ELLINGTON CYBER ACADEMY

KENNETH ELLINGTON

Founder & Instructor

ellingtonCyberAcademy.com

e:kellington@ellingtoncyberacademy.com

ECA ELLINGTON CYBER ACADEMY

About The Webinar

- **Mastering Splunk for Digital Defense**
- **WHAT**. Hands-on labs overview of Splunk and Security basics
- **SCHEDULE**. 1 Night 1-2 Hours long
- **HOW**.
    - Walkthrough of the fundamentals of how Splunk works and SIEM technologies overall
    - Demo of how to set up a basic Splunk Lab
    - Demo of how to ingest Windows logs into you Splunk Lab

Who the HECK is Kenneth?

- **Kenneth Ellington**
- Senior Cybersecurity Consultant at Big 4 firm
- Cyber Security Practitioner specialized in SIEM and SOAR technology
- Former Cyber Security instructor at University of Houston
- Blue team program instructor for Blacks in Cyber Security
- Huge My Hero Academia Fan

Who the HECK is Courtney?

- **Courtney Wright**
- SOC Specialist at Expel
- Specialized in MDR technologies and phishing techniques
- SIEM and SOAR Instructor at ECA
- Huge Marvel fan

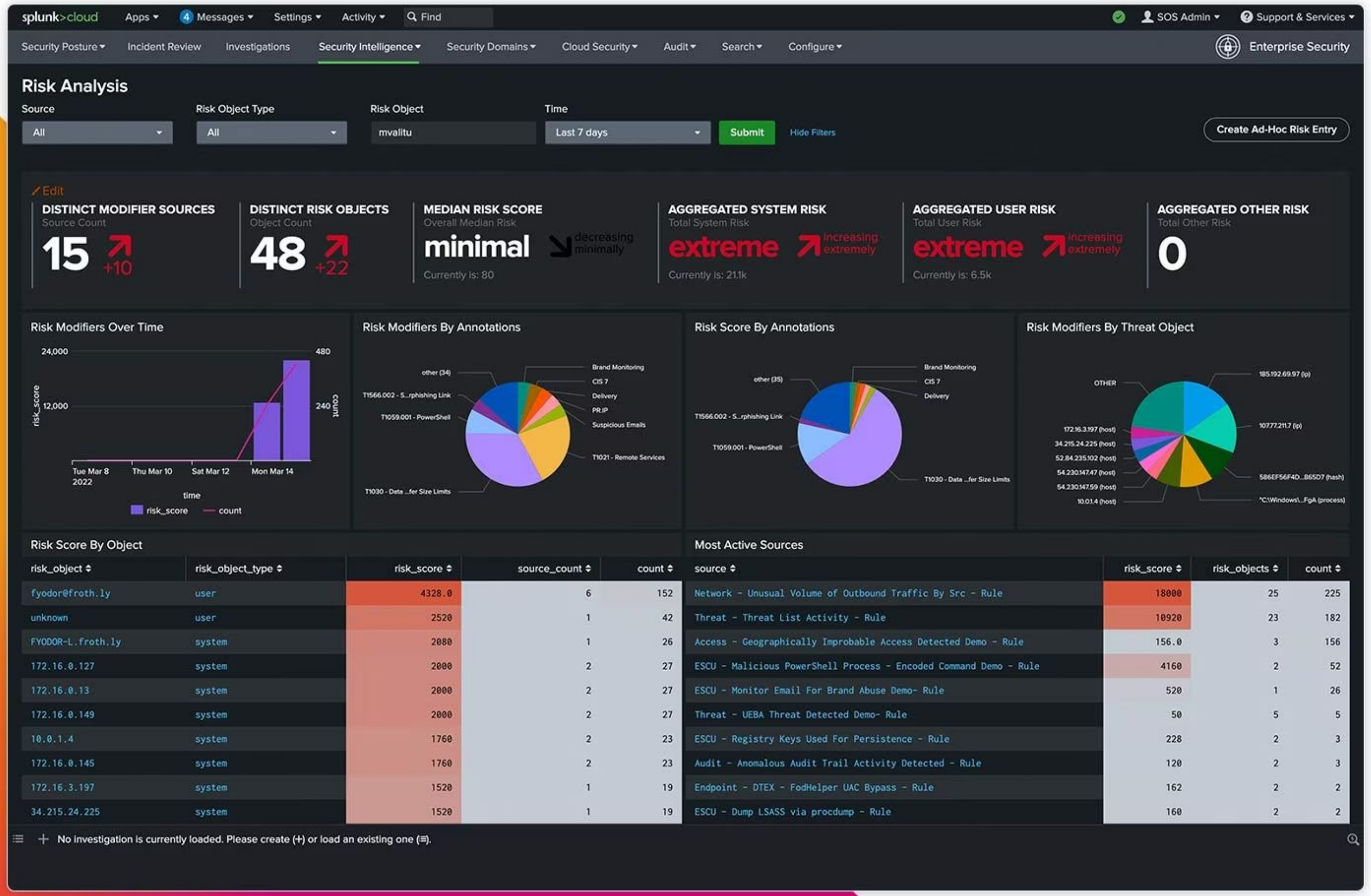
What Exactly is a SIEM?

