Executive Overview

Alchemy Security is a boutique Managed Security Services (MSS) and Professional Services (PS) provider located in Denver CO who helps clients solve simple-to-complex security and compliance requirements for security standards such as the CIS Top 20, NIST 800-53, NIST 800-171, ISO 27001/27002, PCI, HIPAA, CCPA, GDRP, and other compliance, security, and privacy laws.

Product & Service Offerings

Managed Security Services

Alchemy Security enables clients by serving as an extension of internal teams and performs the heavy lifting required to achieve security and compliance objectives including:

Incident Management

• Splunk Platform Management

• 24x7x365 Security Monitoring

• Incident Identification

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 + CMBD

• Managed Vulnerability Scanning

• System Hardening/Policy Scanning to CIS Top 20 security framework by leveraging our GRC Tracking Tool built on Top of Splunk

Professional Services

Splunk Professional Services/Consulting

• Architecture, Planning, Deployments, & Upgrades (New deployments,/Expansion)

• Health Checks for Splunk Core and Enterprise Security

• Consulting

• Implementation of Technical Add-Ons & Applications

• Custom content development (dashboards & reporting)

Splunk Content Subscription Services

• Customized Splunk Query, dashboard & reporting development

• Security Use Case Design & Implementation

• 24+ hours per month up to a full-time resource

• Block of hours – As needed content development support and Subject matter expertise

• Network Penetration Testing

• Web Application Penetration Testing

• vCISO Services

• Risk & Controls Reviews (CIS Top 20, NIST, PCI, HIPAA, etc....)

Key Features & Differentiators

- Because their clients are looking to solver a larger set of cybersecurity requirements than just security monitoring, Alchemy Security delivers exceptional value for the price point by satisfying three major areas of Cybersecurity requirements for organizations of all sizes
- Because they pride ourselves on their expertise and client engagement, Alchemists serve as some of the best & brightest security professionals in the business
- Alchemy Security maintains a deep bench of Splunk experts who are well versed in all aspects of the platform including operations, content and Splunk application development to address complex security monitoring, compliance and reporting requirements
- Alchemy Security is a recognized leader in the field of SIEM Consulting and Operations by Gartner Inc.

Top Industries Served

- Information Technology
- Retail & Consumer Products / eCommerce

Ideal Customer Profile

Primary Target Prospect: Managed Security Services (MSS)

- Company that is interested in Splunk as a SIEM and support tool but lacks the budget, staff or wherewithal to manage and mature their security monitoring program over time
- Company that is looking to solve simple to complex security problems by maximizing the value of their MSS partner by providing three core service elements:
- *Incident Management* – Splunk Platform Management, 24/7/365 Security Monitoring, Incident Identification, Response and Tracking to Closure
- *Security Intelligence* – Real-Time Situational Awareness of their IT Landscape and deeper insights into threats, vulnerabilities, and operational impact

- *Security Program Management*
- Companies who leverage the CIS Top 20 security controls framework to track and provide Executive, Management and Practitioner reporting that depicts security program maturation over time
- Companies that seek to leverage the power of existing security data to quickly satisfy the Top 6 “Basic” controls within the CIS framework

Primary Target Prospect: Splunk Professional Services (PS)

- Company that has Splunk but is not using it to its full capabilities (i.e. needs support with use case design, dashboard & report creation/customization, log onboarding and normalization)

Qualifying & Technical Questions

1. What are some of the challenges you’re facing around Cyber Security that better data analytics could help solve?
2. Do you have any SIEM or Log Management requirements mandated by compliance or audit that you’re currently unable to meet?
3. What would better visibility into your IT Environment mean to you?

Elevator Pitch

Alchemy Security is a boutique Managed Security Services (MSS) and Professional Services (PS) provider who helps clients solve simple-to-complex security and compliance requirements for security standards such as the CIS Top 20, NIST 800-53, NIST 800-171, ISO 27001/27002, PCI, HIPAA, CCPA, GDRP and other security, compliance, and privacy laws. Because they place a high value on the client experience, they provide a holistic approach to cybersecurity and compliance management, supported by some of the best and brightest practitioners in the field to help solve the tactical and operational cybersecurity challenges our clients to face on a daily basis.

Objections & Rebuttals

Splunk is Expensive

One of the most common misconceptions of Splunk is that it’s expensive. The people that often say that do so because they either lack the expertise or manpower to unlock the tremendous amount of stored value provided from the product platform. Alchemy Security provides the expertise to maximize the value on your investment

I don’t have the staff to manage Splunk

Alchemy Security provides an entire team of Cyber Security and Splunk professionals that serve as an extension of your team at the less then the cost of 1 FTE

My friend uses an MSSP, and they continually suffer from alert fatigue with too many false positives

Alchemy Security’s Cyber Defense Center has over 170+ high efficacy security use cases out of the box and every alert that hits the channel is triaged by a human which minimizes the number of the cases that we raise to our customers attention and leads higher fidelity alerts for the ones that we do notify them on