Splunk Offer Summary

Introduction

A growing number of organizations have recognized the need to deploy a SIEM & Log Management solution in order to satisfy audit, compliance and security monitoring objectives. However, as many industry participants have come to realize, SIEM management and monitoring requires a unique set of skills dedicated to maintaining the operations of the technology, and building useful content to derive the full value that most organizations have come to expect out of these solutions. As Gartner Inc. observed in the document SIEM Market Trends, Solutions, Assessment and Select Product Profiles:

> *"Even with today's mature product choices and proven deployment options, SIEM is not a set-it-and-forget-it technology. To ensure successful deployment, enterprises must take several steps in their evaluation and implementation: Plan to use it for both threat and compliance use cases; determine detailed threat and compliance management usage patterns; consider who in the enterprise and which third parties will implement, host and, more importantly, use the SIEM tool; and determine which toolset will be used to complement SIEM. Enterprise-grade SIEM is a powerful technology, but it requires smart people to design and run it. Many organizations struggle with SIEM their deployments, even though it is essential and widely deployed."*

Managed & Monitored Splunk Solutions powered by Alchemy Security

Alchemy Security delivers exceptional value for the price point by satisfying three major areas of Cyber Security requirements for organizations of all sizes

Incident Management	•Splunk Platform Management •24x7x365 Security Monitoring •Incident Identification, Response, and Tracking To Closure
Security Intelligence	•Real Time Situational Awareness of IT Landscape Leveraging Security Data •Provides deeper insights into Threats, Vulnerabilities and Operational Impact
Security Program Management	•CIS Top 20 Security Management Framework •Security Maturity Reporting for Executive, Management, and Practitioners •Solution Satisfies Reporting Requirements for Top 6 ("Basic") Security Controls Including Asset Management + CMDB

Alchemy Security provides three levels of service to support a wide variety of customer objectives within this rapidly accelerating market segment. SIEM Basic, Bronze, Silver, and SIEM Gold. The table below depicts various features comprising the different service levels.

Feature	Basic	Bronze	Silver	Gold
Raw Log Search Access	Included			
Unified Attack Chain Log Analysis/Structured Hunt	Not Included	Daily	24x7x365	
Threat Hunting	Not Included			Included
Honeypot Integration	Not Included	Included		
OSINT Threat Intelligence Integration	Not Included	Included		
Compliance Reporting	Not Included	Included		
Configuration Monitoring Reporting	Not Included	Included		
Advanced Security Metrics Reporting	Not Included		Included	
Annual Auditor Response Support	Not Included	Vary by Solution Size		
SIEM Content, Reporting, & Dashboard Customization	Time and Materials	Up to 3 hours upon setup Up to 1 hour per quarter	Up to 5 hours upon setup Up to 3 hours per quarter	Up to 5 hours upon setup Up to 3 hours per quarter

Service Features

Attach Chain Analysis

Alchemy Security leverages aspects of the Unified Attack Chain framework for all analysis activities. The Unified Attack chain combines the best of both worlds by combining the attack chain framework along with the MITRE ATT&CK™ framework into a holistic and unified framework.

Threat Hunting

Threat Hunting is an evolutionary approach to intrusion analysis that is considered by many practitioners to be a superior method to responding to newly identified threats and serves as a complementary overlay to traditional intrusion analysis techniques. Threat Hunting involves research, planning, and executing threat hunt activities, followed by generating a summary analysis of findings. Threat Hunting typically leverages newly published threats such as recently discovered tools, tactics, techniques and vulnerabilities that advanced threat actors are employing; or establishing areas of trust involving high risk assets or IT processing environments.

Honeypot Integration

Hunt Team Analysis is an evolutionary approach to intrusion analysis that is considered by many practitioners to be the superior method to what has historically been described as Log Analysis. Unstructured Hunt Team analysis includes daily activities to proactively seek out anomalous system or user behavior that would otherwise go undetected from network security analysis tools such as IDS or anti-malware solutions.

OSINT Threat Intelligence Integration

Our open source threat intelligence integration enriches intrusion analysis capabilities by drawing from a multiple threat lists and feeds to better corroborate true-positives as well as reduce false-positive as part of all security monitoring.

Compliance Reporting

The feature provides a number of Compliance Reports to support assessor requests. These reports may be scheduled for email delivery on a periodic basis as specified by Client, or retrieved by user initiated ad-hoc requests.

Configuration Monitoring Reporting

Configuration Monitoring Reporting serves as an additional mechanism to identify when configuration changes to host systems or network configurations and/or related security technologies have occurred

Advanced Security Metrics Reporting

Advanced Security Metrics Reporting is intended to provide a more holistic picture of security events that were observed in order to demonstrate the overall effectiveness of security controls currently in place.

Annual Auditor Response Support

Auditor support is provided to assist auditors in demonstrating compliance to operational requirements. Alchemy Security will support Client by responding to such requests via email or conference calls.

Reporting and Dashboard Customization

Reporting or dashboard customization requests are available as part of the service.

About Alchemy Security

Alchemy Security is a recognized leader for SOC Operations, Consulting, and SIEM deployments by Gartner, Inc. To learn more about our holistic approach to information security, please contact a sales representative by calling us at 970-453-2827 or via email at *sales@alchemysecurity.com* today.