splunk>®

Architecting Splunk Enterprise Deployments

Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is required
- Please do not distribute

Use Cases

Deployment Planning – Discovery

- As the first step, you need to gather the following basic information
  - Who will be the Splunk users?
  - What are their roles?
  - What are the goals for your Splunk deployment?
  - What are the use cases?
  - What is the current IT physical environment?
  - What is the current monitoring and / or logging environment?

Deployment Planning – Identify Users

- User Centered Design is a technique that can help to:
  - Identify the target users and their experience levels
  - Define their tasks and goals
  - Document functions they desire and require from a system
  - Determine the information they desire and require
- Additional info: https://en.wikipedia.org/wiki/User-centered_design

Goals and Usage Categories

- Troubleshoot systems
- Proactively discover problems
- Reduce or eliminate escalations and group analysis

Operations

- Identify security incidents
- Investigate security incidents faster
- Report on security issues

Security

- Meet log review and retention requirements
- Generate reports on controls
- Enable remote log access to locked-down systems

Compliance

- Dramatically reduce application downtime
- Free developers from time-consuming production support
- Find problems before the customer

App Mgmt

- Gain valuable business insight from machine data
- Use predictive analytics to scope growth
- Identify sales/marketing trends in your data

Analytics

Users and Use Cases – Operations

Common users include:

- Customer Support
- Systems Administrators
- IT Operations
- Development and QA
- Business and Finance
- Network Administrators

Common use cases include:

- Infrastructure Monitoring
- Server Virtualization Management
- Desktop Virtualization Management
- Service Desk

Operations

Users and Use Cases – Security

Common users include:

- Network Security Administrators
- Information Security Analysts
- Chief Security Officers
- Security Managers
- Application Security Analyst
- System Security Analyst

Common use cases include:

- Network / Data Security
- Insider Threat
- Patch Management
- Malware / Virus
- Fraud
- Spam

Security

Users and Use Cases – Compliance

Common users include:

- Security Analysts
- IT Operations
- Systems Administrators
- Human Resources
- Compliance staff and auditors
- CSO / CRO / CFO

Common use cases include:

- **PCI Compliance**
- HIPAA Compliance
- FISMA Compliance
- SOX Compliance
- SEC Compliance
- **Others …**

Compliance

Users & Use Cases – Application Development

Common users include:

- Application developers
- Customer Support
- Operations
- Business owners

Common use cases include:

- Custom Application Management
- Packaged Application Management
- Application Development
- Eliminate direct access to production systems for troubleshooting
- Overcome knowledge silos

App Mgmt

Users and Use Cases – Analytics

Common users include:

- Marketing
- Operations
- Business owners
- Business/market analysts

Common use cases include:

- Business Intelligence
- Supply chain management
- Procurement planning
- Real-time business insights

Analytics

More Use Cases

- Splunk publishes customer and industry case studies and success stories at splunk.com

  https://www.splunk.com/en_us/resources/use-cases.html