SIEM = Security Information & Event Monitoring

Designed to log and monitor security events inside of an environment
Not meant to store every single IT event inside of the environment

Examples: Splunk ES, Qradar, Microsoft Sentinel

What the Hell is Splunk?



Risk Analysis

Source: All
Risk Object Type: All
Risk Object: mvalitu
Time: Last 7 days

DISTINCT MODIFIER SOURCES
Source Count
15 +10

DISTINCT RISK OBJECTS
Object Count
48 +22

MEDIAN RISK SCORE
Overall Median Risk
minimal decreasing minimally
Currently is: 80

AGGREGATED SYSTEM RISK
Total System Risk
extreme increasing extremely
Currently is: 21.1k

AGGREGATED USER RISK
Total User Risk
extreme increasing extremely
Currently is: 6.5k

AGGREGATED OTHER RISK
Total Other Risk
0

Risk Score By Object

risk_object	risk_object_type	risk_score	source_count	count
fyodor@froth.ly	user	4328.0	6	152
unknown	user	2520	1	42
FYODOR-L.froth.ly	system	2080	1	26
172.16.0.127	system	2000	2	27
172.16.0.13	system	2000	2	27
172.16.0.149	system	2000	2	27
10.0.1.4	system	1760	2	23
172.16.0.145	system	1760	2	23
172.16.3.197	system	1520	1	19
34.215.24.225	system	1520	1	19

Most Active Sources

source	risk_score	risk_objects	count
Network - Unusual Volume of Outbound Traffic By Src - Rule	18000	25	225
Threat - Threat List Activity - Rule	10920	23	182
Access - Geographically Improbable Access Detected Demo - Rule	156.0	3	156
ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule	4160	2	52
ESCU - Monitor Email For Brand Abuse Demo- Rule	520	1	26
Threat - UEBA Threat Detected Demo- Rule	50	5	5
ESCU - Registry Keys Used For Persistence - Rule	228	2	3
Audit - Anomalous Audit Trail Activity Detected - Rule	120	2	3
Endpoint - DTEX - FodHelper UAC Bypass - Rule	162	2	2
ESCU - Dump LSASS via procdump - Rule	160	2	2

No investigation is currently loaded. Please create (+) or load an existing one (≡).

