X10 NETWORKS
YOUR NETWORK IS OUR BUSINESS

ALIEN VAULT

X10 NETWORKS SECURITY-as-a-SERVICE

Security-as-a-service involves organizations leveraging third-party consultants and managed security service providers (MSSPs) to monitor the security of their infrastructure.

Whether it is the need for log management, threat detection, SIEM-as-a-service, or compliance, many are choosing to outsource this service versus building the capability internally. Cost savings and overcoming staffing and skills gaps are motivating factors for outsourcing day-to-day security functions.

TOP 5 REASONS TO CHOOSE A CERTIFIED ALIENVAULT MSSP FOR SECURITY-AS-A-SERVICE

- ✓ Are you considering deploying a SIEM?
- ✓ Do you already have a SIEM in place, but you are finding it difficult to get useful, actionable data out of it?
- ✓ Are you resource or time constrained?
- ✓ Need to fill a skills gap on your security team?
- ✓ Are you struggling to find (or afford) IT professionals with security incident response expertise?

Alien Vault Certified MSSP

X10 Networks is a security-as-a-service provider leveraging the power of award-winning AlienVault Unified Security Management™ (USM™) platform for security monitoring (asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, and SIEM log management and correlation.). The all-in-one AlienVault USM platform delivers essential security controls and seamlessly integrates real-time threat intelligence from AlienVault Open Threat Exchange™ and the AlienVault Labs team to quickly identify threats affecting your network and prioritize actionable response, within minutes of deployment.

Security-as-a-service from a certified AlienVault MSSP can include:

> Vulnerability Assessment and Remediation
> Threat and Malware Detection
> Log Management, Monitoring and Archiving
> Managed SIEM
> Compliance Monitoring

FEATURES	Alien Vault USM	Traditional SIEM
MANAGEMENT		
Log Management	✓	✓
Event Management	✓	✓
Event Correlation	✓	✓
Reporting	✓	✓
Trouble Ticketing	Built-in	$$ (3rd party product that requires integration)
SECURITY MONITORING TECHNOLOGIES		
Asset Discovery	Built-in	$$ (3rd party product that requires integration)
Network IDs	Built-in	$$ (3rd party product that requires integration)
Host IDs	Built-in	$$ (3rd party product that requires integration)
Netflow	Built-in	$$ (3rd party product that requires integration)
Full Packet Capture	Built-in	$$ (3rd party product that requires integration)
File Integrity Monitoring	Built-in	$$ (3rd party product that requires integration)
Vulnerability Assessment	Built-in	$$ (3rd party product that requires integration)
ADDITIONAL CAPABILITIES		
Continuous Threat Intelligence	Built-in	Not Available
Unified Management Console for security monitoring technologies	Built-in	Not Available

X10 NETWORKS
YOUR NETWORK IS OUR BUSINESS

Contact Us

Address: 510-1199 West Pender Vancouver, BC, V6E 2R1
Phone: 1-866-442-0565
Email:info@x10networks.net
Website: www.x10networks.com

VANCOUVER | CALGARY | TORONTO | MANILA

> *In a recent SANS survey, 59% of respondents indicated that a lack of trained security staff and skills were the biggest challenges when it came to threat intelligence and detection/ SIEM initiatives*

https://www.alienvault.com/products/security-as-a-service
https://www.alienvault.com/solutions/siem-log-management

The promise of SIEM software is particularly powerful—collecting data from disparate technologies, normalizing it, centralizing alerts, and correlating events to tell you exactly which threats to focus on first. Unfortunately, achieving and maintaining the promise of SIEM is time-consuming, costly, and complex.

AlienVault USM centralizes all the security capabilities you need plus a graphical alarm dashboard that utilizes the Kill Chain Taxonomy to focus your attention on the most severe threats.

For each alarm in USM, you have a complete view of threat evidence: attack methods, related events, source and destination IP addresses, as well as remediation recommendations in a unified view, so you can investigate and respond to threats faster. USM works to reduce noisy alarms and false positives, making your work more efficient.

USM breaks out attacks into five threat categories to help you easily identify attack intent and threat severity, based on how threats interact with your environment.

- System Compromise – Behavior indicating a compromised system
- Exploitation & Installation – Behavior indicating a successful exploit of a vulnerability or backdoor/RAT being installed on a system
- Delivery & Attack – Behavior indicating an attempted delivery of an exploit
- Reconnaissance & Probing – Behavior indicating a bad actor attempting to discover information about your network
- Environmental Awareness – Behavior indicating policy violations, vulnerable software, or suspicious communications