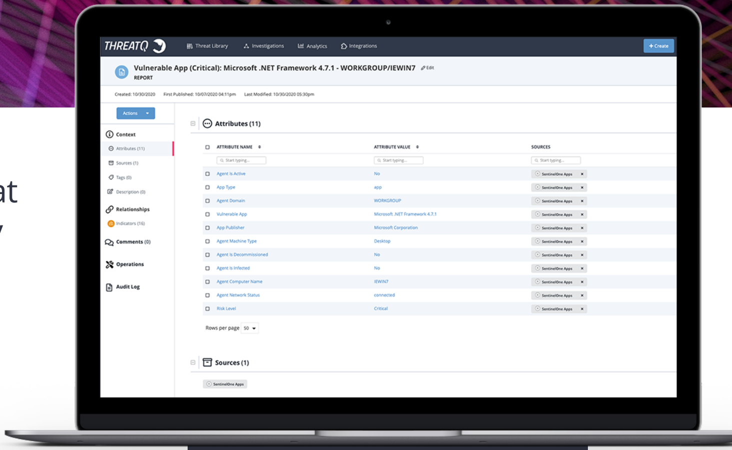
PARTNER SOLUTION OVERVIEW — SENTINELONE

THREATQUOTIENT™ SentinelOne®

THREATQ™ AND SENTINELONE

Technology Segment: Sensors

SentinelOne and ThreatQuotient unite to make threat intelligence prioritized and actionable, giving security teams greater context when performing endpoint investigations. The API-enabled integration between SentinelOne and ThreatQuotient provides security teams the upper hand when preventing, detecting, and responding to endpoint threat activity.



Vulnerable App (Critical): Microsoft .NET Framework 4.7.1 - WORKGROUP/IEWIN7
REPORT

Created: 10/30/2020 First Published: 10/07/2020 04:11pm Last Modified: 10/30/2020 05:30pm

Attributes (11)

ATTRIBUTE NAME	ATTRIBUTE VALUE	SOURCES
Agent Is Active	No	SentinelOne Apps
App Type	app	SentinelOne Apps
Agent Domain	WORKGROUP	SentinelOne Apps
Vulnerable App	Microsoft .NET Framework 4.7.1	SentinelOne Apps
App Publisher	Microsoft Corporation	SentinelOne Apps
Agent Machine Type	Desktop	SentinelOne Apps
Agent Is Decommissioned	No	SentinelOne Apps
Agent Is Infected	No	SentinelOne Apps
Agent Computer Name	IEWIN7	SentinelOne Apps
Agent Network Status	connected	SentinelOne Apps
Risk Level	Critical	SentinelOne Apps

Sources (1)

SentinelOne Apps

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

SINGULARITY XDR PLATFORM BY SENTINELONE

SentinelOne ingests prioritized threat intelligence from ThreatQuotient data collections into blocklists, which improve defenses by preventing known malicious indicators of compromise from executing across the entire endpoint fleet. Vulnerabilities identified by SentinelOne are sent to ThreatQuotient to track and aggregate potential exploits.

SentinelOne incidents triaged within ThreatQuotient are automatically enriched with context about the campaign's motivation, attackers, and intent. While an analyst investigation is taking place, affected SentinelOne endpoints can be quarantined from ThreatQuotient to stem further infection. Analysts can quickly pivot from an endpoint investigation in ThreatQuotient to a Deep Visibility threat hunt to look for additional indicators or affected endpoints. When an incident is confirmed, mitigation can be triggered from ThreatQuotient to automatically remediate or roll back the affected endpoints.

