Module 001
Introduction to Splunk

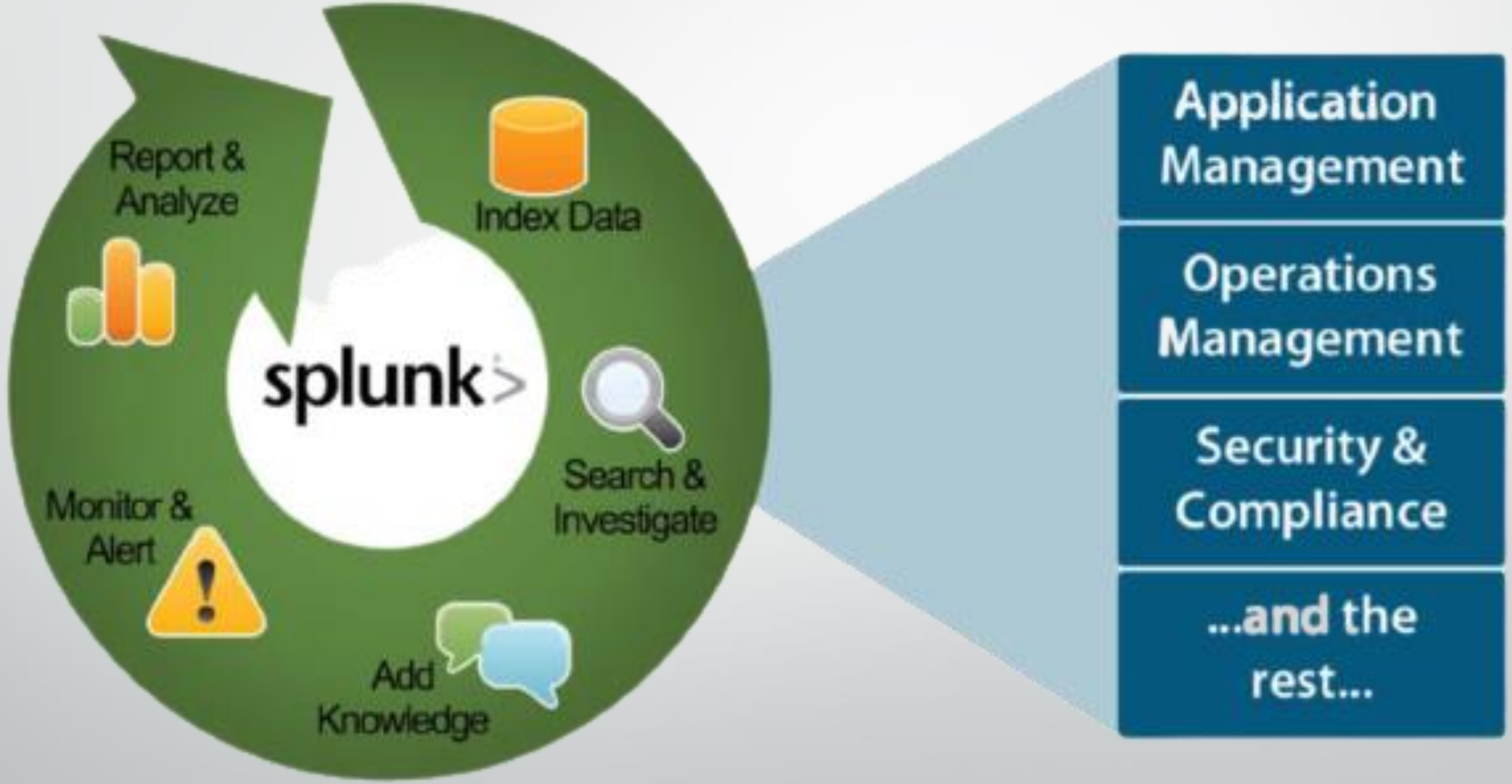
Barakat A. B. Abweh
Information Security Specialist

