



Splunk Core

Feature	Splunk Free	Splunk Light	Splunk Enterprise	Splunk Cloud
Maximum Daily Indexing Volume	500MB	20GB	Unlimited	Unlimited
Maximum Users	1	5	Unlimited	Unlimited
Universal Data Collection/ Indexing	✓	✓	✓	✓
Metrics Store	✓	✓	✓	✓
Data Collection Add-Ons	✓	✓	✓	✓
Monitoring and Alerting		✓	✓	✓

CYBRARY



Specialty Focuses

- Splunk Enterprise Security
- Splunk User Behavior Analytics
- Splunk IT Service Intelligence
- Splunk Insights for Infrastructure
- Splunk Insights for AWS Cloud Monitoring
- Splunk Insights for Ransomware
- Splunk for Industrial IoT

Splunk Enterprise Security
Investigate, Detect, & Respond

Splunk Enterprise Investigation
-Log aggregation
-Data correlation
-Alerts, watches & data ingest
-Breadcrumbs of known

Splunk UBA Detection
-Risk indicator detection
-Behavioral modeling
-400+ rules, graph analysis
-Breadcrumbs of unknown

Human Driven Machine Learning Driven

From Splunk.com

CYBRARY

Other Products

- Phantom
- VictorOps

From Splunk.com

CYBRARY

WHICH OF THE FOLLOWING
IS NOT ONE OF THE SPLUNK
PLATFORMS?

A) SPLUNK CLOUD
B) SPLUNK FREE
C) SPLUNK ENTERPRISE SECURITY

In summary...

Splunk Platforms: Splunk Enterprise, Splunk Cloud, Splunk Light, Splunk Free
Additional analytics, intelligence, operationalization: Splunk Insights, Splunk Enterprise Security, etc.
Other tools: Phantom, VictorOps

CYBRARY

Next: Module 3

CYBRARY
