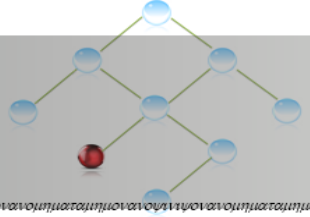
SIEM



Palindrome Technologies
ISO/IEC 17025 Accredited Laboratory
Assurance, Trust, Confidence

Host and Network Event Monitoring
Small and Medium Enterprise Networks

Palindrome's managed SIEM service acts as an extension of your organization's IT team by leveraging our qualified Subject Matter Experts to monitor and maintain your Network Security and IT Governance and Compliance requirements.

FEATURES

- **Asset Management** – Asset discovery scanning, assigned values used in risk assessment calculation
- **Alerting** - Configure and receive automatic alerts based on customized event thresholds.
- **Event Correlation** - Multiple forms of event correlation are available for all events including statistical anomalies, associating IDS event with vulnerabilities, and alerting on 'first time seen' events.
- **Log Normalization** - Normalize, correlate, and analyze user and network activity from log data generated by any device or application across the enterprise in a central portal.
- **User Monitoring** - Monitor user activity. Associate events such as a NetFlow, IDS detection, firewall log activity, file access, system error, or login failure with specific users for easy reporting and insider threat detection.
- **Full Log Indexing & Search** - All logs are compressed and stored, whether they are normalized according to a rule or left raw. Using full-text search, you can rapidly search logs for keywords, user names, IP addresses, and many other terms. Log searches are stored with an independent checksum and can be re-launched at any time.
- **NetFlow Analysis** – Collect NetFlow traffic logs from routers, switches, and other network devices.
- **Malware Detection** - monitors all processes running on Windows machines for malware processes, and can alert the security team if malware is discovered.
- **Network Content Analysis** - Analyze network traffic in real-time. Produce an accurate vulnerability report and a real-time forensic log of network events such as shared files, DNS lookups, and social network activity.
- **Vulnerability Management** - vulnerability and configuration scans and real-time monitoring

BENEFITS

- ✓ **Improve Security Monitoring and Compliance**; vulnerability management, threat monitoring, reporting and management.
- ✓ **Cost reduction**;
  - Eliminate costs associated with appliance ownership through Palindrome's product procurement and deployment channel.
  - Minimize overhead associated with recruiting in-house subject matter experts and training.
- ✓ **Minimize complexity** to align with compliance requirements

Palindrome is a leading provider of Information Security and Assurance professional services and has been supporting its customer's needs since 2005 which span several sectors including, but not limited to Telecommunications, Healthcare, Retail, Energy, Finance and Government. Our performance and commitment to deliver effective and efficient solutions to our clients allows us be recognized as a Trusted Partner for innovative and best-in-class security solutions and services.

Palindrome Technologies
100 Village Court, Suite 102
Hazlet NJ 07730, USA
www.palindrometech.com

Contact:
Christopher Reid
Tel: 732.276.9368
Email: christopher.reid@palindrometech.com