INTEGRATION HIGHLIGHTS

Infuse endpoint protection with contextualized, prioritized threat intelligence

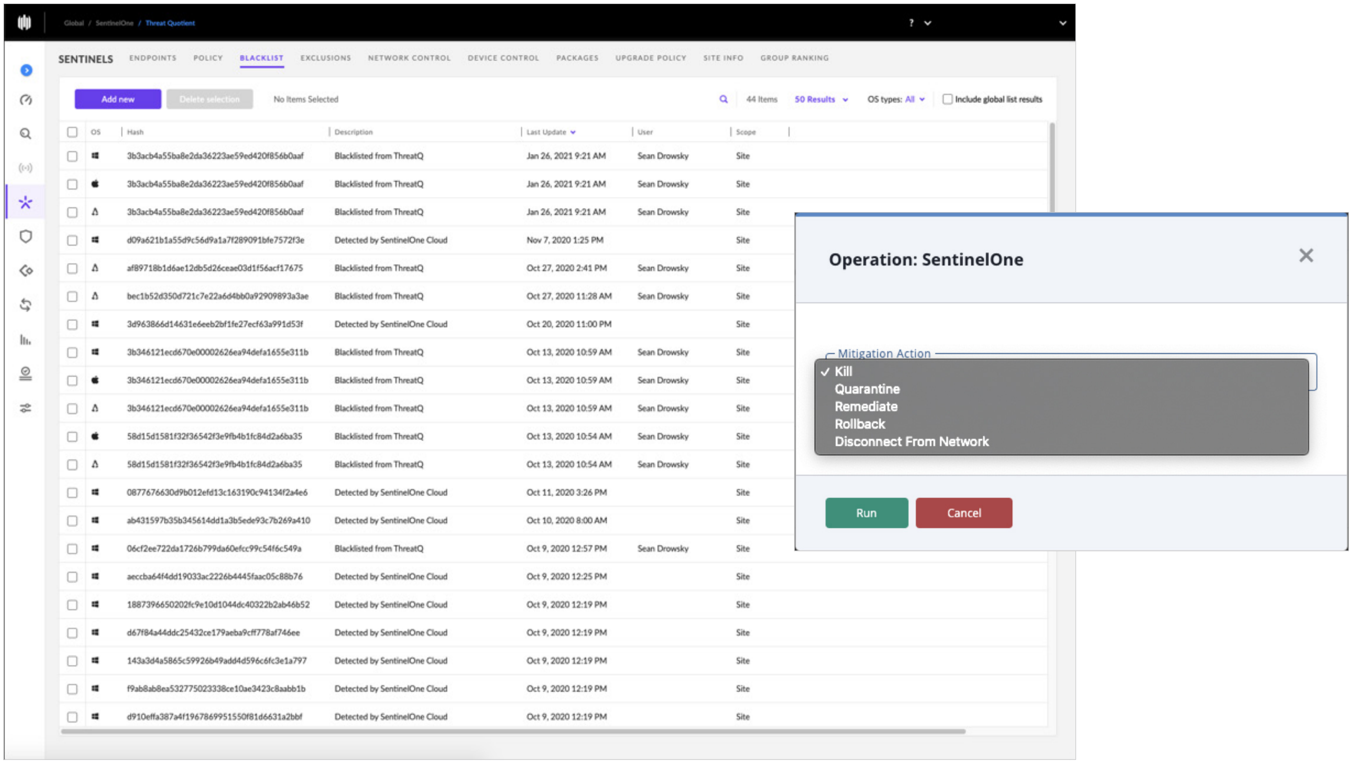
Triage and respond to endpoint threats with adversary context

One-click pivot from attack indicators to Deep Visibility threat hunting

INTEGRATION USE CASES

The Integration supports a variety of use cases such as:

- **Improve Defenses**
  Infuse endpoint prevention with contextualized, prioritized threat intelligence
- **Accelerate Response**
  Triage and respond to endpoint threats with adversary context
- **Informed Threat Hunting**
  One-click pivot from attack indicators to Deep Visibility hunting



