SECURITY ON-DEMAND

ThreatWatch 2.0

Advanced Analytics for Rapid Detection & Response to Cyber Threats

Attackers constantly evolve their approach. You need to defend your network against unknown threats. **ThreatWatch 2.0** is the next generation of threat management, combining behavioral analytics, advanced security use cases, threat intelligence and visualization to provide a higher level of situational awareness. This insight allows you to respond faster to current and emerging threats to your security.

ThreatWatch

ThreatWatch 2.0 is a platform that analyzes business data and traffic patterns to understand the behavior of users, common threat vectors, socially engineered attacks, and network patterns to identify high risk anomalies and defend customer networks and data. Leveraging intelligence gathered from across our client base, coupled with over 80 additional sources of threat intelligence, our service brings together an unparalleled level of visibility and protection.

ThreatWatch 2.0 compliments and enhances Security On-Demand's managed security services portfolio by leveraging the valuable data from all over your environment, providing a comprehensive analysis and a 360-degree view of your threat posture.

THREATWATCH 2.0 BENEFITS

- Respond faster using real-time behavioral analytics to identify and protect against security threats
- Fewer false positives
- Identify advanced threats that bypass traditional detection
- Extended protection by immediately acting on information and blocking traffic through security devices such as:
  - Firewall
  - IPS
  - Web Application Firewall
  - NAC

Behavioral Analytics	**Inbound & outbound traffic pattern analysis to identify outlier events based on time of day and non-normal analysis.**
Threat Intelligence	**IP Reputation Monitoring enhanced with data from over 80 intelligence feeds.**
Asset Discovery & Contextual Analysis	**Fingerprinting of network devices and hosts based on IP information collected from each monitored log souce to allow contexual analysis of events.**
Advanced Use Cases	**Specific use cases designed to detect security threats through advanced data analysis methods and to address specific threat vectors. Supported devices include: DNS, DHCP, Directory Services, scans integration and database.**
Visualization	**Advanced tools to bring complex data streams together in easy-to-understand graphic depictions.**

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

Security On-Demand™ is the leading provider of advanced managed security services. Our solutions help organizations protect against security threats, adhere to compliance requirements, and manage risk. Our scalable architecture eliminates capital outlay, provides 24x7 support/monitoring coverage, and lowers management, maintenance and staffing costs.