CREST DATA SYSTEMS

Services

Development Services

- Custom TAs & Apps
- Enterprise Security Apps
- Splunk OEM

Professional Services

- Infrastructure optimization
- Optimize searches, advanced correlations, and forecasting
- 24x7 Support

Managed Services

- Assess, Architect, and Deploy Splunk Enterprise Solutions
- Data onboarding, deploying apps
- Build custom dashboards with rich UI

Using Splunk Enterprise and ES, Crest helped us establish a baseline and setup appropriate dashboards & alerts to understand and identify anomalies in real-time.

SOC Manager, Forbes Global 2000 Financial Company

SPLUNK SERVICES

Managing & Developing Apps for Large-Scale Splunk Deployment

> **Are you maximizing your Splunk investment?**
> **Are you getting real-time insights from Splunk ES?**
> **Are you finding it difficult to hire Splunk talent?**

If you answered yes to any of the above, let's talk. Our comprehensive Splunk Services have helped companies ranging from small Startups to Global Fortune 500 Enterprises with –

- Deploying large-scale Splunk infrastructure, onboarding data from various IT Ops, Security, and IoT data sources, and upgrading Splunk
- Building custom Apps that follow Splunk best practices
- Implementing customized professional and managed services for Day-0 (Architecture & Design), Day-1 (Installation & Setup), and Day-2 Operations (Maintenance & Upgrades) with our certified Splunk Architects and Consultants

Customers rely on Splunk to make sense of their machine data from various domains such as IT Operations, Security, IoT, Big Data, DevOps, Business Analytics, Cloud Solutions, Log Management, and more—accessible, usable, and valuable through collection, storage, indexing, and search capabilities.

Development Services **Professional Services** **Managed Services**

Crest Data Systems is a leading App Development, Managed Services, and Professional Services Partner of Splunk that was recognized by Splunk as its "APAC Services Partner of the Year" for FY19. Crest has built 250+ Splunk Apps & Technology Add-ons (TA) for customers ranging from Global Fortune 500 companies to Silicon Valley Startups in IT Ops, Security, and IoT. With a dedicated team of Splunk-certified Engineers, Administrators, and Consultants across the US and India, Crest provides Professional Services & 24x7 Managed Support Services to Splunk Enterprise & Cloud to customers across USA, Europe, and APAC. Learn more about us at www.crestdatasys.com

Development Services

Proven Expertise. Agile Development. Certified Apps.

250+	Apps & Add-ons
80+	Security Apps
4	ITSI Modules

Why CREST?

We've built several Splunk IT Operations, Security, and IoT Apps and add-ons for several Fortune 500 companies as well as Silicon Valley startups. Once we gather your requirements, we manage your complete software lifecycle, including App Development, QA, Automation, Posting App on SplunkBase, Documentation, TOI, and Support. We follow Splunk's best practices and implement advanced Splunk features to get the most out of the App.

IT Operations

Crest builds Splunk applications that help IT administrator's trouble shoot problems faster. We can help you develop modules for Splunk ITSI and ES environments, optimize search queries & correlate data, build intuitive workflows with interactive UIs and help comply with best practices.

Security

Whether you are a security product vendor or an InfoSec admin, Crest security experts can help you develop modules for Splunk Enterprise and ES and build intuitive workflows with rich UI. We help create & optimize search queries to correlate security data across multiple data sources. We also build bi-directionally between your products and Splunk, using Adaptive Response framework.

Security Automation with Adaptive Response

CREST can help build bi-directional automation workflow across heterogeneous security appliances and Splunk to rapidly find and remediate ongoing threats using Splunk Enterprise Security's Adaptive Response capability.

Learn more about Crest-built Splunk apps:
https://splunkbase.splunk.com

CREST DATA SYSTEMS

Key Benefits

Improve Splunk Uptime

- 24x7 Support
- Improve SLA
- Meet Compliance criteria

Splunk-Certified Engineers

- Experienced team of Splunk Admins and Consultants
- Follow Splunk best practices

Reduce Operational Costs

- Reduce OpEx costs of Splunk Admin by up to 60%
- Splunk personnel costs 2X that of Splunk License
- Lower Splunk TCO by up to 30%

Advanced Security Analytics

- Improve Security
- Mitigate Threats
- Security Automation with Adaptive Response

Professional & Managed Services

24x7 Support. Improve SLAs. Lower TCO.