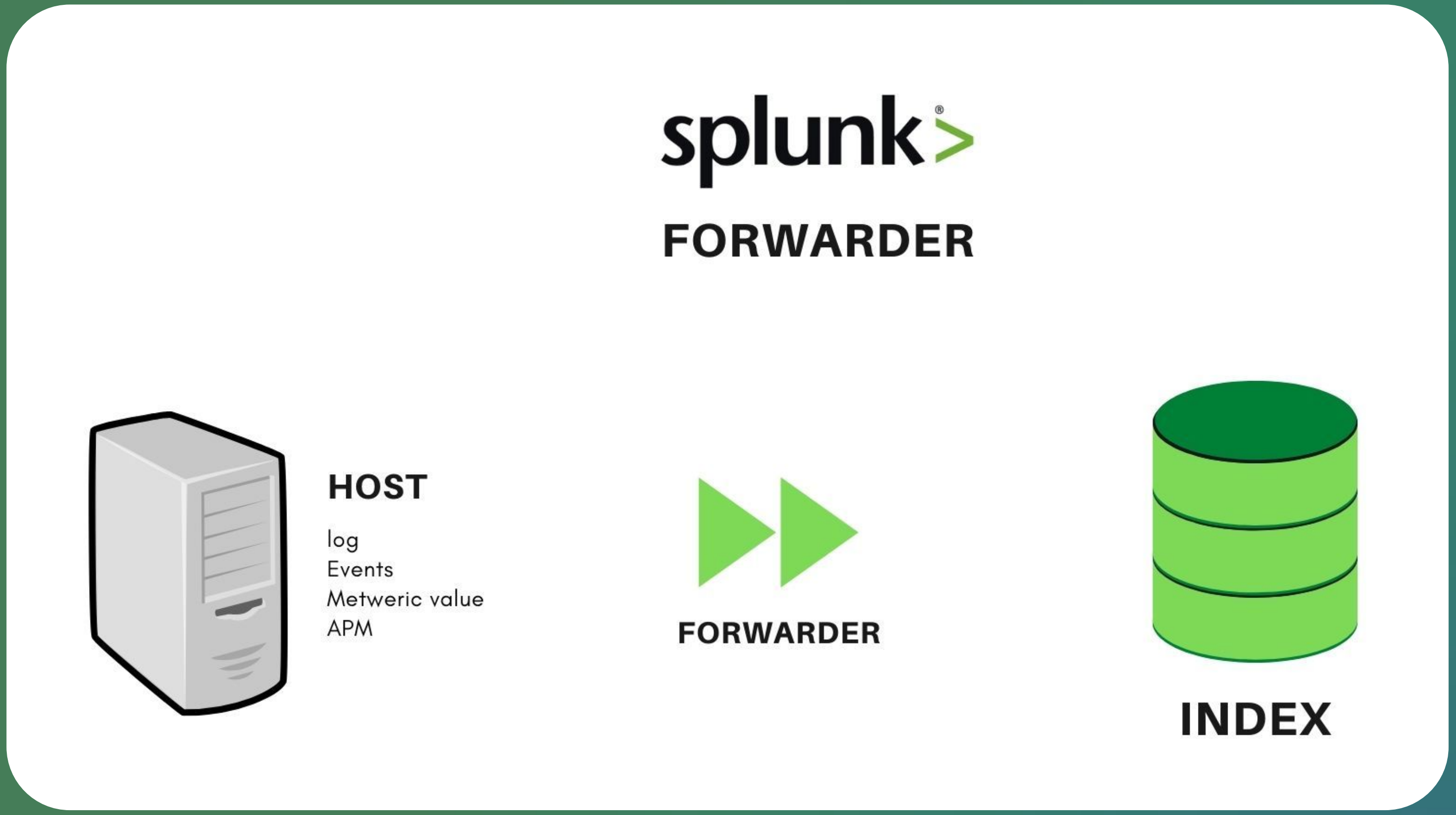
- **Data Aggregation Log Management and visualization platform**

- Used for multiple use cases, including:
  - IT Operations
  - Devops
  - UBEA
  - Cyber Security analytics
  - Network Monitoring

