

RAVENii

Managed SIEM

Complex security solutions made simple.

Providing a simplified security solution that prioritizes the threats that put your business at risk.

RAVENii makes SIEM easy by using Alien Vault® Unified Security Management™ (USM) and RAVENii's proven managed-security framework, allowing our team of security experts to monitor your network when you're at work and more importantly when you're not.

Traditional security point-products require extensive configuration and tuning during deployment, as well as monitoring afterwards. The lack of integration with other tools means that IT teams have to dedicate significant staff time to managing each security control, and even further time to the administration of the various alerts generated by these tools.

Our unified approach eliminates the need for IT teams to spend precious time deploying and configuring individual products, conducting their own research on emerging threats or alerts triggered by their security tools.

Complex security solutions made simple.

- **RAVENii's all-in-one platform** incorporates a managed SIEM service with a managed firewall, so we can detect and respond to threats in real-time
- **Powerful SIEM technology** powered by AlienVault, one of the world's leading SIEM providers
- **Proactive event monitoring and investigation** based on your network's custom parameters
- **Managed threat detection** and response service provides layered network protection
- **Round-the-clock support**, monitoring and response by our RAVENii security experts
- **Certified security engineers** available to administer and support your network security
- **24/7/365 access** to the RAVENii Security Operations Center with SLA options to suit your business
- **Seamless integration into your network** to ensure minimal disruption and maximum effectiveness
- **End-to-end** system deployment and management

USM Platform:

- ✓ SIEM
- ✓ BEHAVIORAL MONITORING
- ✓ ASSET DISCOVERY
- ✓ VULNERABILITY ASSESSMENT
- ✓ INTRUSION DETECTION
- ✓ PRE-BUILT CUSTOM COMPLIANCE REPORTING



RAVENii Managed SIEM

Unified Security Controls

The USM platform unifies these essential technologies into a single platform, providing you with the visibility and control you need from a single management console. Instead of having to deploy and manage each of these separately, you install just one platform.

SIEM

- Log Management
- OTX threat data
- SIEM Event Correlation
- Incident Response

ASSET DISCOVERY

- Active & Passive Network Scanning

BEHAVIORAL MONITORING

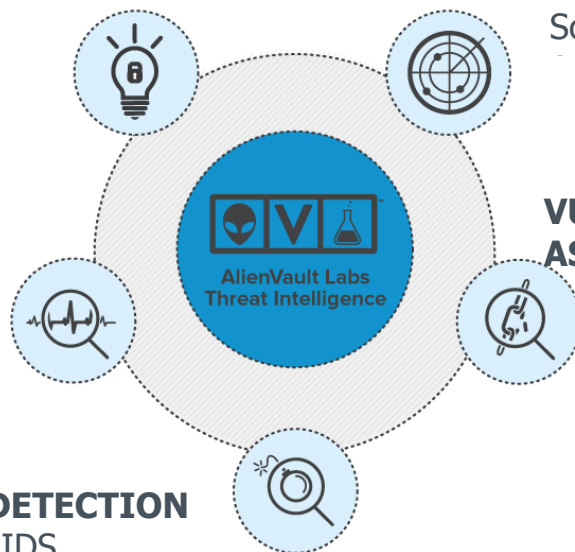
- Netflow Analysis
- Service Availability Monitoring

VULNERABILITY ASSESSMENT

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning
- Remediation Verification

INTRUSION DETECTION

- Network IDS
- Host IDS
- File Integrity Monitoring



The USM platform is designed to give you maximum flexibility to deploy exactly what you need:

- On-premise, in the cloud, or with a Managed Security Service Provider
- Physical or virtual appliances for on-premise
- All-in-One or separate components, your choice!

