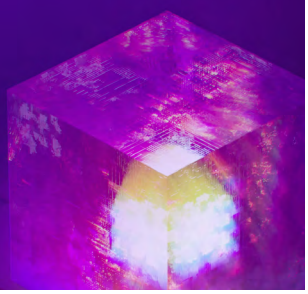
Hunt in SentinelOne using indicators of compromise from Recorded Future Intelligence cards. Recorded Future intelligence cards contain deep context emerging threats and TTPs for threat hunting. The SentinelOne Hunter Browser Extension scrapes Recorded Future for hashes (MD5, SHA1, SHA256), IPs, URLs and creates pre-built queries for threat hunting workflows.

Conclusion

SentinelOne and Recorded Future offer powerful tools that, when used together, provide comprehensive visibility across the corporate network. Their combined capabilities help security teams to reduce time spent on false positives, improve efficiency, and detect malicious threats buried deep within the network. In addition, their unified security measures across the entire technology stack better defend systems against attacks or breaches before they occur.

Singularity™ Platform

Proactively resolve threats in real-time at the site of the cybersecurity battle: the computing and cloud edge.



READY FOR A DEMO?

Visit the SentinelOne website for more details.

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733