SecureWorks

DATA SHEET

Log Management

Protect Your Infrastructure from Known and Emerging Threats

A flood of events cross your network hourly, but most of those events are irrelevant. The daunting task for you is to identify the significant events that pose a security risk to your information assets so you can respond to them in real time, before a compromise.

More Logs Than a Lumberjack

You have probably invested in a variety of technologies, such as network firewalls, IPS/IDS, VPNs, routers and switches to detect events. Every security appliance, business-critical system, noncritical server and endpoint in your organization generates extensive logs daily. These raw logs need to be monitored continuously, analyzed and correlated to filter out false positives in order to identify real security events of concern. This requires dedicated, skilled resources around the clock to review and interpret all the logs and alerts in all the different formats generated by your infrastructure.

A SecureWorks Solution

SecureWorks Log Management service monitors, correlates and analyzes logs and alerts across virtually any security technology and critical information asset, 24x7, to identify anomalies and respond to threats in real time. Deeply skilled security experts working from our integrated Counter Threat Operations Centers (CTOCs) investigate and respond immediately to any malicious activity.

Protect Against Internal and Insider Threats

SecureWorks Log Management service provides continuous vigilance over the security activity occurring in your organization. Alerts and logs are carefully analyzed by our team of security experts to detect any signs of malicious activity. This ensures that both insider threats, such as unauthorized activity, and external threats, such as zero-day exploits, are identified and thwarted before damage is done.

Easily Adhere to and Demonstrate Compliance

Regulations and industry guidelines require log monitoring of critical servers to ensure the integrity of sensitive data. Our Log Management service automates this time-intensive process. It audits your server logs in real time to identify and alert you to compliance-specific events. You can easily demonstrate compliance controls, and produce digitally signed reports containing all the activity from across your critical servers, via the secure web-based Client Portal.

Expert Management and Support

- 24x7 security event and log monitoring and analysis
- Real-time security event response
- Customized escalation procedures
- Automated log analysis and compliance reporting
- Integration with virtually any security device or critical information asset
- Powerful, asset-based security reporting
- Unlimited, unmetered access to certified security experts

24x7

Immediate Response to Security Events and Defense Against Emerging Threats

Our Log Management service protects your infrastructure from known and emerging threats in real time. Our Counter Threat Platform (CTP), strengthened by the global threat visibility we gain from monitoring billions of events every day, provides real-time information and protection against known and emerging threats around the clock. This next generation technology platform enables us to identify malicious traffic and emerging threats, and to develop intelligence-driven countermeasures to keep your critical information assets secured. All known and emerging malicious activity is immediately analyzed and responded to by our security experts. This service is tailored to your unique monitoring requirements and customized to identify specific events of interest to your organization. And escalation procedures are easily customized to your current processes, whether they are specific to a group of assets or individual devices.

View Your Security Posture and Program Effectiveness on Demand

The Client Portal provides on-demand access to management and technical level reports that can be used to view the security activity in your environment and measure the effectiveness of your security program. Hundreds of predefined and custom reports, including trending and comparative analyses, summary views and detailed lists, let you easily demonstrate compliance and security control effectiveness to both executive and technical audiences, as well as auditors and examiners.

より詳細な内容に関しては下記のメールアドレスにご連絡ください
SWRX_PreSales@Dell.com
代表03-6893-2317
www.secureworks.jp/
SecureWorks Japan株式会社

SecureWorks