206-247-6655 | community@arcusdata.io | arcusdata.io/services

Splunk Cloud Enterprise Security Implementation Success

Leverage Arcus Data's team of experts to help you jump start your Splunk Enterprise Security (ES) deployment in the cloud and accelerate your time to value.

This offering supports the rapid implementation of Splunk ES in the cloud and increases your overall return on investment (ROI). You benefit from the vast experience of our team, who deploy and work with Splunk every day, and the best practices we have established that ensures that ES is quickly optimized for your unique environment.

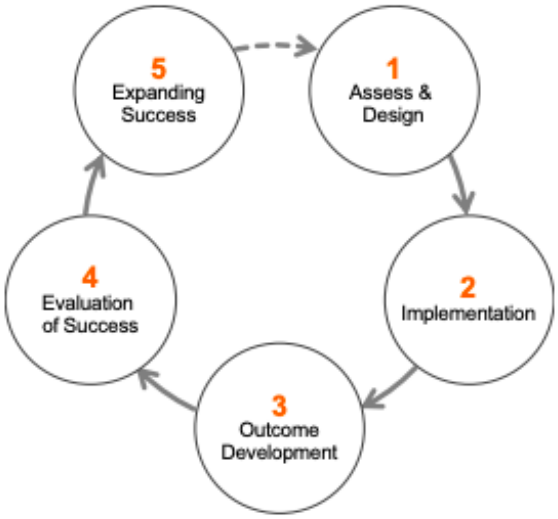
OFFERING HIGHLIGHTS

With Arcus Data you can accelerate the time to value of your Splunk enterprise security deployment with

- Our Solutions Architect designing plan around your needs
- Best-practice based Splunk configuration
- Data onboarding of essential data sources
- Installation of Enterprise Security
- Prescriptive use cases implemented

SPLUNK SUCCESS METHODOLOGY

Leveraging the experience of thousands of Splunk deployments, the Splunk success methodology will quickly bring you to your desired outcome with our enterprise security implementation offering.

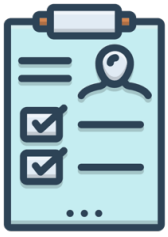


OPTIONS TO FIT YOUR NEEDS

The Splunk Cloud ES Implementation Success Offering comes in three sizes – Base, Standard, and Premium – to provide the capabilities that will optimize the implementation and TTV within your environment.

OFFERING CAPABILTIIES & FEATURES

Prescriptive Outcomes



Arcus Data recommends certain data sources and use cases to get immediate value from Enterprise Security.

All levels of this offering have a set of required data sources and a set of recommended use cases they power, to get to those outcomes.

- **The Base offering** contains a slimmed-down list of data sources and use cases for base security monitoring outcomes.
- **Standard** has a full set of recommended data sources and use cases.
- **Premium** goes beyond and can contain custom analysis and development.

Security Use Case Discovery

Arcus Data provides workshops designed to help you monitor and increase the effectiveness of your security posture.

Our experts will help you identify and customize the security queries (use cases) that will provide the greatest added benefit to your security posture and align with your business needs and risk priorities.

ES Health Check

Our Splunk Professional Services will come back twice during the first year of deployment to optimize your environment, validate any changes you have implemented, and work with your staff to increase productivity.

ES Upgrade

During the Health Check, our Splunk Professional Services will upgrade you to the most recent version of Splunk ES and review new features and capabilities with your staff.

	Splunk Enterprise Cloud Confg.	On-Prem Forwarder Installation	Data Sources	Splunk ES Configuration	Use Cases	Security Use Case Discovery	Future ES Health Check
Base	X	X	7	X	5-10		
Standard	X	X	9	X	10-20		
Premium	X	X	9+	X	20+	X	X

THREE SIZES TO MEET YOUR NEEDS

Every customer is different, so we have built three different sizes to provide flexibility to your needs. Each of our offerings includes the alignment of our experts and are surrounded by the support of our talented Delivery Managers.

Base Offering

- Base is designed for customers with more internal resources dedicated to the Splunk project.
- Internal Splunk Admins and Users will receive informal training from the Splunk Accredited Consultant and will complete tasks remaining after Splunk Professional Services finishes their work.

Standard Offering

- For customers looking for more support during the initial installation but are confident that ongoing maintenance and optimization of Splunk will be handled well by internal resources, build upon the services offered in Base with our Standard offering.

Premium Offering

- This is designed for customers who recognize the opportunity for additional business value beyond the set of initial use cases.
- Additional services beyond Standard are included, such as ongoing architectural, workshop, and optimization assistance, plus staff augmentation time to meet additional use case and outcome needs.

INCLUDED IN EVERY OFFERING

Planning

- Workshop with a Solutions Architect to develop a plan for implementation.

Coordination

- A Delivery Manager tracks your path to success

Installation

- Configure Splunk Enterprise in the cloud
- Install On-Premises forwarders to get data to the cloud
- On-board seven or nine essential data sources
- Install Splunk Enterprise Security
- Deploy and optimize 5 or more use cases (correlation searches) for your environment
- Optimizing out-of-the-box content

Training

- Providing over-the-shoulder training for your Splunk Admins
- Completing a walk-through of ES functionality for your staff
- Reviewing best practices for on-boarding data
- Reviewing best practices for creating correlation searches

DATA SOURCES

To ensure Splunk ES can provide the insights you need to make faster and smarter security decisions, you need to ensure Splunk is getting data from critical systems throughout your environment. The ES Implementation Success Offering on-boards seven to nine essential data sources:

Base Offering

- Active Directory
- Exchange
- Windows or Linux servers
- DNS
- Endpoint Anti-Malware
- Network Communication (Firewalls)
- Web Proxy Request

Standard and Premium Offering

- Mail
- DNS
- Authentication
- Endpoint Anti-Malware
- Web Proxy Request
- User Activity
- Audit Trail
- Network Communication (Firewalls)
- Network Intrusion Detection

SETTING UP QUERIES

There are certain things you should be looking for that indicate potential threats within your environment. Our team will customize use cases designed to look for indications of malicious activity on your network. These queries are the foundation of a robust security monitoring program and are recommended, based on the data sources implemented in your environment.

TARGET CUSTOMER ATTRIBUTES

The Splunk Enterprise Implementation Success offering is designed for customers looking to build a production Splunk Enterprise Security installation (without significant on-premises infrastructure) who are seeking a quick time to value for key business initiatives, from requirements gathering through production deployment.

SPLUNK PROFESSIONAL SERVICES

Our services are backed by Splunk Accredited Consultants, Solutions Architects, and Delivery Managers. They leverage Splunk best practices and experience from thousands of Splunk deployments. We only exist to get customers to valuable outcomes with their machine data – faster than they could on their own.