SECURITY ON-DEMAND

Advanced Threat and Log Analysis Service

INCREASE YOUR TIME TO DETECTION AND GAIN VISIBILITY INTO AN ATTACK BEFORE IT WREAKS HAVOC ON YOUR SYSTEMS.

Your detection time windows are shrinking

Historically, the time it took an attacker to compromise your systems was 90 days or more. Then it changed to only a month. Then a week and then 24 hours. Now, the average time for a Russian state-sponsored hacking group to compromise a system is 19 minutes.* You can't detect and respond that quickly, no human can.

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Attack methods constantly change, and the old methods of detection have become outdated.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.

The Solution: Analyzing All the Data

The human side of analysis can't keep up with the flow of data and alerts being generated. That's why we analyze all of the data, all the time. SIEM solutions reduce the log data to a small subset and can't analyze or afford to process the full data set.

- Our layered threat analytics uses three layers of analysis to find the alerts that are actionable and indicate your real threats.

- Those alerts are further analyzed via powerful machine learning systems that prioritize and add further context for our analysts to respond.

*According to the Department of Defense, USA

SECURITY ON-DEMAND

Features

24x7 Coverage - Gain access to triage, analysis, and incident response assistance with our around-the-clock-monitoring between multiple SOC's of all security event data and alerts.

3-Types of Behavioral Threat Detection - Extend your detection capability beyond rule-based analysis systems, such as SEIMS, Firewalls, and IPS. We combine user, asset, and network behavior into a comprehensive detection capability.

Patented Analytics - Detect unknown threats via AI without the use of known threat indicators (IOC's) through our Big Data threat analytics technology (AQ).

Advanced Correlations - Enrich and improve detection ability through data integrations from DNS, Active Directory, DHCP, scan reports, and e-mail systems.

Public Cloud Integration - Collect and correlate log data in near real-time through our native integration with public cloud infrastructure (AWS, Azure) and other vendors via API.

Secure Client Portal - Gain extensive visibility through tools for alert and log analysis, interactive dashboards, and one-click visual drill-downs. Master and tiered portals are available for organizations that need to provide departmental views.

Reporting - Generate reports with our comprehensive report library, regulatory compliance reports, threat analytics reports and ad hoc query report tools.

Response - Automate your responses to quarantine systems that have been compromised or are acting suspiciously, based on defined policies or run-books.

Threat Recon Unit – Stay up to date on best security practices and SOD's threat research, publication, and investigation unit designed to apply threat intelligence, conduct campaign analysis, and expand threat research capabilities.

ThreatWatch Advanced Threat and Log Analysis will help you:

- Reduce complexity & cost of operations
- Detect threats faster and reduce impact from potential breaches
- Mitigate brand impact and business risk
- Meet regulatory compliance needs (PCI, HIPAA, GLBA, etc)
- 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.

