SOD SECURITY ON·DEMAND

ThreatWatch Hunt Service

REDUCE THE TIME BETWEEN A BREACH AND ITS DISCOVERY

Your time to detection window matters

Companies that identified a breach in less than 100 days saved more than $1 million as compared to those that took more than 100 days. Similarly, companies that contained a breach in less than 30 days saved over $1 million as compared to those that took more than 30 days to resolve. (IBM 2018 Cost of Data Breach study) Discovering breaches quickly reduces the attacker's reach and data loss that typically is costly to recover.

Attackers are ahead of the defenders

Even with great vigilance, threats are still evading system defenses. Your organization must be able to:

- detect the unknown threats that can attack your systems
- prevent confidential information leakage or data loss
- know if someone is going to bring your operations to a halt.

Attack methods constantly change, and the old methods of detection have become outdated. Older, 3rd Generation SIEM solutions cannot detect the newest hacking innovations. The bad guys just hide in the reduced data sets.

What is Proactive Threat Hunting?

Proactive Threat Hunting requires toolsets technology beyond what normal Security Operations maintain to perform their day-to-day threat monitoring and triage activities. ThreatWatch Hunt provides out-of-band threat hunting for malware and APTs utilizing memory forensics, which does not rely solely on device logs for detection.

With the advanced threat hunting, you can:

- Reduce dwell time (time between a breach and its discovery)
- Reduce False Posititives
- Enhance Detection Accuracy
- Identify positive threats quickly
- Respond to the attack faster

How it works

Proactive Threat Hunting integrates toolsets and methods with Security On-Demand's proprietary correlation and behavioral analysis capabilities, such as machine learning-based artificial intelligence and supervised learning models that use behavioral attack patterns.

As part of the service, SOD will:

Correlate activities with logs, alerts, and other informaiotn received.

Monitor the alerts, logs, and output provided by the advanced threat hunting activities.

Validate the threat as part of the triage and investigation process

Tune and provide continual feedback to ensure that normal system behavior is baselined.

ThreatWatch™ Hunt Benefits

- Close the gap between post event and time to detect
- Provides insight into malware that might be “hidden” on a device
- More cost-effective than additional real-time detection layers
- Denies ability of attackers to persist undetected
- Get analysis of entire customer environment, not just alerts from specific devices

ThreatWatch Hunt also enables our team to look at every device on the network, not just devices we are collecting data from. By looking at every device, we are equipped to hunt for malicious threats coming from every direction. We can look holistically at what doesn't belong or what abnormal changes occur in your environment.

ThreatWatch is a layered detection service that goes beyond what typical security protection products can analyze.

ThreatWatch Hunt will help you:

- Reduce complexity & cost of operations
- Detect threats faster and reduce impact from potential breaches
- Mitigate brand impact and business risk
- Cover departmental cyber-skills gap
- Reduce false positives that waste your staff's time
- Extend your threat monitoring coverage to 24x7

Threat Recon Unit (TRU)

