AT&T Threat Manager – Log Analysis

Full service security monitoring, mitigation assistance, and compliance solution

Are you on data overload? Does your company need to comply with a wide variety of governmental and trade regulations in order to maintain business operations? Are you finding that keeping up with ever-evolving threats to your network is becoming impossible?

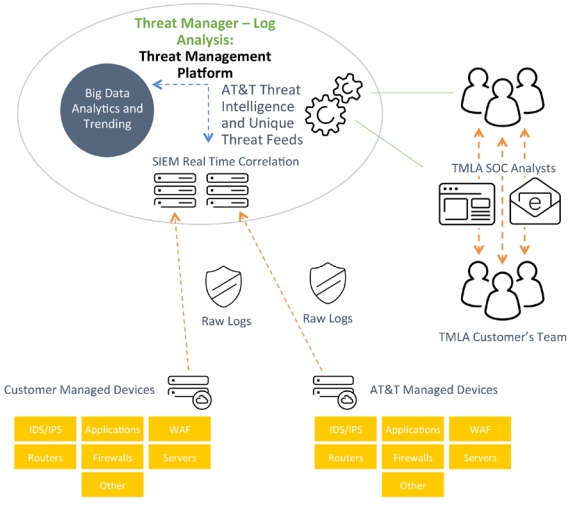
Complete Threat Analysis and Management

AT&T Threat Manager – Log Analysis (TMLA) is here to help. In harnessing the power of AT&T's Threat Intellect, the tools, processes and security experts which are the backbone of our security service portfolio, TMLA delivers real-time log monitoring, correlation and expert analysis of security activity across customer's enterprise. This improves the effectiveness of AT&T customers' security infrastructure by actively analyzing logs and alerts from the customer devices in real-time, 24x7. Our experts provide prioritization and customer notification around high and critical severity security incidents.

TMLA takes events from multiple security and networking devices, including security controls located in the AT&T network, and correlates these alerts through our threat intelligence tools. The generated alerts are prioritized and you are notified of actionable events in a manner appropriate with the assigned criticality.

TMLA provides:

- Expert threat analysis
- Remediation recommendations for critical events
- Comprehensive reports
- Log storage
- Deployment assistance
- Policy tuning
- Highly efficient user portal



Potential Benefits

- Provides a broad view of the security in your network by efficiently correlating alerts from multiple devices and device types across the entire enterprise
- Prioritizes security events based on threat and risk management methodologies
- Rapid notification when security events are detected and identified as critical by AT&T
- Helps you to be proactive vs. reactive when working to help protect your network against malicious intruders and unauthorized activities
- Helps in maintaining compliance with government and industry regulations
- Protects information against unauthorized use and assists in keeping business applications running effectively and efficiently

Features

- Security portal for service and status reporting
- Notification via email, page and person-to-person for critical security alerts identified by AT&T
- Options for equipment, monitoring and management
- Services available include emergency response teams, Security Expert on-call, log storage and outsourcing

To learn more about AT&T Threat Manager, visit www.att.com/threat-management or have us contact you.

Share this with your peers

How Does it Work?

Relevant security log and event information is collected from a customer's firewalls, intrusion prevention sensors, and other network devices including security controls within the AT&T network or on your premises using AT&T's agent-less parser/aggregator technology. This information is correlated by an AT&T database management system which prioritizes threats based on their risk to you and the ability to mitigate them.

Although the database can process a single stream of data, a diverse set of "feeds" from security devices and services is recommended to a multi-layered view of identified threats to your systems and data. The intelligence produced is reviewed by a team of AT&T expert security analysts to make the most optimal security recommendations to you regarding identified threats. This reduces your need for full time security personnel to spend their time pouring through threat data.

Notifications are made in an appropriate fashion based on the criticality of the alert with critical event notifications made person-to-person and less critical threat notifications made via email or through the AT&T Security Management portal where you can also view your current security profile and preferences. Threat Reports are distributed through the portal, or emailed, providing specific analysis to augment the information provided.

Command and Control

The AT&T Security Operations Center (SOC) is an advanced nerve center (central command and control) for identifying and directing the resolution of security issues that impact your network. The AT&T SOC has tools to aggregate and analyze all security and network event data to provide a correlated near real-time picture of what is occurring in your network on a continuous 24 hour basis, seven days a week.

Share this with your peers

For more information contact an AT&T Representative or visit www.att.com/threat-management

To learn more about AT&T Threat Manager, visit www.att.com/threat-management or have us contact you.

06/02/16 AB-3150