□	OS	Hash	Description	Last Update	User	Scope
□	⊞	3b3acb4a55ba8e2da36223ae59ed420f856b0aaf	Blacklisted from ThreatQ	Jan 26, 2021 9:21 AM	Sean Drowsky	Site
□	🍎	3b3acb4a55ba8e2da36223ae59ed420f856b0aaf	Blacklisted from ThreatQ	Jan 26, 2021 9:21 AM	Sean Drowsky	Site
□	Δ	3b3acb4a55ba8e2da36223ae59ed420f856b0aaf	Blacklisted from ThreatQ	Jan 26, 2021 9:21 AM	Sean Drowsky	Site
□	⊞	d09a621b1a55d9c56d9a1a7f289091bfe7572f3e	Detected by SentinelOne Cloud	Nov 7, 2020 1:25 PM		Site
□	Δ	af89718b1d6ae12db5d26ceae03d1f56acf17675	Blacklisted from ThreatQ	Oct 27, 2020 2:41 PM	Sean Drowsky	Site
□	Δ	bec1b52d350d721c7e22a6d4bb0a92909893a3ae	Blacklisted from ThreatQ	Oct 27, 2020 11:28 AM	Sean Drowsky	Site
□	⊞	3d963866d14631e6eeb2bf1fe27ecf63a991d53f	Detected by SentinelOne Cloud	Oct 20, 2020 11:00 PM		Site
□	⊞	3b346121ecd670e00002626ea94defa1655e311b	Blacklisted from ThreatQ	Oct 13, 2020 10:59 AM	Sean Drowsky	Site
□	🍎	3b346121ecd670e00002626ea94defa1655e311b	Blacklisted from ThreatQ	Oct 13, 2020 10:59 AM	Sean Drowsky	Site
□	Δ	3b346121ecd670e00002626ea94defa1655e311b	Blacklisted from ThreatQ	Oct 13, 2020 10:59 AM	Sean Drowsky	Site
□	🍎	58d15d1581f32f36542f3e9fb4b1fc84d2a6ba35	Blacklisted from ThreatQ	Oct 13, 2020 10:54 AM	Sean Drowsky	Site
□	Δ	58d15d1581f32f36542f3e9fb4b1fc84d2a6ba35	Blacklisted from ThreatQ	Oct 13, 2020 10:54 AM	Sean Drowsky	Site
□	⊞	0877676630d9b012efd13c163190c94134f2a4e6	Detected by SentinelOne Cloud	Oct 11, 2020 3:26 PM		Site
□	⊞	ab431597b35b345614dd1a3b5ede93c7b269a410	Detected by SentinelOne Cloud	Oct 10, 2020 8:00 AM		Site
□	⊞	06cf2ee722da1726b799da60efcc99c54f6c549a	Blacklisted from ThreatQ	Oct 9, 2020 12:57 PM	Sean Drowsky	Site
□	⊞	aeccba64f4dd19033ac2226b4445faac05c88b76	Detected by SentinelOne Cloud	Oct 9, 2020 12:25 PM		Site
□	⊞	1887396650202fc9e10d1044dc40322b2ab46b52	Detected by SentinelOne Cloud	Oct 9, 2020 12:19 PM		Site
□	⊞	d67f84a44ddc25432ce179aeba9cff778af746ee	Detected by SentinelOne Cloud	Oct 9, 2020 12:19 PM		Site
□	⊞	143a3d4a5865c59926b49add4d596c6fc3e1a797	Detected by SentinelOne Cloud	Oct 9, 2020 12:19 PM		Site
□	⊞	f9ab8ab8ea532775023338ce10ae3423c8aabb1b	Detected by SentinelOne Cloud	Oct 9, 2020 12:19 PM		Site
□	⊞	d910effa387a4f1967869951550f81d6631a2bbf	Detected by SentinelOne Cloud	Oct 9, 2020 12:19 PM		Site

Operation: SentinelOne

Mitigation Action: ✓ Kill

ABOUT THREATQUOTIENT™

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA.

For more information, visit www.threatquotient.com.

ABOUT SENTINELONE

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

For more information, visit www.sentinelone.com.