CYBERGEEK

Agenda

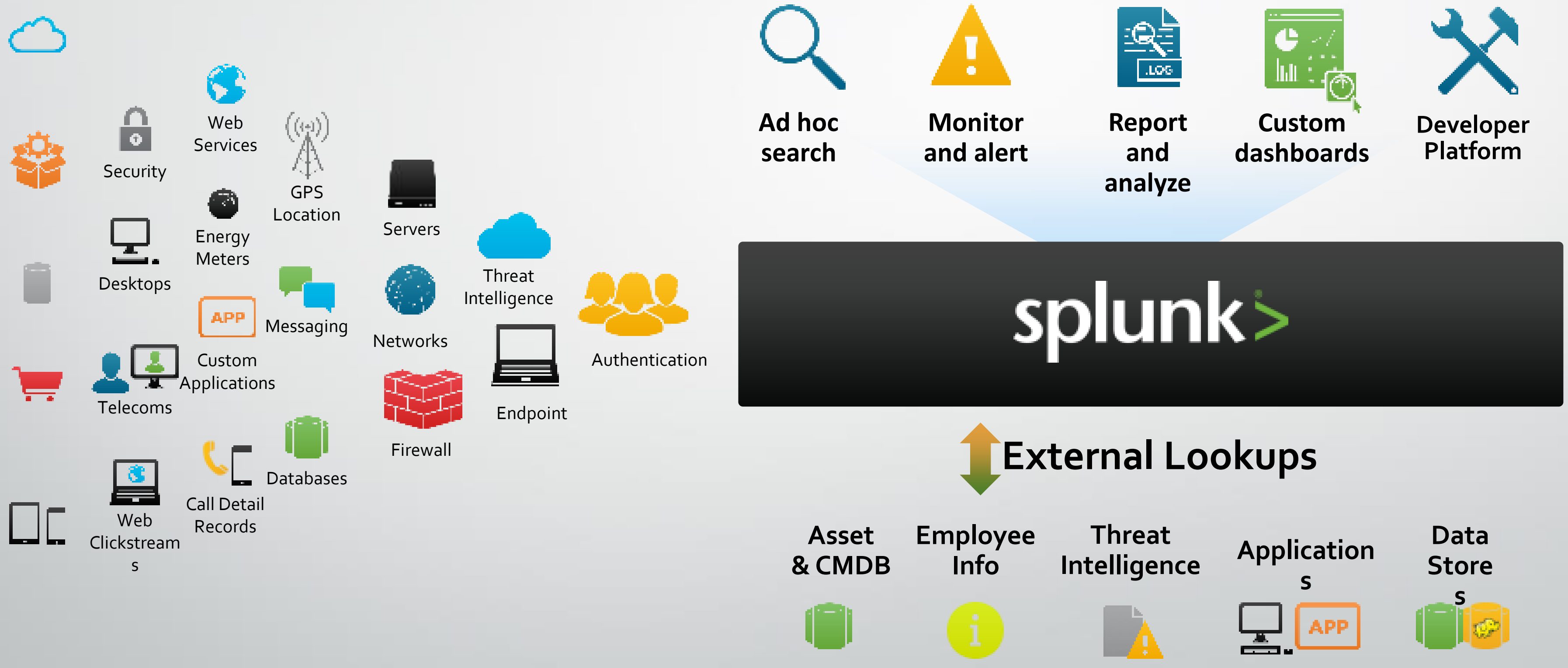
- What is Splunk?
- What Data can we index and store in Splunk?
- Splunk main Components & How it Works?
- How Splunk is Deployed & Used?
- What are Splunk apps & add-ons?
- What are Splunk enhanced solutions?
- What are Splunk roles & permissions?
- How to log into Splunk & what the first thing you see?
- What is search app?

What is Splunk?