- It is not a SIEM!
- Used by 80%+ of Fortune 100 companies

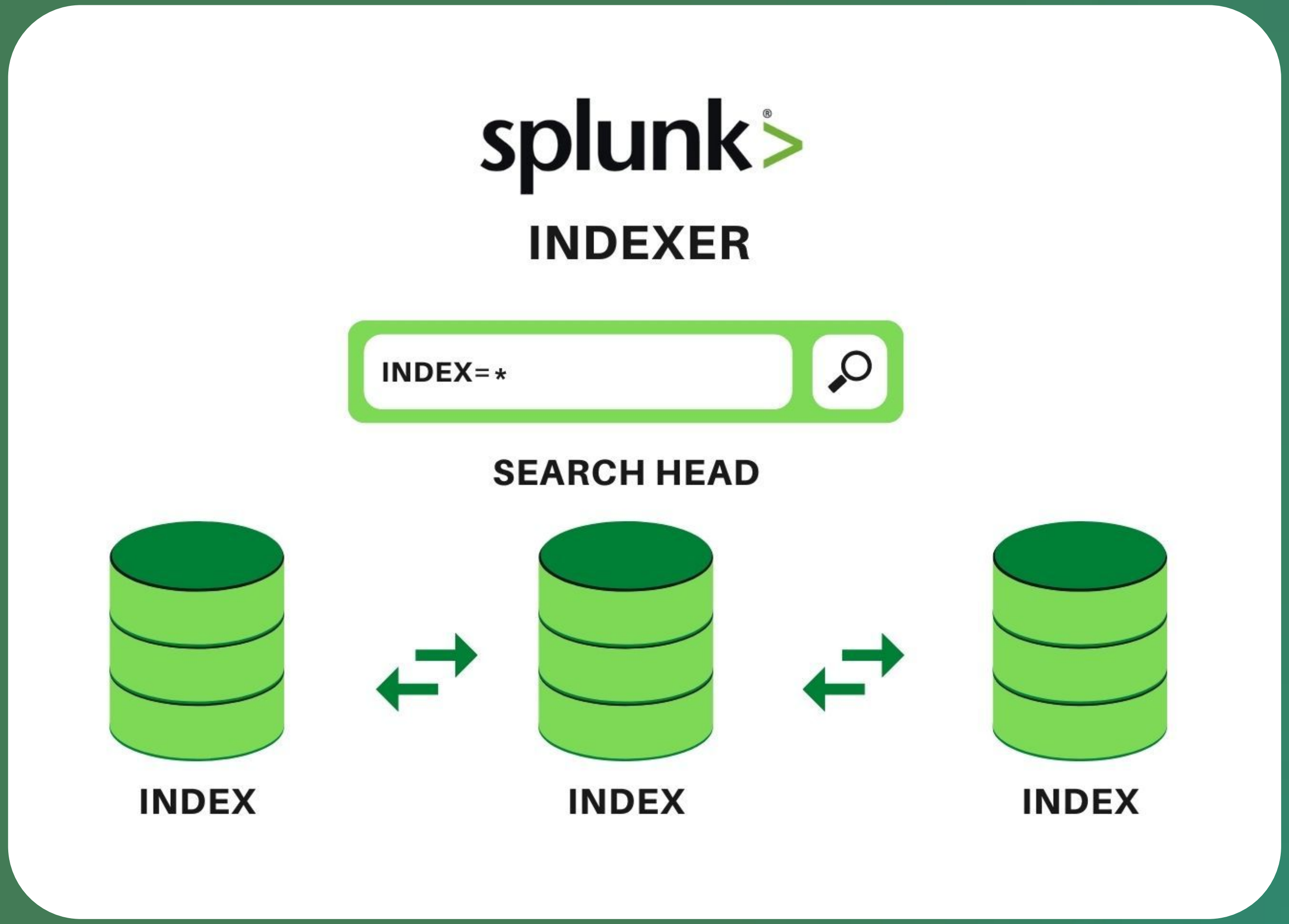
What is a Forwarder?