IT Infrastructure and Security Challenges

Enterprises today require Big Data security solutions to gain broader insights into cyber attacks. Continuous security monitoring is essential to remain a step ahead of threats. However, IT infrastructure deployment can be challenging, while day-to-day operations can be even more daunting. MSPs help them streamline their operations, reduce infrastructure management costs, and adhere to stringent security and compliance standards.

Splunk for IT Ops and Security Ops

Managing Splunk for IT operations and security, whether on premise or in the cloud, is demanding. Both play a central role in aggregating information from various security appliances, IT applications, and IT infrastructures. Customers need expertise not only with Splunk, but with their peripheral IT functions such as IT ticketing and change management systems, as well as applications, infrastructure, security and compliance requirements.

CREST's Splunk Professional & Managed Services

Architecture
- Design Scalable Infrastructure
- Optimize Performance
- Capacity Planning

Data Onboarding
- Standard & custom data sources
- Parsing & Normalizing Data for CIM compatibility

Dashboards & Alerts
- Visualizations with drill-downs
- Take alert-based actions using AR Framework

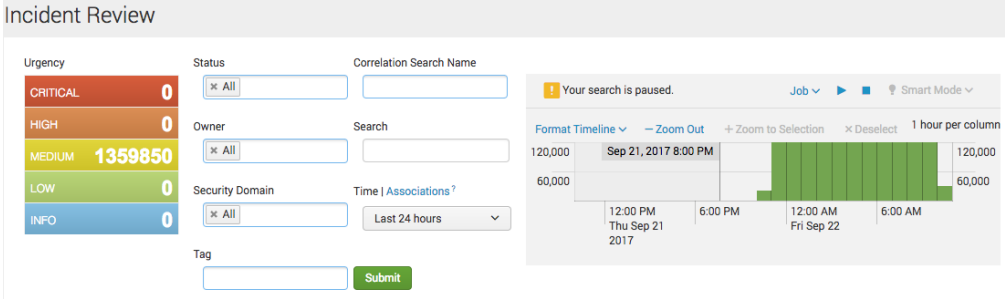
Infrastructure Admin
- Health check of Splunk clusters
- Role-based Access Control
- Data Archiving & Retention Policy

Custom Use Cases
- Configure custom Data Sources
- Create custom Correlations
- Build new Dashboards

Asset & Identity Management
- Automate Asset Discovery
- Categorize assets & Identities
- Add context to Security Events

Threat Intelligence (TI)
- Configure new threat sources
- Add context by comparing TI content to indexed events

Migration Services
- Move to AWS or Splunk Cloud
- Migrate from legacy SIEM to Splunk Enterprise Security (ES)



Case Study: Development Services

Cisco builds a Splunk App with rich UI to enable its SDN customers monitor KPIs using Splunk easily

180% Improvement in Query search-time

3,500 App & TA Downloads

250+ Dashboards

Customer Challenge

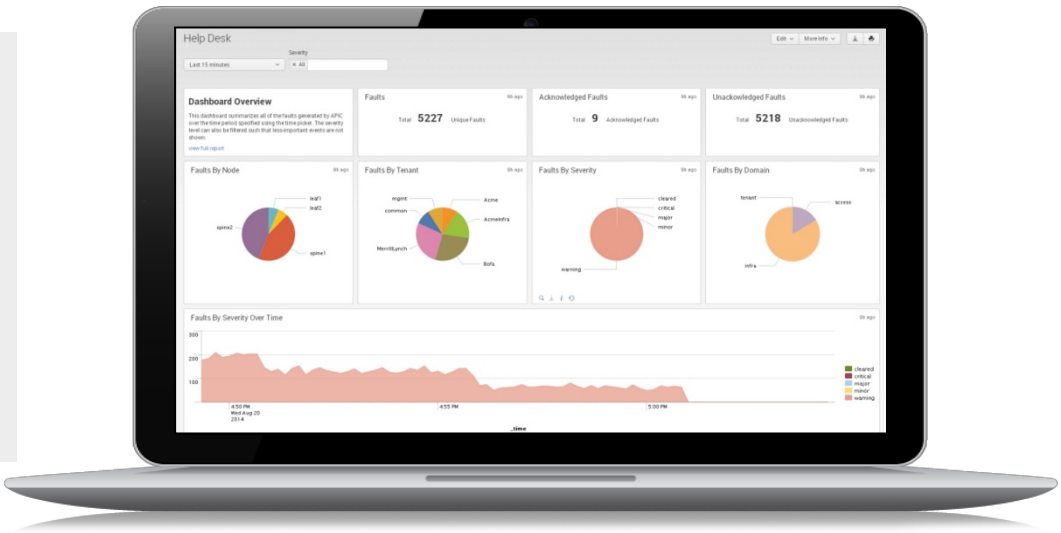
Cisco Application Centric Infrastructure product reduces TCO, automates IT tasks, & accelerates Data Center application deployments by using business-relevant software defined networking (SDN) policy model across networks, servers, storage, security, and services. APIC Controller manages storage, compute and network for all applications in your Data Center. Therefore, it becomes extremely complex for administrator to get continuous visibility into the infrastructure and monitor important KPIs on a regular basis.

