SentinelOne

SOLUTION BRIEF

Scale Security Operations with Automated Alert Investigations

SentinelOne & Intezer Joint Solution Brief

Manual Incident Triage Limits Investigations

Manual incident triage processes are time-consuming, presenting challenges for organizations that need to scale up security operations but don't have the budget for a large in-house team or an outsourced SOC provider. The deluge of alerts from security tooling and repetitive nature of the Tier 1 analyst position makes these tasks a prime opportunity for automating your processes. Automation can alleviate the repetitive tasks of incident triage, so teams can focus their limited resources on the most critical incidents and reduce the time to respond.

Joint Solution

The combination of SentinelOne Singularity and Intezer's technologies to automatically triage incidents and escalate confirmed threats with deep investigation results. SentinelOne provides endpoint prevention, detection, response and threat hunting across all major OSes and cloud workloads. When an incident is created in SentinelOne, the artifact is automatically sent to Intezer for deep analysis and investigation down to the code level. The results of Intezer's analysis are returned in the SentinelOne console, along with a verdict and link to Intezer for additional context and prebuilt threat hunting queries. By replacing manual processes with machine speed detection, investigation results, and auto remediation, security teams can respond to incidents with greater speed and confidence.

How it Works

- SentinelOne detects malicious activity on an endpoint and creates an incident.
- Intezer monitors SentinelOne for new incidents, with SentinelOne automatically retrieving and sending artifacts from endpoints to Intezer for analysis.
- Intezer investigates and enriches the incident in SentinelOne with detailed threat context, confirms verdicts, and links to analysis results with IOCs, TPPs mapped to MITRE ATT&CK, and more.
- Leverage Singularity RemoteOps to deploy Intezer's forensic scanner across the endpoint fleet to investigate in-memory threats.
- Auto remediate incidents in SentinelOne based on analysis results from Intezer, autonomously updating and closing incidents.
- Users can dive into the linked Intezer Analysis Report to get additional IOCs and threat hunting queries to use with SentinelOne Deep Visibility.
- Additional indicators can be added to the SentinelOne blocklist or used in a Storyline Active Response (STAR) rule to alert and perform an automated response next time those indicators are seen.
- Get clear, recommended actions from Intezer for reducing noise, identifying your top threat clusters, and faster incident response.

INTEZER

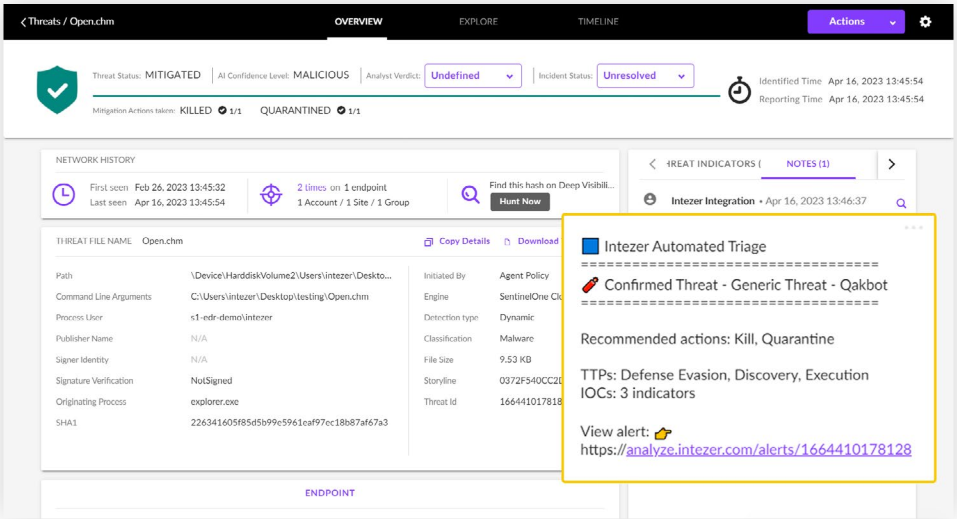
JOINT SOLUTION HIGHLIGHTS

+ Automatically triage and investigate every incident with automated analysis
+ Respond faster to escalated incidents with deep investigation results on confirmed threats
+ Reduce noise from your environment with auto-remediation and recommendations that highlight urgent threats detected by SentinelOne

> "Too many teams face challenges hiring and retaining skilled security professionals, but they can feel empowered by introducing more automation into their workflows for alert triage, response, and threat hunting with Intezer's integration that combine seamlessly with SentinelOne's platform.
>
> **Itai Tevet**
> CEO and Founder, Intezer

Solution Use Cases

Alert Triage - Automated investigation of all incidents and artifacts, giving you detailed threat analysis and confirmation whether an alert is a true positive which warrants escalation for response.



