Introduction to Splunk

Module 2: Splunk Products

Natasha Staples

CYBRARY

Splunk Core

Features	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

Pricing

From Splunk.com

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

From Splunk.com

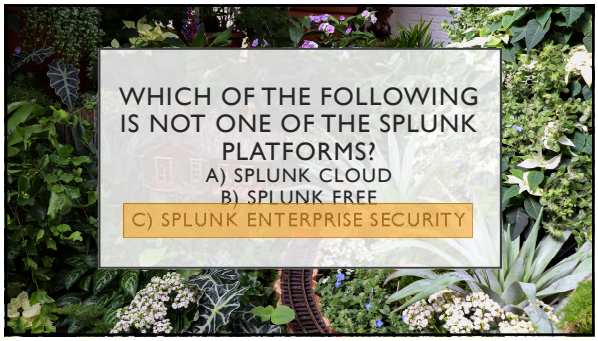
CYBRARY

Other Products

Phantom
VictorOps

From Splunk.com

CYBRARY



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