The CREST Difference in 90 Days

Splunk App for ACI provides a single point of management for all the customer's data and lets the administrator track and escalate issues easily across different roles in the organization. This app provides dashboard visibility based on various roles in the ACI deployment. The app consists of a technology add-on (TA) as well as variety of dashboards and reporting interfaces (App). The add-on collects data from APIC controller via the Splunk universal forwarder and REST APIs. Once this data is collected in Splunk, the add-on provides the parsing configuration and the app provides the reporting interface.

Following dashboards provided in the app help the administrator track important aspects of the infrastructure easily:

- Authentication Dashboard
- Helpdesk Dashboard
- Fabric Inventory Dashboard
- Tenant Dashboard



> *Crest collected our product's data using API, syslogs, and custom scripts and correlated it to provide deep operational insights. Their ability to gain domain expertise and their professionalism exceeded our expectations.*
>
> ***Sr. Director, Tech. Marketing***
> ***Cisco, Inc.***

Case Study: Professional Services

Re-architecting, Automating, and Migrating Splunk Enterprise from one AWS Region to another without any downtime

0	**Downtime**
300TB	**Data Migrated**
50+	**Splunk Use Case Automation**

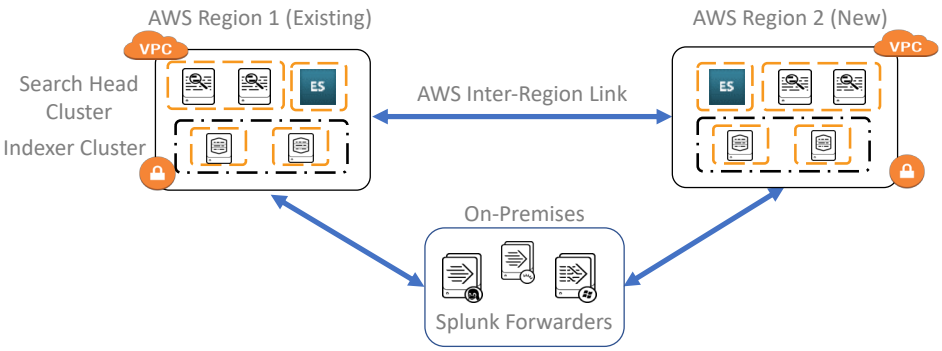
Customer Challenge

NASDAQ-listed multi-billion-dollar hi-tech enterprise software company was using Splunk infrastructure in the Cloud, wanted to migrate Splunk from one AWS region to another to reduce cloud infrastructure costs without causing any downtime. Also, the new infrastructure needed to be fully automated and possess self-healing elements to scale Splunk as the business grows.