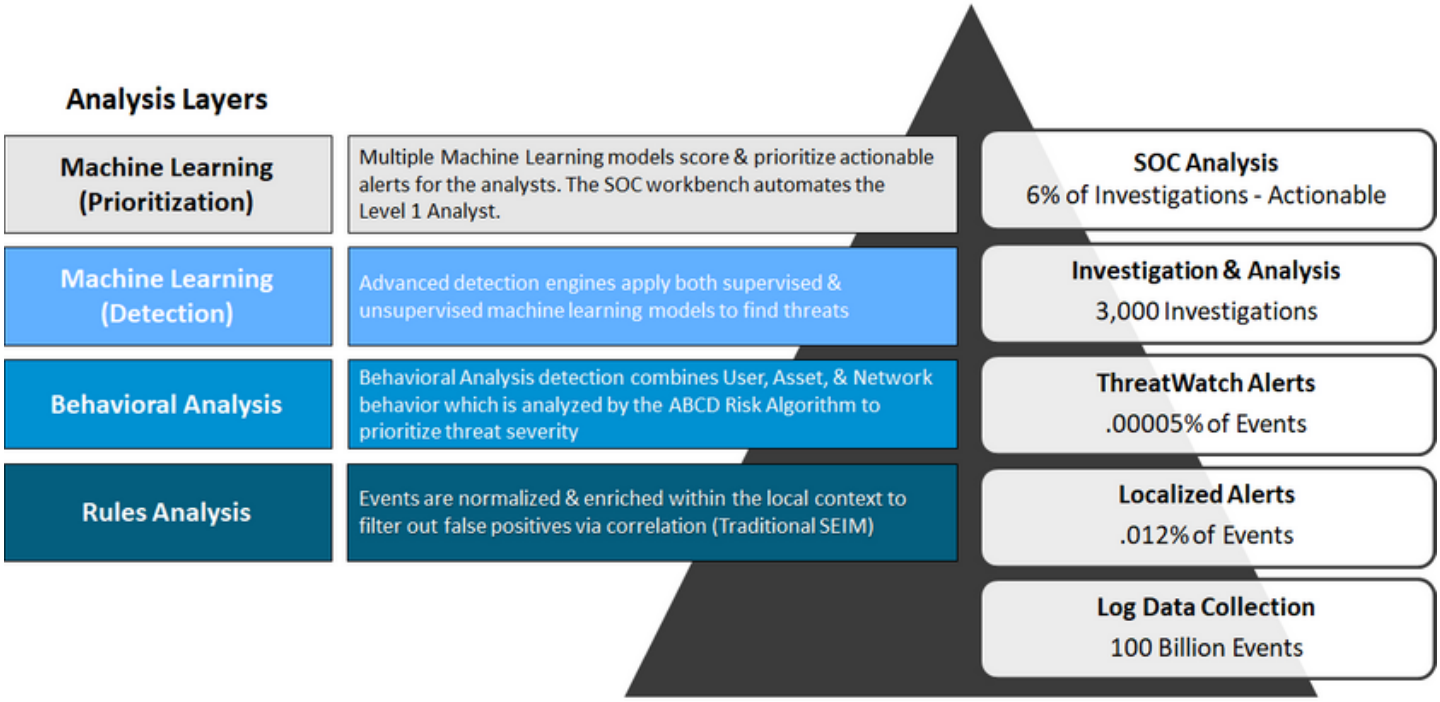
ThreatWatch™ MDR Analysis Layers

Key components of the System Architecture include:

- Human Enhanced Threat Intelligence
- AI-based Big Data Analytics (AQ Technology) to Analyze all the Data
- Rules Analysis
- Behavioral Analysis
- Machine Learning using both Supervised & Unsupervised models
- Automated Level 1 Analysis with Multiple ML models for Alert scoring and prioritization
- Human Analysis utilizing the SOC Workbench tools

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

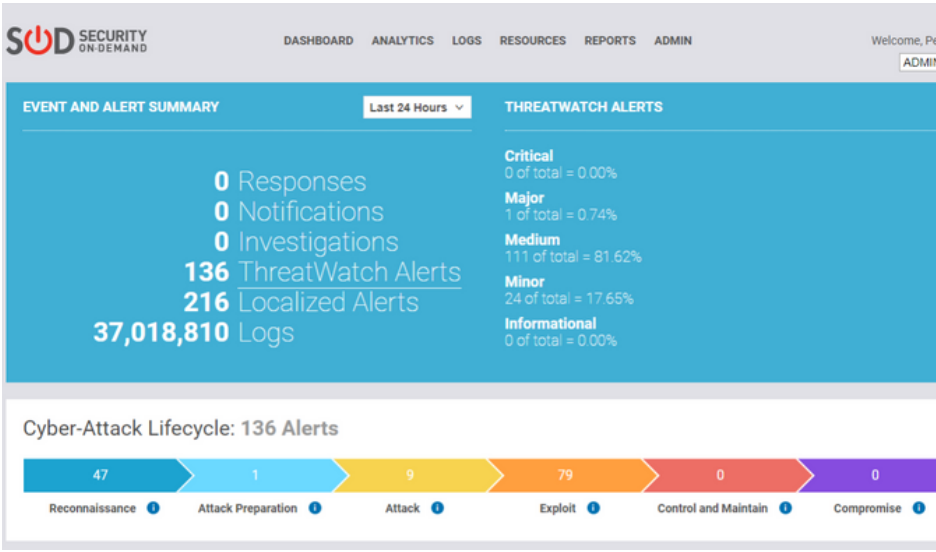


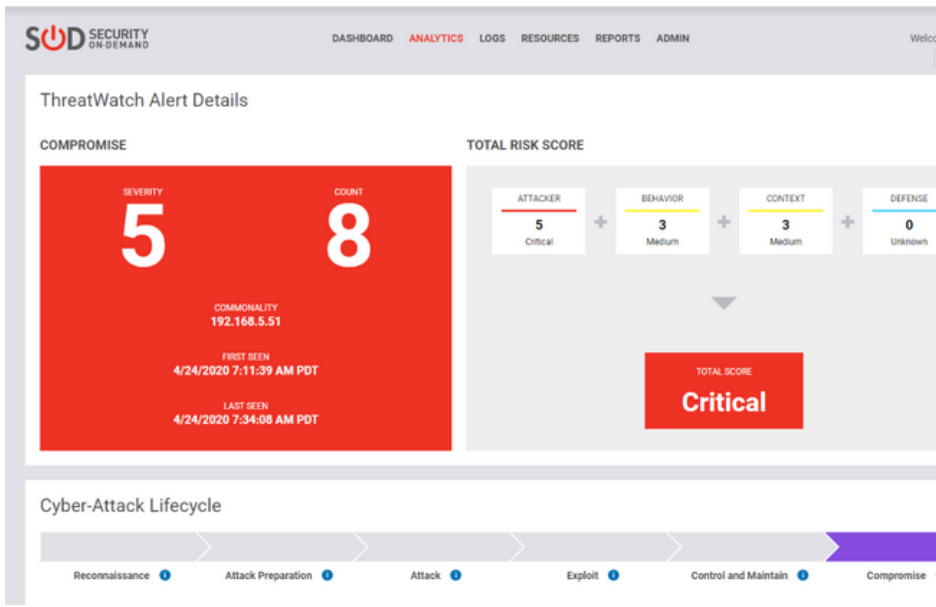
Client Portal

- **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.





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.