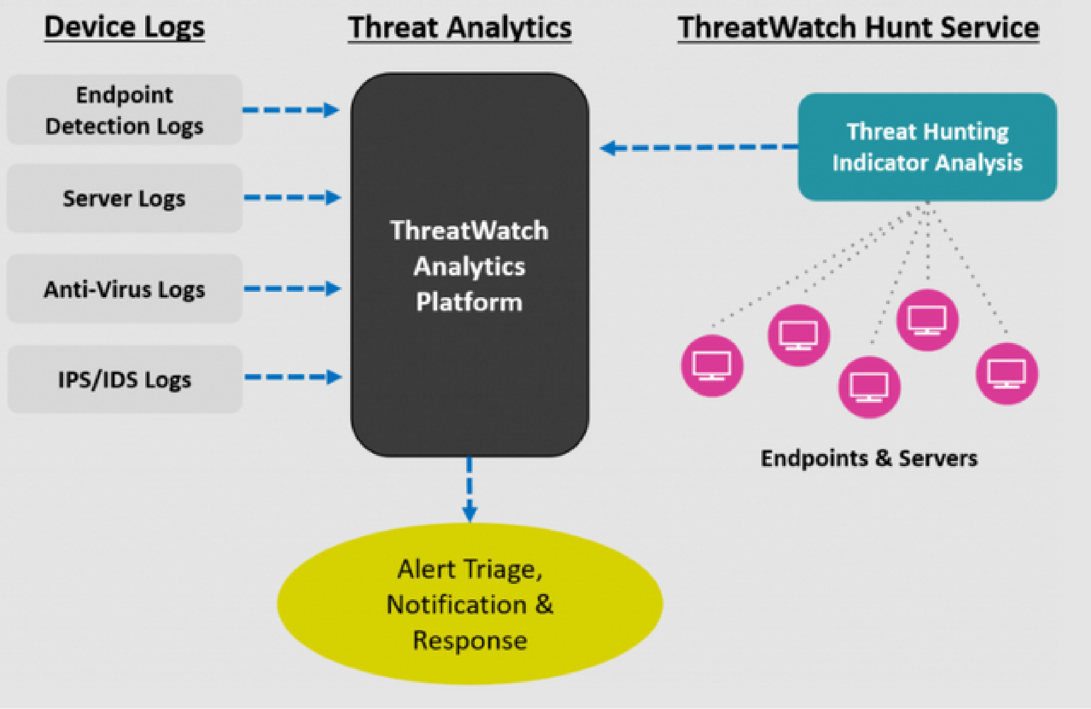
Our Threat Reconnaissance Unit identifies global cyber threats specific to your organization. The TRU uses advanced monitoring of the global internet, hunting via security operations, and counter intelligence pre-threat information. All this data is then correlated through machine learning and advanced analytics to provide you with actionable decision-making information.

TRU services include client briefings, flash alerts, advisories, whitepapers, threat research and industry and thought leadership.

The ThreatWatch Process

Our process includes three main categories: Attack prevention, threat monitoring, and threat hunting or (post-breach detection). As a part of our post-breach detection, we conduct periodic scans of network devices and send the implants and threats discovered during a sweep to the ATLAS Analytics alert platform.

Once an alert for a potential threat is received, the data is correlated with other security information and then our SOC team will respond to further triage and investigate the suspicious activity.



Pricing Model

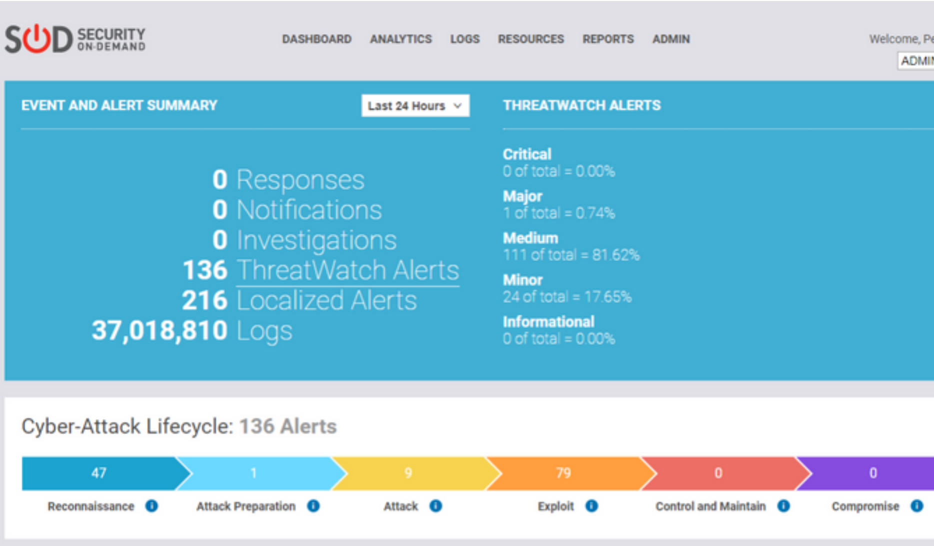
- Pay-as-you-grow, device-based pricing
- No EPD or data volume limits
- Pay a fixed monthly price per device
- Discounts for term commitments
- 100% subscription model with no hardware or license purchases required

Client Portal

- **Regulatory Compliance Reporting:** We store all of your device logs as required by PCI, SOX, GLBA, HIPAA and other regulatory requirements. We provide a holistic reporting dashboard to generate the necessary compliance reporting.