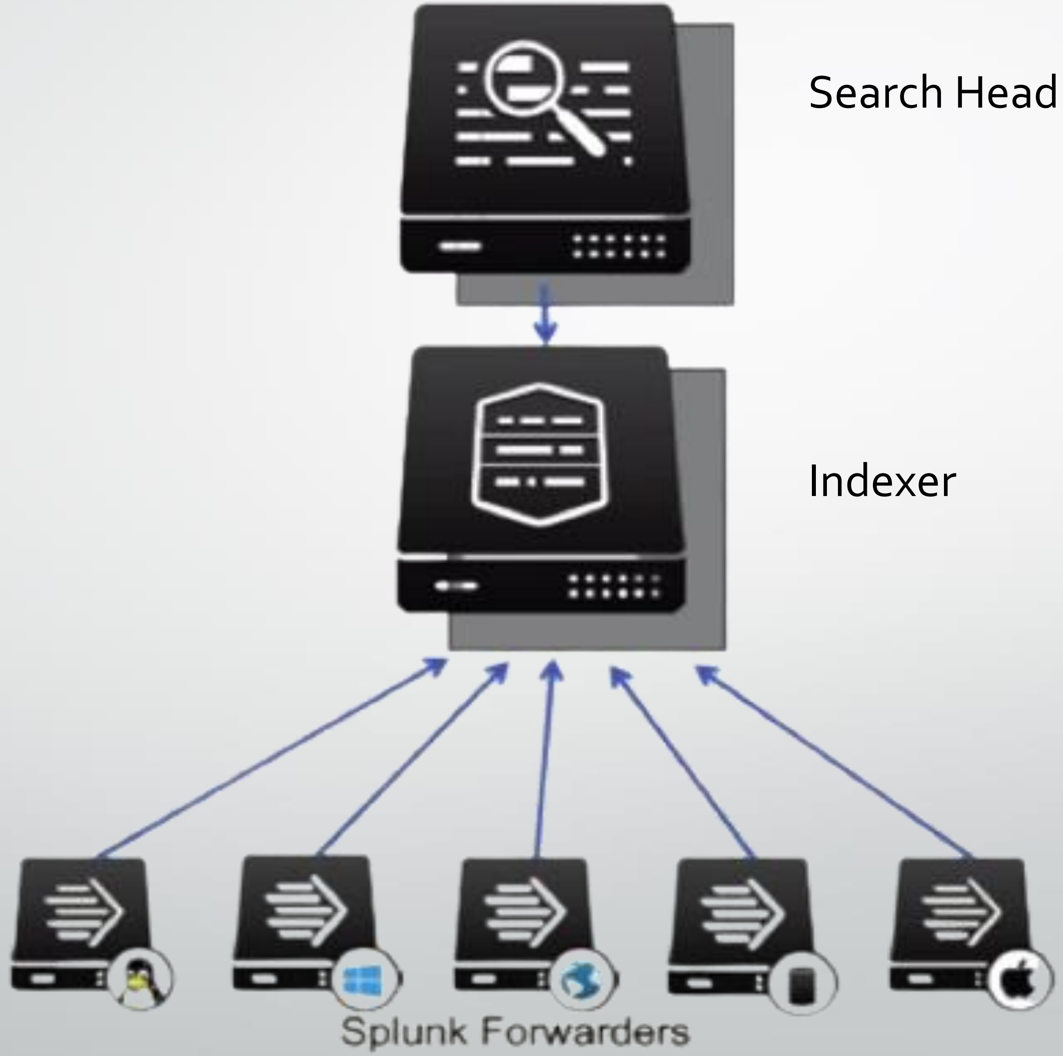


What Data can we index and store in Splunk?

Any data from any source



Splunk main Components & How it Works?



Search Head

Indexer

Splunk Forwarders

CYBERGEEK

How Splunk is Deployed & Used?

Splunk Enterprise

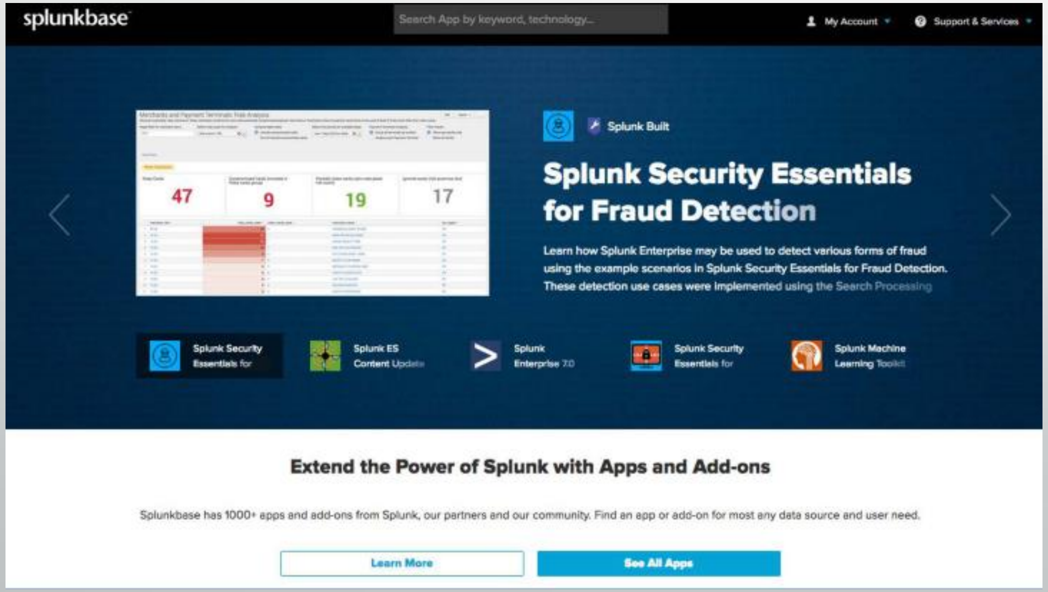
Splunk Cloud

Splunk Light

CYBERGEEK

What are Splunk apps & add-ons?

- Special config.
- Regex
- Saved searches
- Reports
- Alerts
- Dashboard


splunkbase
Search App by keyword, technology...
My Account
Support & Services
47
9
19
17
Splunk Security Essentials for
Splunk ES Content Update
Splunk Enterprise 7.0
Splunk Security Essentials for
Splunk Machine Learning Toolkit
Learn More
See All Apps

