SentinelOne

DATA SHEET

Vigilance MDR Escalation Process

How SentinelOne Engages with MDR Customers

SentinelOne's Vigilance Managed Detect & Respond (MDR) service subscription is designed to supplement our endpoint security SaaS offerings.

The Vigilance MDR Team is the human side to our AI-based Singularity platform. We are a 100% in-house, non-outsourced Team of Tier-1, Tier-2, and Tier-3 cybersecurity experts monitoring millions of endpoints. Our mission is to augment customer security organizations by providing a second set of eyes on the events produced by the SentinelOne deployment. Vigilance MDR adds value by ensuring that every threat is reviewed, acted upon, documented, and escalated as needed. In most cases we interpret and resolve threats in minutes and only contact you for urgent matters.

Vigilance MDR empowers customers to focus only on the incidents that matter making it the perfect endpoint add-on solution for overstretched IT/SOC Teams.

NEED MORE INFO?
Visit s1.ai/s1mdr

Vigilance MDR: From Detection to Resolution

Vigilance MDR Analysts use a documented, controlled process to work through customer incidents to ensure focused attention is placed onto what is most important. In almost all cases, analysts resolve most threats without customer interaction.

Threat Detected

AI queuing mechanisms prioritize threats

Analyst Deep Dive

Threats are classified by feature extraction, intel, ActiveEDR + Storyline, logs, and the analyst's professional judgement

Threats Insight

All console incidents are interpreted and annotated to keep you in the loop

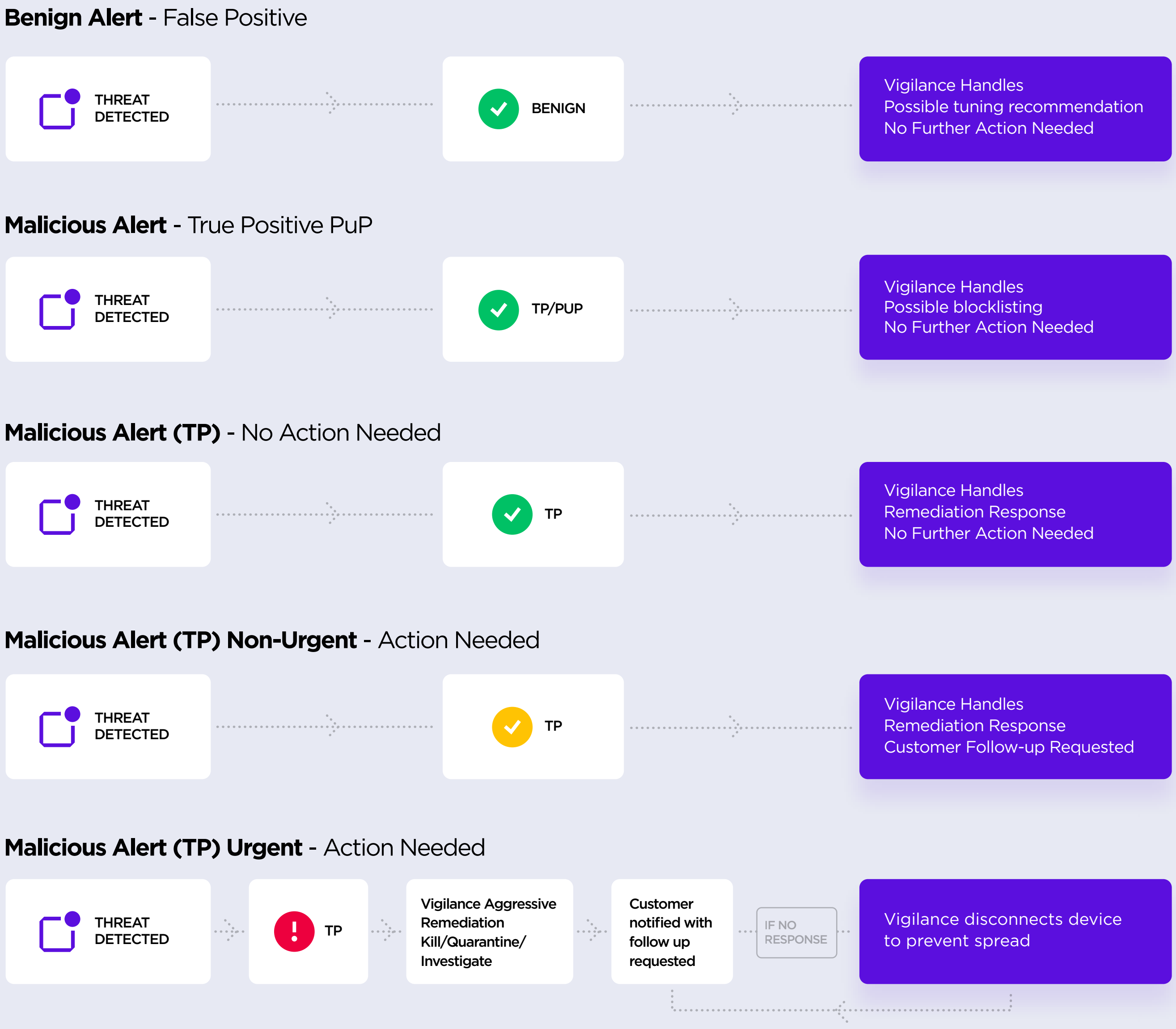
Action & Next Steps

Vigilance mitigates and resolves threats for you and opens proactive escalation as needed

