CREST DATA SYSTEMS

## Services

### Development Services

- Custom TAs & Apps
- Adaptive Response for ES
- ITSI modules

### 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 Admins and Architects

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. Crest has built 150+ Splunk Apps & Technology Add-ons (TA) for customers ranging from Global Fortune 500 companies to Silicon Valley Startups in IT Ops, Security, and IoT domains. With a dedicated team of Splunk-certified Administrators, Engineers, and Consultants across the US and India, Crest provides Professional Services & 24x7 Managed Support Services to Splunk Enterprise & Cloud to customers across US, Europe, and APAC.

-

# Development Services

Proven Expertise. Agile Development. Certified Apps.

| | |
|---|---|
| 150+ | Apps & Add-ons |
| 50+ | 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.

> *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***
> ***Fortune 500 Hi-Tech Company***


## 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**

## 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. IT infrastructure deployment is challenging, but day-to-day operations is even more daunting. That's why companies rely on MSPs to 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

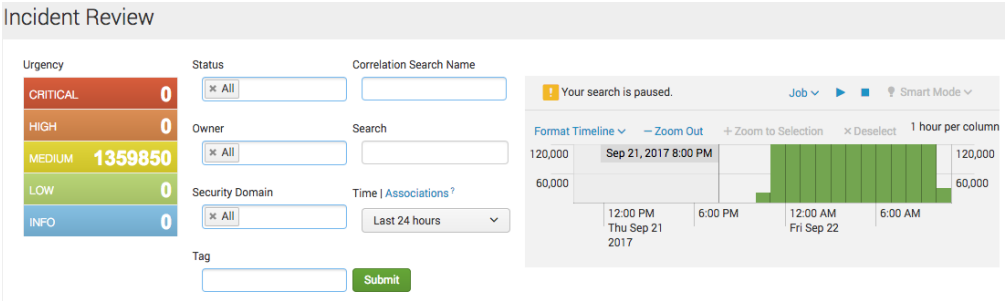
### Infrastructure Admin
- Health check of Splunk clusters
- Role-based Access Control
- Data Archiving & Retention Policy

### 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: Professional Services

Leading Retailer Gains Competitive Advantage by getting deep business insights while reducing Splunk Admin Costs by more than 50%Tickets

**50%** Reduction in Admin costs

**30%** Reduction in effort through Automation

**20+** Trainings per week

**20%** Reduction in Incoming Tickets

## Customer Challenge

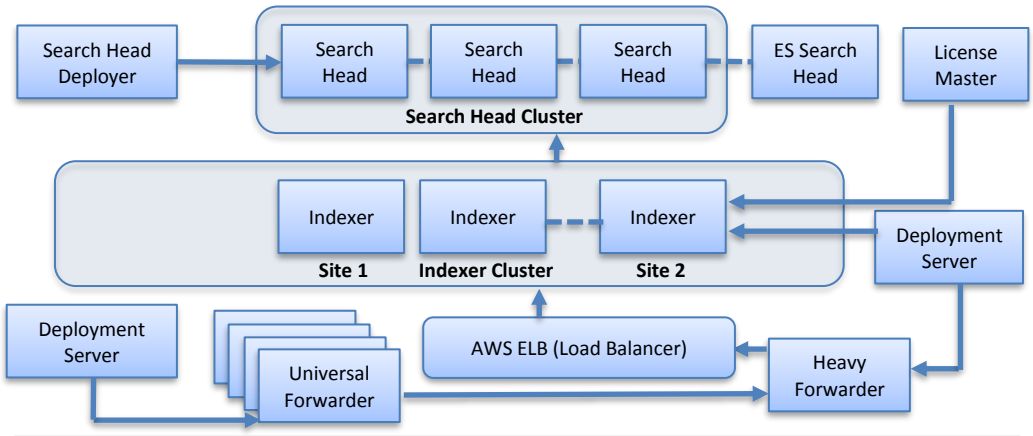
With $100B+ revenue from 7,000+ retail stores across 13 countries, this retail giant was in dire need of reducing operational costs and gaining business insights to achieve competitive advantage over local and online retailers. Despite deploying Splunk, IT troubleshooting was ad hoc, inefficient, and time-consuming. Having had a bad experience with their on-premise Splunk Enterprise, first challenge was to migrate the teams to AWS. Other monumental challenge was education and onboarding 125+ internal teams.

## The CREST Difference in 90 Days

Two Consultants worked with 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. 1000GB+/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***

**Large Highly-Distributed Splunk Deployment**




### Splunk Infrastructure Details:

Splunk License: 7.0 TB/day
800+ Data Sources / Splunk Apps
Product: Splunk Enterprise 6.5
Enterprise Security (ES) 4.5
Location: AWS

### Distributed Splunk Architecture:

40 indexers
12 Search Head Cluster
60,000+ Universal Forwarders
2 Search Head Deployer
1 License Master
9 Deployment Servers


CREST DATA SYSTEMS

**USA**
2107 N. 1st Street, #205
San Jose CA 95131

**INDIA**
First Floor, Bhaskar House
SG Road, Ahmedabad 380 015

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