- Light instance of Splunk Enterprise
- Mainly used to send data to Indexer
- Installed on devices that are owned by firm
- Multiple Types such as:
  - Universal Forwarder (Most Common)
  - Intermediate Forwarder
  - Heavy Forwarder



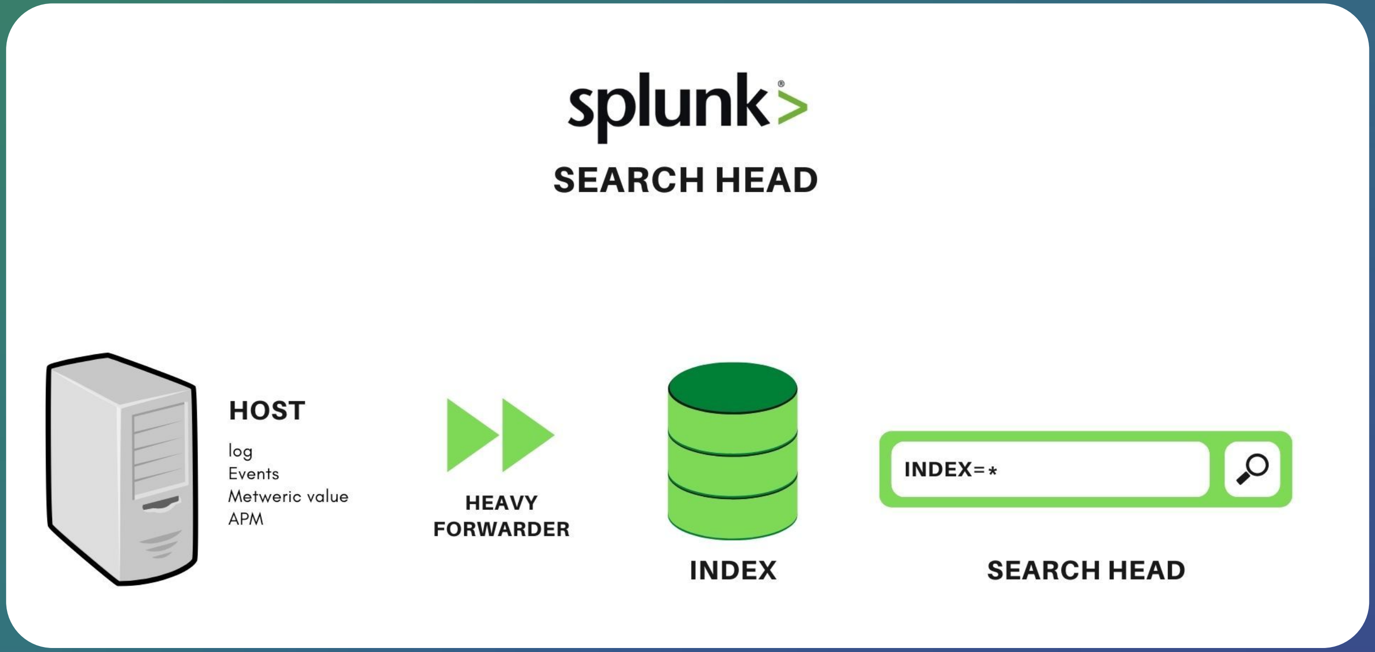
What is An Indexer?

- Storage medium where data is sent to and stored from the forwarders.
- Stored on Flat files and queried from the Search head
- Where the indexing and parsing happens most of the time.
- Licensing meter is also run here.



What is a Search Head?