Splunk Built

Splunk Security Essentials for Fraud Detection

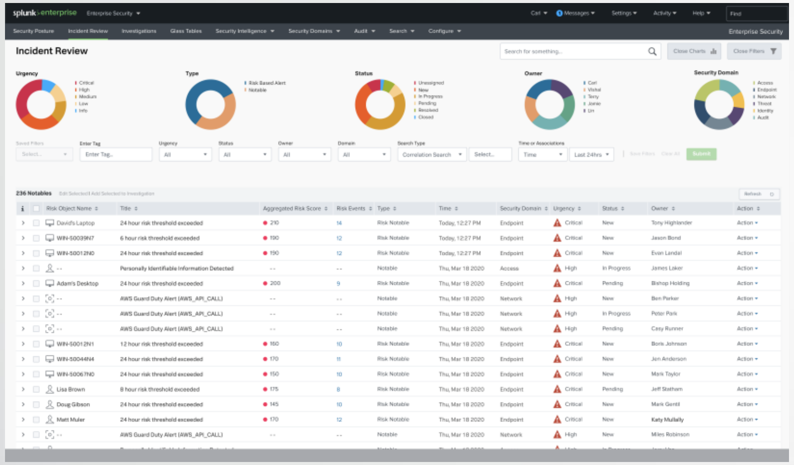
Learn how Splunk Enterprise may be used to detect various forms of fraud using the example scenarios in Splunk Security Essentials for Fraud Detection. These detection use cases were implemented using the Search Processing

Extend the Power of Splunk with Apps and Add-ons

Splunkbase has 1000+ apps and add-ons from Splunk, our partners and our community. Find an app or add-on for most any data source and user need.

What are Splunk Enhanced Solutions?

Splunk Enterprise Security



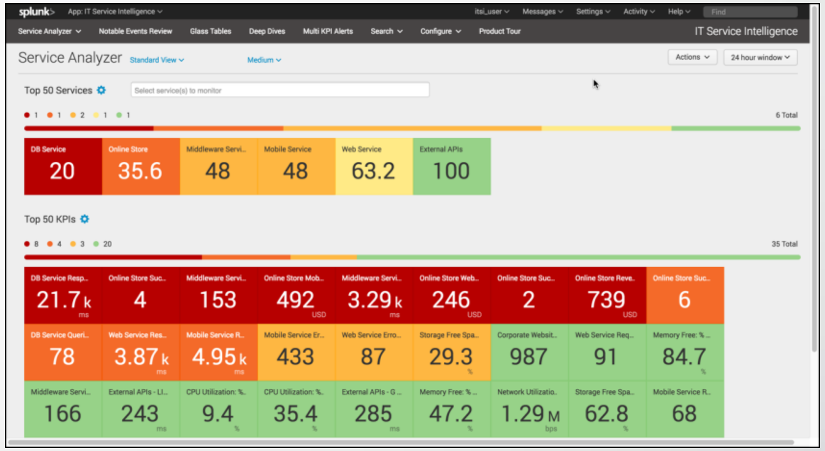
Incident Review

Enter Tag: Enter Tag... | Urgency: All | Status: All | Owner: All | Domain: All | Search Type: Correlation Search | Select... | Time or Associations: Time | Last 24hrs

236 Notables Edit Selected | Add Selected to Investigation

Risk Object Name	Title	Aggregated Risk Score	Risk Events	Type	Time	Security Domain	Urgency	Status	Owner	Action
David's Laptop	24 hour risk threshold exceeded	210	14	Risk Notable	Today, 12:27 PM	Endpoint	Critical	New	Tony Highlander	Action
WIN-S0039N7	6 hour risk threshold exceeded	190	12	Risk Notable	Today, 12:27 PM	Endpoint	Critical	New	Jason Bond	Action
WIN-S0012N0	24 hour risk threshold exceeded	190	12	Risk Notable	Today, 12:27 PM	Endpoint	Critical	New	Evan Landal	Action
--	Personally Identifiable Information Detected	--	--	Notable	Thu, Mar 18 2020	Access	High	In Progress	James Laker	Action
Adam's Desktop	24 hour risk threshold exceeded	200	9	Risk Notable	Thu, Mar 18 2020	Endpoint	Critical	Pending	Bishop Holding	Action
--	AWS Guard Duty Alert (AWS_API_CALL)	--	--	Notable	Thu, Mar 18 2020	Network	High	New	Ben Parker	Action
--	AWS Guard Duty Alert (AWS_API_CALL)	--	--	Notable	Thu, Mar 18 2020	Network	High	In Progress	Peter Park	Action
--	AWS Guard Duty Alert (AWS_API_CALL)	--	--	Notable	Thu, Mar 18 2020	Network	High	Pending	Casy Runner	Action
WIN-S0012N1	12 hour risk threshold exceeded	160	10	Risk Notable	Thu, Mar 18 2020	Endpoint	Critical	New	Boris Johnson	Action
WIN-S0044N4	24 hour risk threshold exceeded	170	11	Risk Notable	Thu, Mar 18 2020	Endpoint	Critical	New	Jen Anderson	Action
WIN-S0067N0	24 hour risk threshold exceeded	150	10	Risk Notable	Thu, Mar 18 2020	Endpoint	Critical	New	Mark Taylor	Action
Lisa Brown	8 hour risk threshold exceeded	175	8	Risk Notable	Thu, Mar 18 2020	Endpoint	Critical	Pending	Jeff Statham	Action
Doug Gibson	24 hour risk threshold exceeded	145	10	Risk Notable	Thu, Mar 18 2020	Endpoint	Critical	New	Mark Gentil	Action
Matt Muler	24 hour risk threshold exceeded	170	12	Risk Notable	Thu, Mar 18 2020	Endpoint	Critical	New	Katy Mullally	Action
--	AWS Guard Duty Alert (AWS_API_CALL)	--	--	Notable	Thu, Mar 18 2020	Network	High	New	Miles Robinson	Action