Threat Status: MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: Undefined | Incident Status: Unresolved

Mitigation Actions taken: KILLED 1/1 QUARANTINED 1/1

Identified Time Apr 16, 2023 13:45:54
Reporting Time Apr 16, 2023 13:45:54

NETWORK HISTORY

First seen Feb 26, 2023 13:45:32
Last seen Apr 16, 2023 13:45:54

2 times on 1 endpoint
1 Account / 1 Site / 1 Group

Find this hash on Deep Visibili...
Hunt Now

THREAT FILE NAME Open.chm
Copy Details | Download

Path	\Device\HarddiskVolume2\Users\intezer\Deskto...
Command Line Arguments	C:\Users\intezer\Desktop\testing\Open.chm
Process User	s1-edr-demo\intezer
Publisher Name	N/A
Signer Identity	N/A
Signature Verification	NotSigned
Originating Process	explorer.exe
SHA1	226341605f85d5b99e5961eaf97ec18b87af67a3

Initiated By	Agent Policy
Engine	SentinelOne Cl
Detection type	Dynamic
Classification	Malware
File Size	9.53 KB
Storyline	0372F540CC2I
Threat Id	166441017818

ENDPOINT

‹ HREAT INDICATORS (NOTES (1) ›

Intezer Integration • Apr 16, 2023 13:46:37

🟦 Intezer Automated Triage
====================================
Confirmed Threat - Generic Threat - Qakbot
====================================

Recommended actions: Kill, Quarantine

TTPs: Defense Evasion, Discovery, Execution
IOCs: 3 indicators

View alert: 👉
https://analyze.intezer.com/alerts/1664410178128

SentinelOne alert triaged and identified by Intezer as Quakbot.

Additional Context - Deep investigation reports that provide forensic reports on scanned endpoints, related IOCs from Intezer's database, and TTPs mapped to MITRE ATT&CK from Intezer's code-level analysis of each artifact.

Curated Threat Hunting - Intezer provides out of the box detection content and threat hunting queries that can be used within SentinelOne Deep Visibility.

Forensics - Deploy remote forensics tools with RemoteOps including Intezer Memory forensics.

Summary

When security teams are overwhelmed with alerts and experiencing alert fatigue, integrating automation into your alert triage process is key for reducing the mean time to respond to an incident.

If you are an Intezer customer, use your license key to activate the app on the SentinelOne Singularity Marketplace. If you are not yet an Intezer customer, you can book a demo at https://www.intezer.com/get-a-demo/.

INTEGRATION BENEFITS

- ✓ **Automate Incident Triage:** Monitor and triage alerts 24/7 to save time spent on benign or low-risk alerts.
- ✓ **Escalate with Context:** Confirm threats and escalate with automated analysis of every file or artifact.
- ✓ **Memory Forensics:** Use Singularity RemoteOps with Intezer's Endpoint Scanner to collect memory forensics from across your endpoint fleet.
- ✓ **Reduce Noise:** Auto-resolve more alerts and optimize your SentinelOne deployment.
- ✓ **Fast time-to-value:** No engineering required to integrate and automate processes.

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 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 Intezer

Your virtual, autonomous SOC: get high-quality and faster alert triage, incident response, and threat hunting with Intezer. Save budget by replacing costly outsourced services with Intezer's automated solution to automatically resolve 89% of false positives, deeply investigate 98% of alerts and hunt for 700 trending threats per week. Get transparent analysis reports and verdicts your team can trust to keep your business secure. Follow at @intezerlabs or read more at www.intezer.com

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733