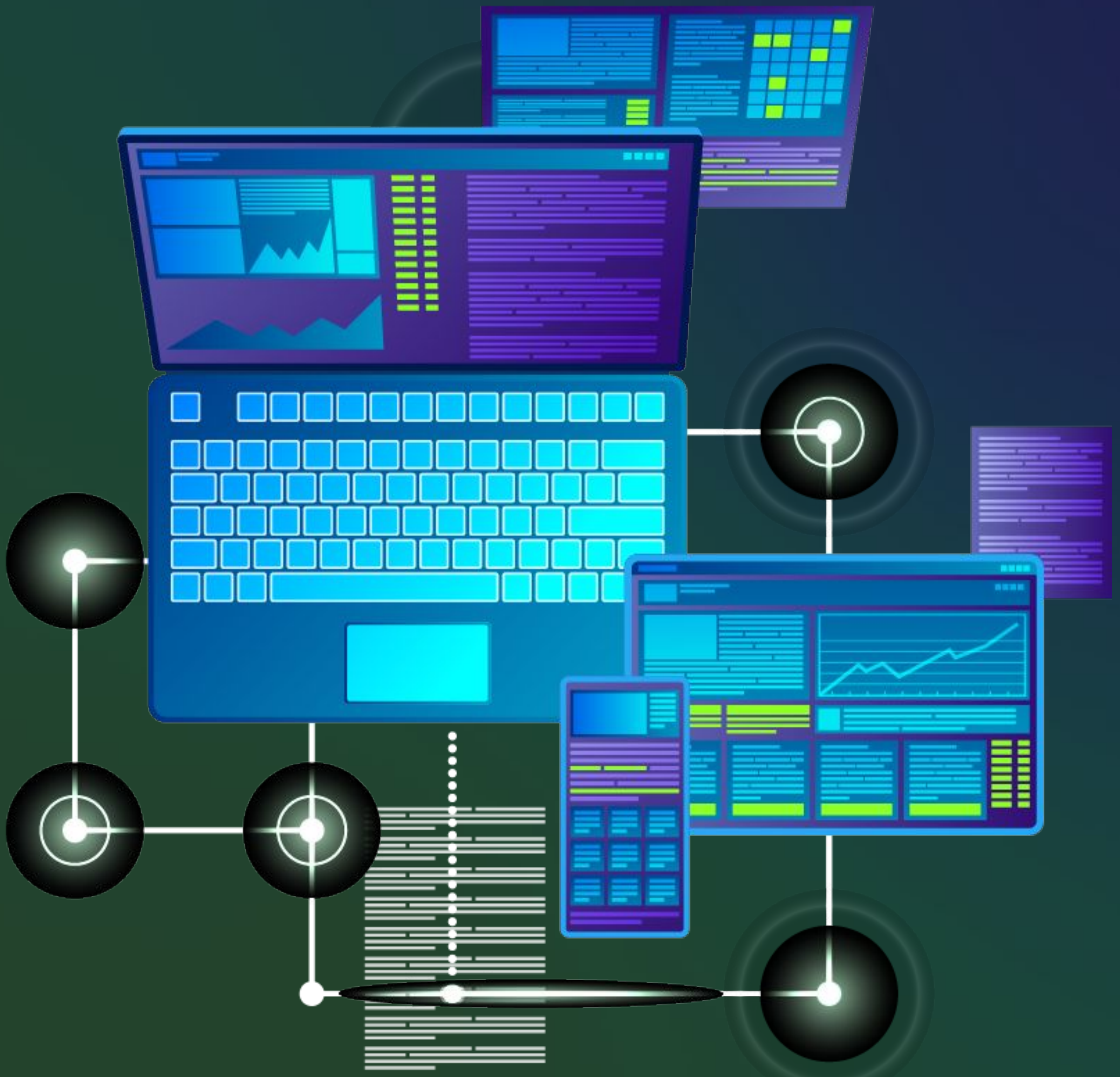
- Splunk component that the end user has access to
- Splunk Web or the GUI sits on the Search Head



- Where the visualizations are created such as Dashboards or reports, as well as where searches are run
- Search head queries the index back for information then displays it