Splunk IT Service Entillegence



Service Analyzer

Top 50 Services

● 1 ● 1 ● 2 ● 1 ● 1 — 6 Total

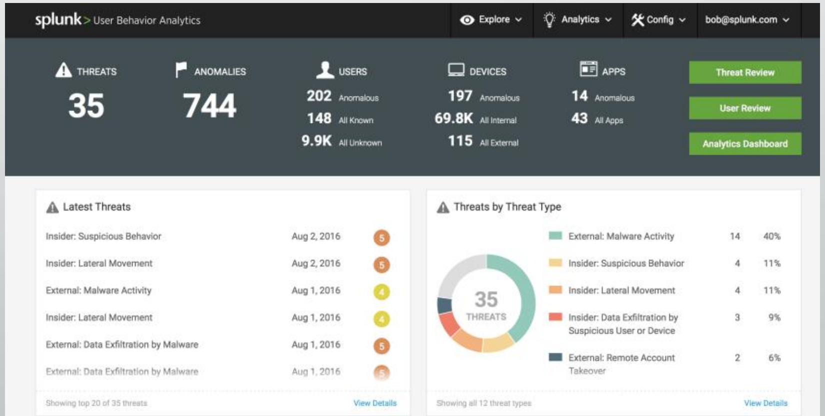
DB Service	Online Store	Middleware Servi...	Mobile Service	Web Service	External APIs
20	35.6	48	48	63.2	100

Top 50 KPIs

● 8 ● 4 ● 3 ● 20 — 35 Total

DB Service Resp... 21.7k ms	Online Store Suc... 4	Middleware Servi... 153	Online Store Mob... 492 USD	Middleware Servi... 3.29k ms	Online Store Web... 246 USD	Online Store Suc... 2	Online Store Reve... 739 USD	Online Store Suc... 6
DB Service Queri... 78	Web Service Res... 3.87k ms	Mobile Service R... 4.95k ms	Mobile Service Er... 433	Web Service Erro... 87	Storage Free Spa... 29.3 %	Corporate Websit... 987	Web Service Req... 91	Memory Free: % ... 84.7 %
Middleware Servi... 166	External APIs - Ll... 243 ms	CPU Utilization: %... 9.4 %	CPU Utilization: %... 35.4 %	External APIs - G ... 285 ms	Memory Free: % ... 47.2 %	Network Utilizatio... 1.29M bps	Storage Free Spa... 62.8 %	Mobile Service R... 68

Splunk User Behavior Analytics



THREATS 35

ANOMALIES 744

USERS: 202 Anomalous; 148 All Known; 9.9K All Unknown

DEVICES: 197 Anomalous; 69.8K All Internal; 115 All External

APPS: 14 Anomalous; 43 All Apps

Latest Threats

Insider: Suspicious Behavior	Aug 2, 2016	5
Insider: Lateral Movement	Aug 2, 2016	5
External: Malware Activity	Aug 1, 2016	4
Insider: Lateral Movement	Aug 1, 2016	4
External: Data Exfiltration by Malware	Aug 1, 2016	5
External: Data Exfiltration by Malware	Aug 1, 2016	5

Showing top 20 of 35 threats

Threats by Threat Type

External: Malware Activity	14	40%
Insider: Suspicious Behavior	4	11%
Insider: Lateral Movement	4	11%
Insider: Data Exfiltration by Suspicious User or Device	3	9%
External: Remote Account Takeover	2	6%