Appropriate actions and resolutions are made by Vigilance Analysts depending on the situation's severity. All threats receive some level of in-console threat incident annotation. In most situations, Analysts can annotate and resolve in minutes. For incidents we perceive to be more serious, Vigilance customers are made aware via an email notification to a confirmed email alias chosen by the customer. As the situation evolves, the email thread is annotated and refreshed to keep the customer apprised. In extreme situations, the Vigilance Team may both email and call the customer or their SOC directly. In some cases, affected machines are disconnected (quarantined from) the network to slow an infection's spread while further analysis is performed (typically via Deep Visibility or remote shell if permitted by the customer) on affected machines to triage the situation. Vigilance Analysts keep the customer informed at all points.

Threat Handling Hierarchy

From Benign to Urgent True Positive threat classifications, this is what to expect from Vigilance Analysts:



Benign Alert - False Positive

THREAT DETECTED → ✓ BENIGN → Vigilance Handles
Possible tuning recommendation
No Further Action Needed

Malicious Alert - True Positive PuP

THREAT DETECTED → ✓ TP/PUP → Vigilance Handles
Possible blocklisting
No Further Action Needed

Malicious Alert (TP) - No Action Needed

THREAT DETECTED → ✓ TP → Vigilance Handles
Remediation Response
No Further Action Needed

Malicious Alert (TP) Non-Urgent - Action Needed

THREAT DETECTED → ✓ TP → Vigilance Handles
Remediation Response
Customer Follow-up Requested

Malicious Alert (TP) Urgent - Action Needed

THREAT DETECTED → ! TP → Vigilance Aggressive Remediation Kill/Quarantine/ Investigate → Customer notified with follow up requested → IF NO RESPONSE → Vigilance disconnects device to prevent spread

Benign Alert (FP)

Alert is classified as Benign False Positive

Vigilance takes proper action to resolve and annotate the console. No further actions or notifications are needed. Recurrent False alerts will be escalated to the customer to offer or approve an appropriate exclusion or agent upgrade as needed.

Malicious Alert (TP/PuP)

Alert is classified as True Positive, Potentially unwanted Program

Vigilance takes proper action to ensure the threat is blocklisted, resolved, and annotated. In most cases, a notification will not be sent to the customer alias unless there are follow up items required.

Malicious Alert (TP) - No Action Needed

Alert is classified as Malicious True Positive / No Action

Vigilance takes proper actions including Remediation to ensure the threat is isolated. Once the Analyst confirms that remediations eliminate the threat, the Analyst will send a notification to the customer's email alias alerting them to the incident as a courtesy.

Malicious Alert (TP) Non-Urgent - Action Needed

Alert is classified as Malicious True Positive Non-Urgent / Action Needed

Vigilance takes proper actions including Remediation to ensure the threat is isolated. Once the Analyst confirms that remediations eliminate the threat, the Analyst will send a notification to the customer's email alias alerting them to the incident as a courtesy. Follow up actions such as re-imaging may be recommended in some cases.

Malicious Alert (TP) Urgent - Action Needed

Alert is classified as Malicious True Positive Urgent / Action Needed

Vigilance may take aggressive actions in high priority breach cases including agent Remediation actions and disconnecting affected network[1] devices to isolate the attack and prevent further lateral movement and spread. The Analysts will send a Proactive Notification alerting the customer to the situation and request immediate Response.

No Response

If there is no response from the customer related to a Proactive Ticket, especially one classified as Urgent - Action Needed, the Analyst may attempt further customer contact via a ranked set of contact telephone numbers and backup email addresses.

[1] In urgent cases, Vigilance MDR will disconnect machine(s) before approval from the customer due to the risk to the organization.

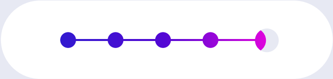
SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

96%

96% of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

Customer Satisfaction (CSAT) is ~97%



Net Promoter Score in the "great" to "excellent" range

About SentinelOne

SentinelOne founded in 2013 and headquartered in Mountain View, California, is a cybersecurity software company. SentinelOne Singularity is one platform to prevent, detect, respond, and hunt in the context of all enterprise assets.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733