AT&T Security Event & Threat Analysis Service

Full service security monitoring, mitigation and compliance solution

Businesses must comply with a wide variety of governmental and trade regulations in order to maintain business operations. Many of these regulations, and industry best practices, require the regular or weekly review of security event logs from appropriate network security tools that can issue alerts as needed. Although compliance with industry mandates is a near consistent top 10 CIO priority, companies also want to strengthen their threat monitoring and existing threat identification intelligence capabilities to help reduce risk, reaction time and response to identified security issues to keep their information and assets safe.

Complete Threat Analysis and Management

AT&T has harnessed the power of our network, our strength in network security, and access to world-class processes, tools and people to provide a service that not only can help meet regulatory and industry requirements, but also address your needs for security intelligence, and the drive to proactive or rapid resolution of impeding or newly discovered threats. To help, AT&T Security Event and Threat Analysis Service takes events from multiple security and networking devices, including security controls located in the AT&T network, and correlates these alerts with proprietary AT&T technology. The generated alerts are prioritized and you are notified of events identified as actionable in a manner appropriate with the assigned criticality. The service also provides expert threat analysis; remediation recommendations for critical events; comprehensive reports; log storage; implementation assistance; and policy tuning.

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
- Assists 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 security alerts identified by AT&T as critical
- Options for equipment, monitoring and management
- Services available include emergency response teams, Security Expert on-call, log storage and outsourcing

To learn more about Managed Security Services, visit www.att.com/siem 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 get a comprehensive view of identified threats to your systems and data to take full advantage of the threat management correlation capabilities of the database. 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.

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 Event & Threat Analysis management security portal where you can also see your current security profile and preferences. Threat Reports are distributed through the portal or email providing specific analysis to augment the information provided by AT&T Internet Protect®.

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, the center provides:

- Proactive operational and situational awareness
- Detection and management of security events
- Protection against threats and exploitable vulnerabilities
- Zero hour incident response capability

AT&T makes use of these innovations and state-of-the-art tools in our Security Operations Center (SOC) and an AT&T developed integrated data mining system with a powerful query language providing an additional layer of anomaly detection algorithms that produce rich, correlated security alert information. AT&T security engineers have developed, and continue to improve, detection algorithms that run 24x7 against log information as it is processed in near real-time by the Threat Management System. Patented methods are used to efficiently process 100 million events or more per hour while generating a minimal number of "de-duplicated" security alerts.

Leveraging Innovation and Best Practices

AT&T has been focusing on network security for most of our history. We have been on the forefront of many developments that have become today's network security best practices including: a security governance policy model; risk management methodologies; defense in depth security design; firewalls; threat analysis; and multiple device security event correlation. As well as being aware of the challenges a business faces in today's complex security environment.

AT&T makes use of these innovations and state of the art tools in our Security Operations Center (SOC):

- Automatic filters built into our systems are designed to suppress duplicative alerts and alarms allowing us to focus on the identified important issues
- Focus is on identifying the known precursors of network security events and moving security controls into the core of our network

Therefore, AT&T brings a preventative approach to security with the goal of identifying, detecting and managing identified intrusions before they inflict damage. We collect, analyze, interpret and communicate data to you in near real-time, enabling fast incident response. AT&T looks for traffic anomalies and cyber attacks with a goal of identifying them in the early stages or predicting them by looking for the signs of an impending incident. This advance notice enables you to take action that can prevent damage, reduce the risks associated with impending attacks or quickly take remedial action to contain and minimize potential damage. At AT&T, security is viewed at both the macro level, addressing routers, firewalls and gateways; and at the micro level, looking at specific attacks and malware.

We have utilized our best practices, security philosophy and knowledge base to develop security analysis and threat management systems and solutions to help you protect your network and information assets.

Security Services Provided by AT&T

AT&T has a long legacy of developing security services which answer the need to address a defense in depth architecture, from the information level to the network level. You can count on AT&T as a reliable provider with true global reach for a comprehensive range of security services that can provide your business with integrated solutions to help support your complex networking environments.

Share this with your peers

For more information about AT&T Managed Security Services, visit us at www.att.com/siem, call us at 877.542.8666.

To learn more about Managed Security Services, visit www.att.com/siem or have us contact you.

04/28/14 AB-1700-02