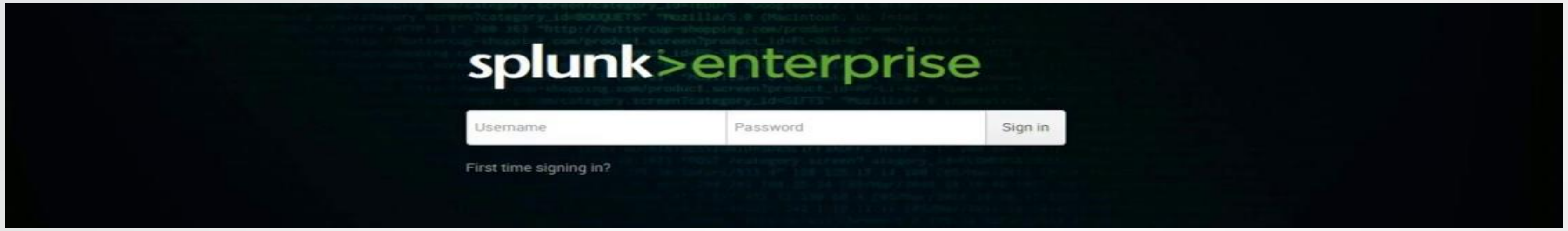
Showing all 12 threat types

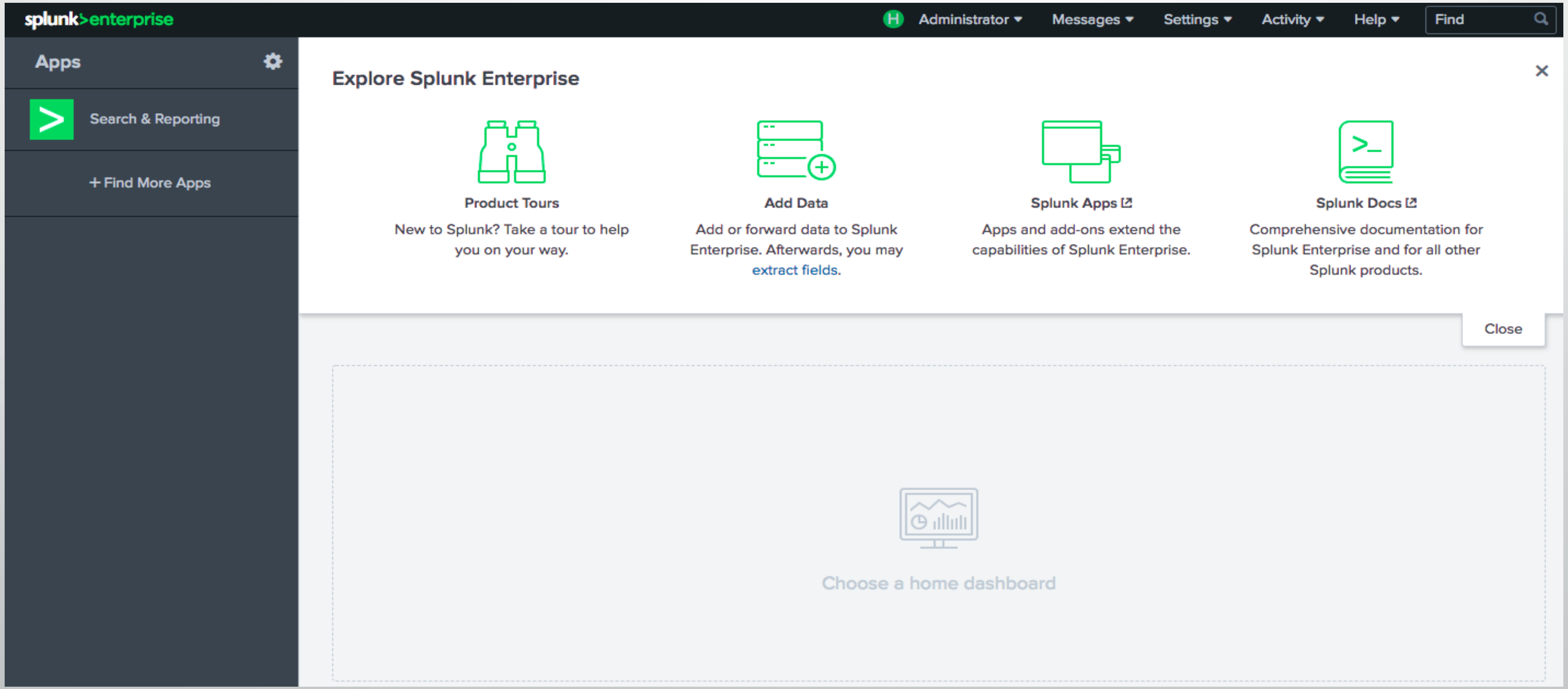
CYBERGEEK

Splunk roles & users

Admin
Power
User

How to log into Splunk & what the first thing you see?





Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

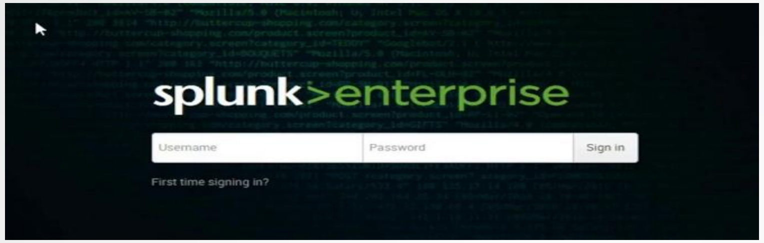
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

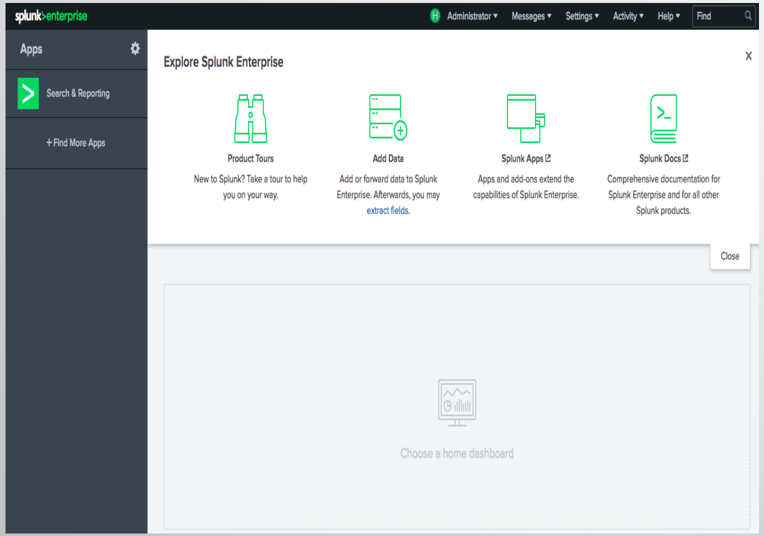
Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

Choose a home dashboard

CYBERGEEK

How to log into Splunk & what the first thing you see?





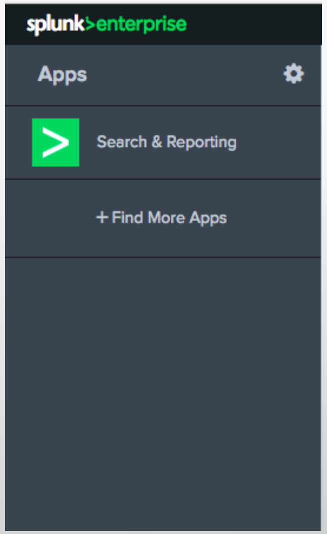
Explore Splunk Enterprise

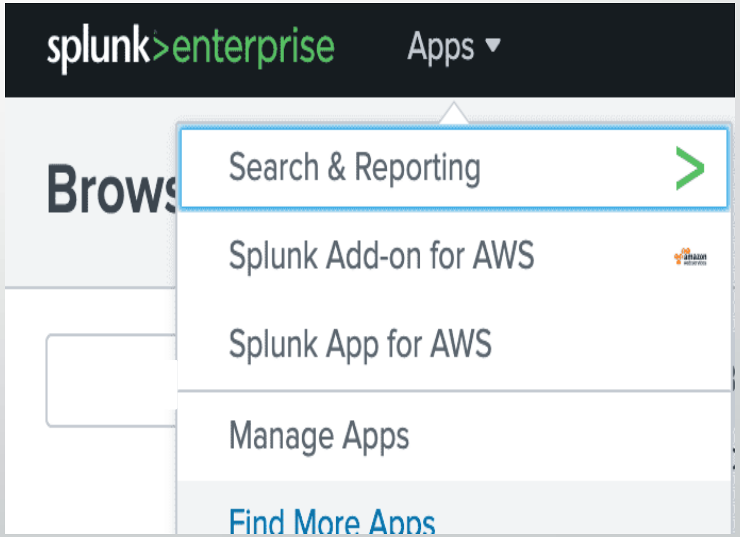
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

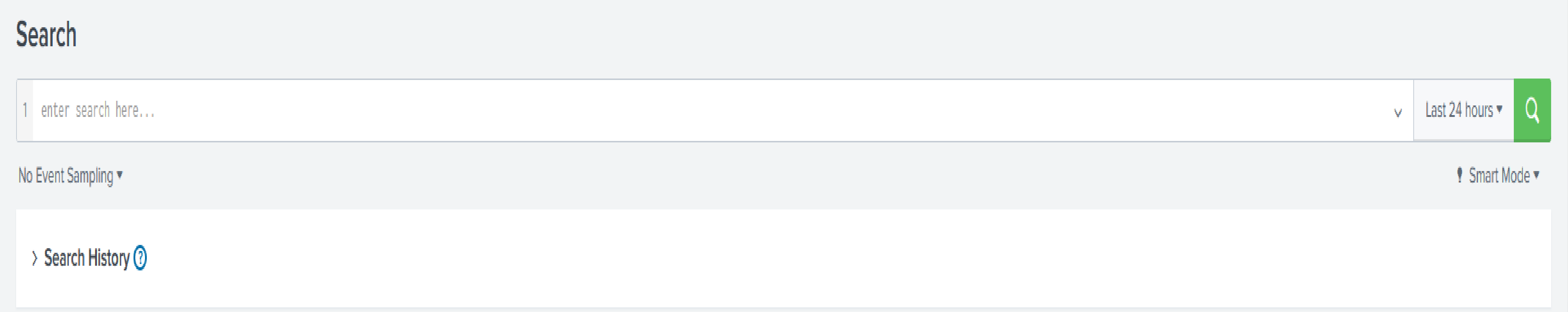
Apps and add-ons extend the capabilities of Splunk Enterprise.

