SECURITY ON-DEMAND

Advanced Threat & Log Analysis Service

You have all the right defenses in place but you know that it isn't enough. You need to do more. You want to do more. You want to have the confidence that you will be able to detect a breach when it happens – not months later.

But how? Attacks are impossibly sophisticated. They are built to sneak in under the radar, not setting off any alarms. Attackers have an advantage and they know how to leverage it. New attacks are launched every day. There are patches and signature updates, but who can keep up with all of that? And, what about the zero day attacks?

You're suffering from data overload. This isn't a problem you can solve with more people. There is just too much data flying at you, and without context, it doesn't make sense. You need an intelligent, automated way to pull it together and turn it into something meaningful. If you don't find a better way, it could take you up to 259 days to detect a breach*. You need Advanced Threat and Log Analysis Service, powered by ThreatWatch 2.0.

How it works

We collect and correlate data from all over your network into a single database. Next, we partner with you to tune our threat analytics platform, ThreatWatch 2.0, to develop a baseline of normal activity, specific to your network and users. With this baseline established, ThreatWatch 2.0 uses powerful algorithms and big data analytics to identify real anomalies, which indicate a genuine threat. These are prioritized and escalated to our cyber analysts who work with you to respond to these threats in near real time.

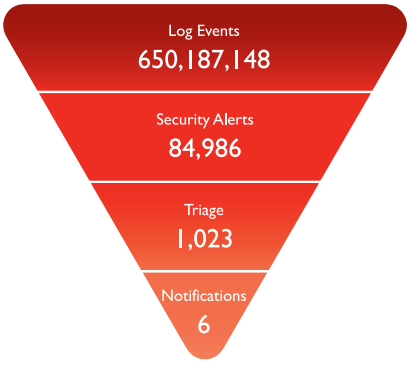
With Advanced Threat and Log Analysis Service you know:

- What devices are on your network
- What your users are doing
- Which assets are vulnerable to attack
- If and which assets are communicating with known bad actors
- If there are active threats on the network

With This Service You Will:

- Detect breaches faster
- Reduce the impact of a breach
- Minimize business interruptions
- Streamline security policies and procedures
- Improve breach investigation efficiency and reduce resolution time

Real Customer Example



30 Day window
11 Devices reporting

Situational Awareness With Actionable Data:

Our cutting edge correlation and analytics tools give your team the upper hand against cyber threats. Keep pace with high velocity data surges and the new breed of attackers.

The Bottom Line: All the noise from massive flows of log alerts is translated into a manageable stream of actionable notifications.

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.

Case Study Example:

A customer's firewall was allowing traffic out to a particular destination. Because this traffic was allowed by the firewall, the customer and most other service providers would not take a second look at this traffic. However, because Advanced Threat and Log Analysis Service examines the behavioral aspects the traffic, we took a closer look and found the traffic to be malicious.

We were able to look back historically at both the machine in question and the rest of the customer's environment to get a more detailed picture of what was really happening. Through this analysis, we discovered that at least ten machines in the environment were going out to sites associated with IPs controlled by China. We had never seen this client engaging in this activity before. We alerted the customer immediately.

Because we found this early, the customer was able to quickly contain the incident. The malware we identified was a file transfer looking for certain file types and sending them out of the network. If left unchecked, this attack could have resulted in data exfiltration and exposure of personal information or company intellectual property.

Features:

- **24 x 7 Coverage** – Around the clock monitoring of all security event data and alerts, including alert triage, analysis, & response assistance
- **3 Way Event Correlation with Behavioral Analytics** – Integrates rules, risk and behavior into a proprietary analysis decision system using patented algorithms and an advanced case management system.
- **ThreatWatch® 2.0** – Cutting edge threat analytics with industry leading security analysis tools that can provide unique detection ability to discover advanced attack vectors.
- **Advanced Security Use Cases** – Integrates logs from DNS, Active Directory, DHCP, Databases and Scans as optional data sources to enrich and improve detection ability.
- **Full Log Management** – Big data analysis technology to parse, analyze and store all log data in real-time.
- **Advanced Client Portal** – Tools for threat and log analysis, interactive dashboards, and one-click visual drill-downs. Supports Master and Tiered Portals for organizations that need to provide departmental views.
- **Reporting** – A comprehensive report library, regulatory compliance reports, threat analytics reports and ad hoc query report tools.

Benefits of the Advanced Threat and Log Analysis Service:

- **Scale** – By analyzing behavior, our technology does more of the threat identification work so we need fewer analysts to process alerts.
- **Visibility** – Correlating all of the data means we see the big picture and can easily identify what doesn't belong.
- **Speed** – We cut through the noise and bring forward YOUR critical threats in minutes, not weeks or months.
- **Compliance** – We provide the required documentation of policies, retain audit trails and deliver comprehensive compliance reporting capabilities.
- **Forensic Support** – We store full log data, which is required for forensic examination of security incidents.

Security On-Demand Can Help:

Address Compliance Needs: Performs the required logging of devices required by PCI, HIPAA and other regulatory acts. Provides a single pane of glass where you can generate the necessary compliance reporting.

Reduce Incident Response Times: By detecting threats faster and providing actionable notifications including threat summary, analysis details and recommendations.

Improve Visibility & Control: Customized parent-child views in the portal allow management staff to look at trends across the whole business while individual departments only see the information relevant to their group.

Get started today. Request your 30 minute demo of Advanced Threat and Log Analysis Service. Contact a Security On-Demand Representative by emailing sales@securityondemand.com, or call us at 858.693.5655

*2105 Cost of Cyber Crime Study, Ponemon Institute