

Accelerate detection and response to advanced cyber threats



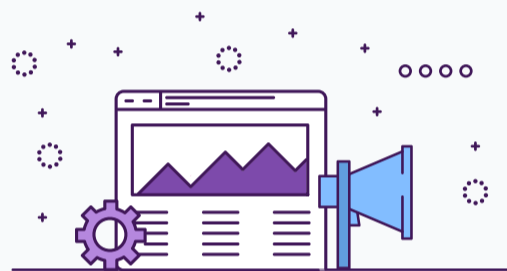
How do you handle those 3am alerts on a Saturday?

SentinelOne Vigilance provides a turnkey solution to augment your security and IT teams by accelerating the detection, prioritization, and response to advanced cyber threats and reducing your risk of missing a critical threat that goes undetected.

The SentinelOne Vigilance cyber security analysts will assess suspicious alerts, review raw data of threats,

process operations, and network connections. They will also correlate the information with threat intelligence feeds, analyze low level log-data, and collaborate with security researchers to identify and prioritize events. Vigilance security analysts will also notify security personnel and execute applicable policy-driven actions to limit the impact of any threat to your organization.

Vigilance Plans



Monitoring

First response SLA

STANDARD

- ✔ Service Onboarding
- ✔ 24/7 Coverage
- ✔ Threat Insights
- ✔ Proactive Notification
- ✔ Notifications
- ✔ Expert Consultation
- ✔ Vigilance insights report



Response

First response SLA

PREMIUM

- ✔ Includes all monitoring plan deliverables
- ✔ Threat Response
- ✔ Benign Detection Tuning
- ✔ Threat Hunting*

*Rolling out to response customers Q4'18



24 x 7 follow-the-sun SOC operations



Security events monitoring and prioritization



Hunting capabilities to detect latent threats and gain deep visibility



Accelerate response time with automated mitigation and containment



Policy tuning, exclusions, and reduction of false positives



Reporting to aid administrations gain more visibility on Vigilance handled threats, actions taken, and SLAs.