The CREST Difference in 90 Days

Following steps were taken to migrate Splunk:

- Crest's Splunk Consultants worked closely with the customer to understand their current requirements and future growth needs
- Calculating new Splunk infra needs for EC2 instances and EBS volumes based on the ingestion capacity & retention policy – reducing AWS costs
- Upgrading Splunk in the existing region from version 6.3 to 7.1
- Deploying Splunk v7.1 with optimized AWS infra in the new region
- Copying Splunk configs (conf files, certificates, authentication, etc.) from existing region to the new region
- Migrating the apps, dashboards, data models, and 300TB+ existing data
- Moving traffic without downtime by peering existing & new Splunk infra
- Configuring alerts to send notifications when any thresholds are crossed



Splunk Automation

- Write Infrastructure Automation using AWS CloudFormation to provision Splunk infrastructure dynamically
- Automate frequently used Splunk Operations use cases using Ansible
- Add self-healing capabilities to Splunk:
  - If private keys from a Splunk server are deleted erroneously, automation will check the status & re-install them within 15 minutes
  - If "splunkd" service crashes, monit will restart the Splunk daemon automatically

> *Crest's consultants are not only experts in Splunk but also in migrating AWS workloads. Combination of these skills helped us migrate from one AWS region to another in less than 4 weeks without any downtime.*
>
> ***Sr. Director, Analytics***
> ***Leading Hi-Tech Enterprise Software Company***

Case Study: Managed Services

Multi-Billion Enterprise Customer Sees 60% Reduction in Admin Costs and 20% Drop in IT Tickets

60%	**Reduction in Admin costs**
31%	**Reduction in Splunk TCO**
2	**Average # of Days for Ticket Closure**
20%	**Reduction in Incoming Tickets**

Customer Challenge

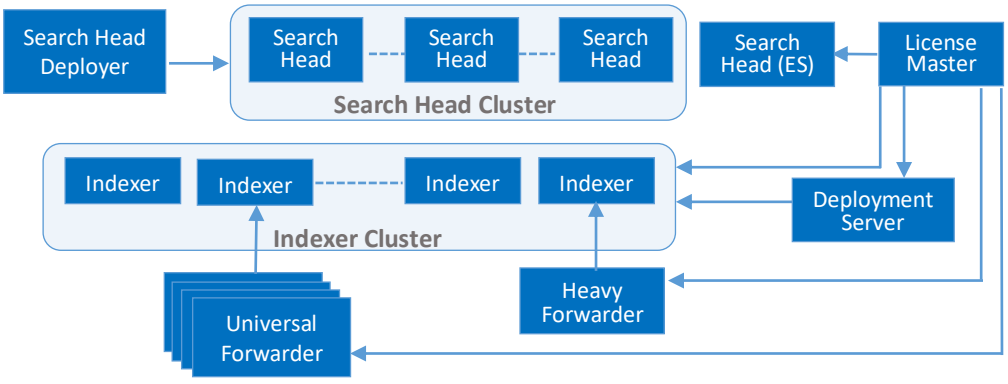
A multi-billion-dollar high-tech enterprise in the U.S. purchased Splunk to monitor their data center infrastructure, applications, and security. Splunk's professional services team designed and implemented an architecture, however the company was struggling to keep their Splunk investment operational. Frequent outages made it difficult for the customer to receive their desired operational intelligence. They also wanted an experienced "Day 2 Operations" team that would manage the Splunk infrastructure.

The CREST Difference in 90 Days

After working with Crest for 90 days, the customer saw rapid improvements and savings, along with, robust change management processes. Search queries were optimized, that improved Splunk performance by 5X factor. 1,100 GB/day data from 40+ apps and 4000+ nodes was onboarded. Splunk integrations with ServiceNow, Zenoss & Big Panda, ensured ticket creation from Splunk alerts. Splunk login was migrated to Active Directory for SSO and compliance. Custom reports were created for multiple Splunk users and a newly created internal knowledge base, trained them effectively.

> *Crest team helped onboard data quickly from several groups across IT. Our teams are gaining more business insights in real-time as a result now.*
>
> ***Director, Monitoring, IT Ops***

Distributed Splunk Deployment



Splunk Infrastructure Details:

Product: Splunk Enterprise 7.x & Enterprise Security (ES) 5.x
License Capacity: 1,100 GB/day
40+ Data Sources / Splunk Apps
Location: AWS

Distributed Splunk Architecture:

5 indexers
3 Search Head Clusters
4,000+ Universal Forwarders
1 Search Head Deployer
1 License Master and Deployment Master

USA
2107 North First Street #205
San Jose CA 95131

INDIA
First Floor, Bhaskar House
SG Road, Ahmedabad 380015

+1 (408) 909-9161
info@crestdatasys.com
http://www.crestdatasys.com/