Demo Time

Installing and Configuring Splunk

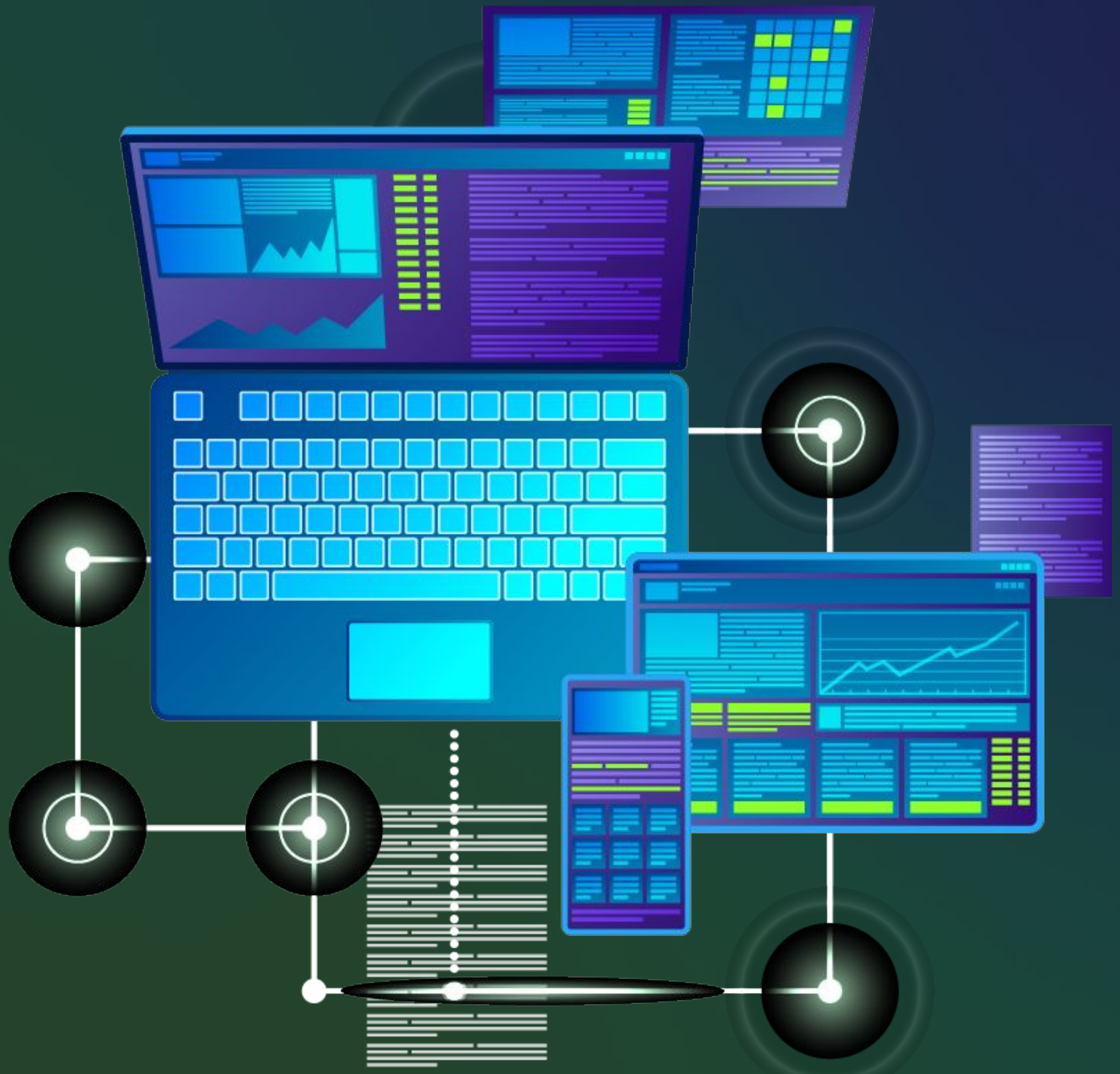


Searching Windows Event Logs

1	Key Points	● Understanding why it's important to monitor Window logs in your environment ● Learning how to build Detection rules on them certain Event Codes
2	Setting up Windows Forwarding inside of your environment	● Configuring the proper ports inside of Splunk ● No TA vs. Using a Windows TA for data ingestion
3	Windows Event Codes to look out for	● Security - 4624, 5136 ● Application - 1001

Demo Time

Splunking Windows logs



THANK YOU

KENNETH ELLINGTON

Founder & Instructor

ellingtoncyberacademy.com

e:kellington@ellingtoncyberacademy.com

ECA ELLINGTON CYBER ACADEMY