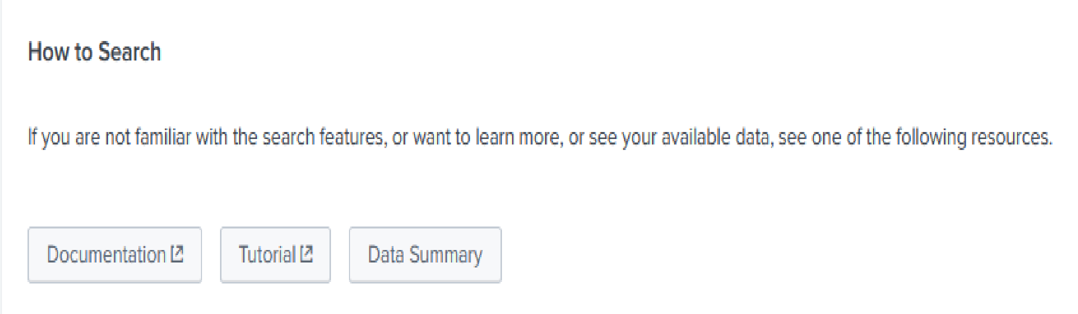
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.





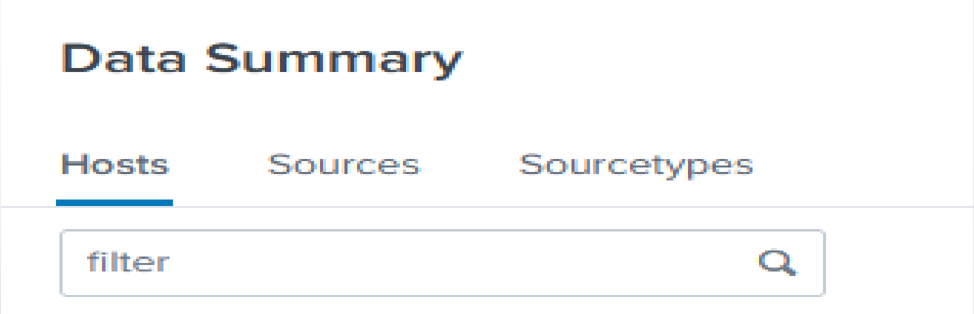
What is search app?

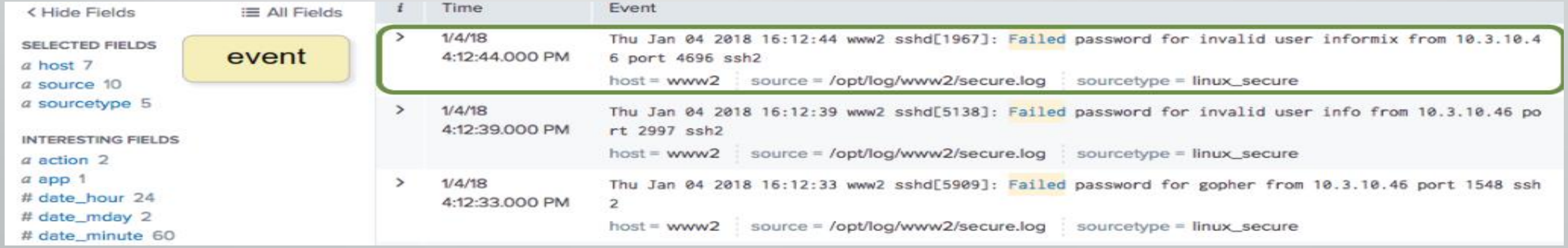




How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.





```
>  1/4/18            Thu Jan 04 2018 16:12:44 www2 sshd[1967]: Failed password for invalid user informix from 10.3.10.4
   4:12:44.000 PM    6 port 4696 ssh2
                     host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure
>  1/4/18            Thu Jan 04 2018 16:12:39 www2 sshd[5138]: Failed password for invalid user info from 10.3.10.46 po
   4:12:39.000 PM    rt 2997 ssh2
                     host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure
>  1/4/18            Thu Jan 04 2018 16:12:33 www2 sshd[5909]: Failed password for gopher from 10.3.10.46 port 1548 ssh
   4:12:33.000 PM    2
                     host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure
```