SOLUTION SYNERGY PULSE

UNIFIED SECURITY OPERATIONS SERVICE

People

We have created an expert cyber-security team to constantly and effectively monitor your environment.

Process

Refined SOC processes that are tailored towards the subscribers needs that enable them do business securely.

Technology

We have chosen the AlienVault platform after an exhaustive evaluation of security event management platforms. We augment AlienVault in our SOC with other SOC related tools to reduce investigation and remediation times.

Contact Us

Solution Synergy
3048 E. Janelle Way
Gilbert, AZ 85298 USA
(480) 767-7660
steve.bouck@solutionsynergy.net

Ask Us About A No Cost POC

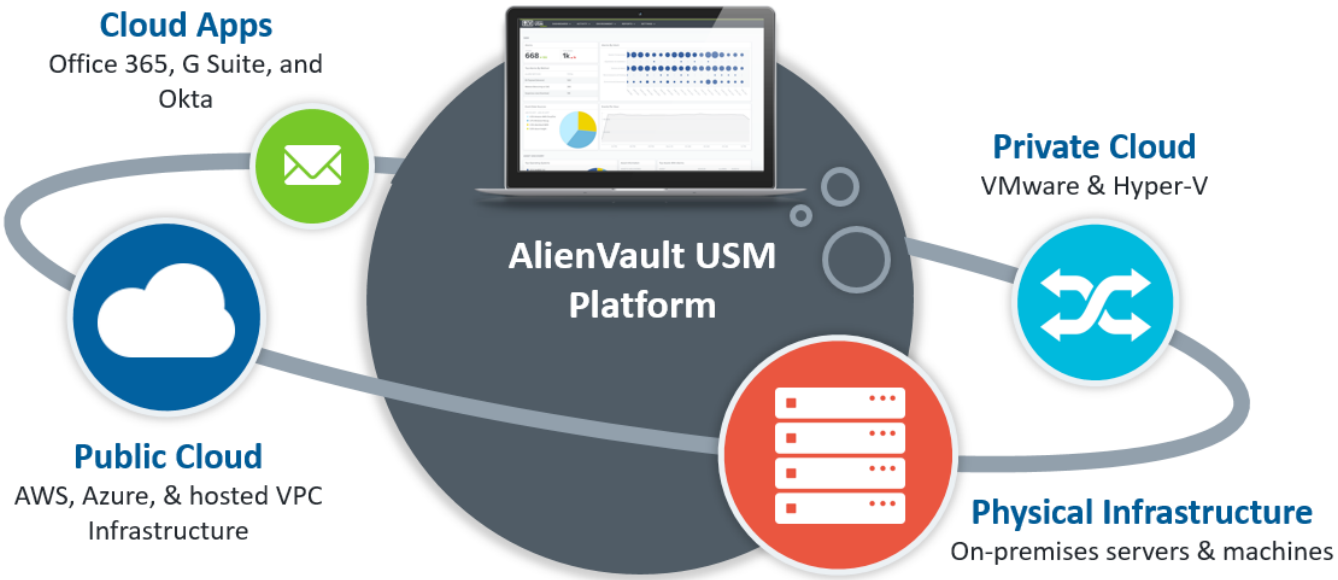
People, Process & Technology – Better Together

Solution Synergy Pulse bundles a comprehensive Unified Security Management leveraging the AlienVault platform, expert security engineering staff and a 24x7 hardened Security Operations Center.

Solution Synergy Pulse Core Offering Overview & Benefits

Feature	Benefit
24x7 – Hardened Physical Security Operations Center	Turn-Key dedicated cyber security facility housing security engineers, analysts, tools and infrastructure.
Comprehensive Unified Security Platform powered by AlienVault	Proven by over 5,000 well known customers. We have built our SOC practice using the AlienVault platform.
Asset Discovery	In order to protect we must first identify and classify what we are protecting. We will scan identified networks and set asset crtiticality ratings
Vulnerability Assessment	Scheduled Authenticated and Un-Authenticated vulnerability scanning and reporting to determine any vulnerabilities that exist on the network that may need to be addressed.
IDS (Host Based & Network Based)	Gain visibility from host machines and the network to identify potential threats.
Behavorial Analysis / Threat Intelligence	Open Threat Exchange feeds, AlienVault labs and Solution Synergy analysts monitor traffic in Realtime against known threats.to dramatically reduce exposure time.
Security Event Management	All events from all devices and networks including cloud and on-premises will be aggregated, correlated, statically and dynamically investigated so that your team doesn't have to.
Amazon AWS Security Visibility	Gain visibility into what is coming in and going out of your Amazon infrastructure
Microsoft Azure Security Visibility	Gain visibility into what is coming in and going out of your Azure infrastructure
Compliance Reporting (HIPAA, PCI, SOX etc..)	Reports to integrate your incidents and data to provide a compliance specific report and aid in your audits.
Security engineer investigation on alerts	Our security engineers will manually inspect events to determine severity and validate the threat.
Defined SLA's	Published according to level of severity. Defined risk windows
Secure Customer Support Portal	Quickly and security create new or view existing support tickets.
SIEM to SIEM Integration	If you have a SIEM currently deployed logs can be forwarded to our Alienvault SIEM and SOC services enabled.
Customer Specific Monthly Threat Review Session	Scheduled monthly calls with our SOC to review open threats and address potential gaps.
Log Integration from existing security tools (plugin enablement)	Integration of logs and netflow from existing systems as part of the deployment
File Integrity Monitoring	Support compliance requirements enabling FIM on your servers to monitor critical system file changes.

Detect Threats Across All Your Environments



The Following Add On's Are Available For The Pulse Service

Security Automation (Palo Alto, Carbon Black, Cisco Umbrella)	Detect and automatically block malicious IPs
Manual Cyber Threat Hunting	Manual hunting for dormant or stealth Advanced Persistent Threats
Office 365 Integration	Monitor O365 user, admin, and file activities for threats
G Suite Integration	Monitor G Suite user, admin, and file activities for threats
Service Now	Automatically open incident tickets based on alarms and events
VMWare	Monitor and detect threats in your VMware environment
Okta	Monitor your users' single sign-on and multi-factor authentication activities as well as your Okta accoun
Dark Web Monitoring	Monitor the dark web for your users' stolen and personal user credentials.

Five Essentials In One Platform

Asset Discovery
Know who and what is connected to your environment at all times.

Vulnerability Assessment
Find and remediate your vulnerabilities before an exploit or intrusion.

Intrusion Detection
Be alerted to suspicious activities with HIDS, NIDS, and Cloud IDS.

Behavioral Monitoring
Identify anomalous or suspicious behaviors in your environment.

SIEM & Log Management
Correlate and analyze event data from across your environment.