- **Instant Alert Visibility:** Situational Awareness of the current threats to systems and data assets. Visibility Tools include timelines, Node Maps, charts, graphs & other interactive visualization tools.

- **Log & Alert Analysis:** – Full access to all your data with filtering, reporting, and drill down analysis into threats, logs, and alerts. "One-click" alert drill downs, charting, graphing, threat analysis powered by our patented AQ Technology engine.



EVENT AND ALERT SUMMARY — Last 24 Hours

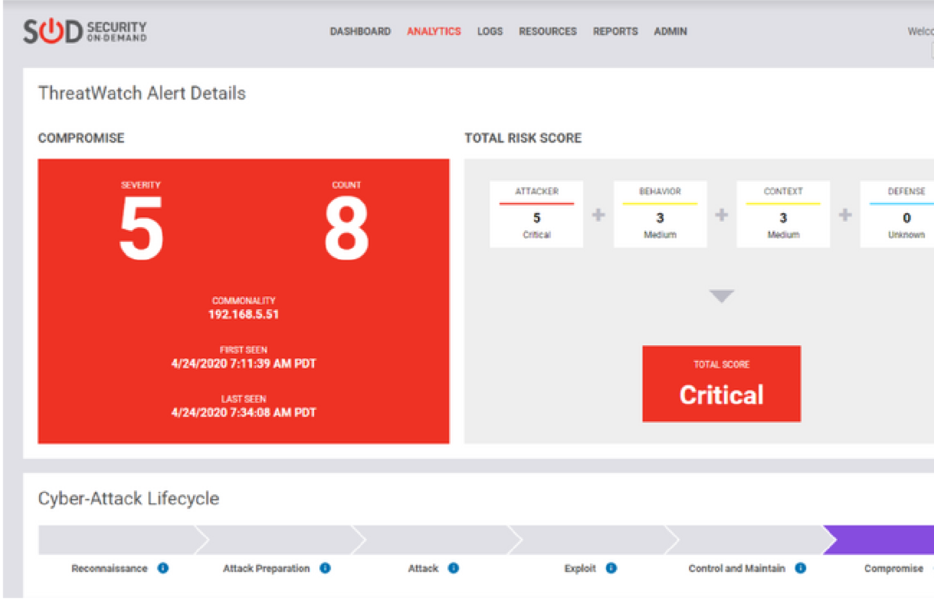
0 Responses
0 Notifications
0 Investigations
136 ThreatWatch Alerts
216 Localized Alerts
37,018,810 Logs

THREATWATCH ALERTS

Critical
0 of total = 0.00%
Major
1 of total = 0.74%
Medium
111 of total = 81.62%
Minor
24 of total = 17.65%
Informational
0 of total = 0.00%

Cyber-Attack Lifecycle: 136 Alerts

Reconnaissance	Attack Preparation	Attack	Exploit	Control and Maintain	Compromise
47	1	9	79	0	0



ThreatWatch Alert Details

COMPROMISE

SEVERITY 5
COUNT 8
COMMONALITY 192.168.5.51
FIRST SEEN 4/24/2020 7:11:39 AM PDT
LAST SEEN 4/24/2020 7:34:08 AM PDT

TOTAL RISK SCORE

ATTACKER	BEHAVIOR	CONTEXT	DEFENSE
5 Critical	3 Medium	3 Medium	0 Unknown

TOTAL SCORE Critical

Cyber-Attack Lifecycle

Why wait? Contact us for a demo.

Sales@securityondemand.com or call (858) 693-5655

Security On-Demand
sales@securityondemand.com
858.693.5655
www.securityondemand.com

Security On-Demand (SOD) provides 24x7 advanced cyber-threatdetection services for businesses and government agencies. SOD’s “security-as-a-service” solutions include24x7 advanced threat monitoring and detection, network intrusion protection, automated remediation, log analysis, and regulatory compliance solutions. For more information please visit www.securityondemand.com and follow us on Twitter @SecurityOnDemand.