

## **Splunk SIEM – Log Ingestion, Detection & Security Monitoring**

Splunk is one of the most widely used machine-data analytics platforms in the world. It enables organizations to collect, index, search, analyze, and visualize massive volumes of log and event data. This paper introduces Splunk, its core components, capabilities, use cases in IT and cybersecurity, and provides a technical yet student-friendly overview suitable for academic presentation purposes.

### **Introduction**

As digital infrastructures expand, organizations generate millions of machine events from servers, networks, security tools, and applications. Traditional methods cannot efficiently analyze this volume of data. Splunk was designed to solve this problem by turning raw machine data into actionable insights. Although originally a log management tool, Splunk has evolved into a powerful platform supporting security operations, real-time monitoring, automation, and even machine learning.

### **What is Splunk?**

Splunk is a data analytics platform that allows the collection, indexing, searching, and visualization of machine-generated data. In simple terms, Splunk gathers digital exhaust from systems and applications and transforms it into meaningful information that supports decision-making, troubleshooting, and threat detection.

### **Splunk Architecture**

Splunk's core architecture is built around three primary components:

#### **a. Universal Forwarder (UF)**

A lightweight software agent installed on Windows, Linux, or other systems. Its role is to collect logs and forward them securely to Splunk Indexers.

### **b. Indexer**

The Indexer is the core engine of Splunk. It receives data from Forwarders, indexes it, and stores it efficiently. Searches and queries are executed on indexed data, making retrieval extremely fast.

### **c. Search Head**

The user-facing interface where analysts and engineers run queries, create dashboards, analyze data, and build alerts. It supports data visualization and interactive investigation workflows. The architecture is scalable and can be deployed in standalone or distributed (multi-node) environments for large enterprises.

## **Search Processing Language (SPL)**

One of Splunk's strengths is its Search Processing Language (SPL), a powerful query language designed for filtering, transforming, and analyzing log data.

**Example SPL query:**

Index=windows Event Code=4625

Stats count by Account\_Name, Workstation\_Name

This query counts failed login attempts for each user and workstation.

## **Key Capabilities of Splunk**

### **a. Log Management**

Splunk excels at collecting and managing logs from diverse sources, allowing rapid search across millions of events.

#### b. SIEM and Cybersecurity

Splunk Enterprise Security (ES) transforms Splunk into a full SIEM platform. It provides:

- Threat detection
- Event correlation
- Security dashboards
- Automated alerting
- Investigation tools

Example security query:

```
index=firewall action=blocked  
| stats count by src_ip
```

This identifies the top IP addresses being blocked by the firewall.

#### c. Observability and Monitoring

Splunk supports modern DevOps and cloud environments by offering:

- Real-time performance monitoring

- Application Performance Monitoring (APM)
- Infrastructure health analytics
- Error and latency monitoring

d. Dashboards and Visualization

Splunk provides advanced visualization tools for building operational and security dashboards using charts, maps, gauges, and real-time panels.

e. Alerting and Automation

Splunk can trigger:

- Email alerts
- Automated scripts
- SOAR playbooks through Splunk Phantom

f. Machine Learning Toolkit (MLTK)

MLTK enables:

- Anomaly detection
- Forecasting
- Behavioral analytics

**Splunk in Security Operations Centers (SOC)**

### **a. Threat Detection**

Analysts use SPL queries to detect brute-force attacks, malware activity, and lateral movement within networks.

### **b. Incident Investigation**

Splunk provides timeline analysis and event correlation, helping analysts understand attack paths and methods.

### **c. Response and Automation**

When integrated with SOAR platforms, Splunk can automatically

- Block malicious IPs
- Disable compromised accounts
- Isolate infected endpoints

### **d. SOC Dashboards**

Common SOC dashboards include:

- Failed authentication attempts
- Malware alerts
- Network anomalies
- User behavior analytics

## **Use Cases beyond Security**

Splunk is widely used outside cybersecurity:

- IT Operations: uptime, performance, and failure analysis
- DevOps: log aggregation for debugging
- IoT: sensor data analytics
- Business Intelligence: user behavior and transaction monitoring

## **Challenges and Limitations**

### **a. High Cost**

Splunk licensing is expensive because it is based on daily ingested data volume, making it costly for smaller organizations.

### **b. Complexity of SPL**

Although powerful, SPL has a learning curve that requires practice and training.

### **c. Resource Consumption**

Indexers require significant CPU, RAM, and storage for optimal performance.

## **Future of Splunk**

Splunk is evolving toward:

- Cloud-native deployments

- AI-driven analytics
- Faster real-time processing
- Enhanced SOAR automation

## **Project Setup Summary**

For this project, we worked inside the environment provided through the Netlab pod (Group C), which acted as the outer layer of our entire setup.

Once we logged into our assigned pod (Group C), we were placed on the host Windows Server, which is the main machine responsible for running Hyper-V.

From there, we installed and opened Hyper-V Manager, which allowed us to create and control virtual machines inside the host system.

Inside Hyper-V Manager, we accessed the Windows Server Virtual Machine (the inner VM), and this is where we were required to install and configure Splunk Enterprise. Before we could install anything, we had to make sure the VM itself had proper network connectivity.

To do this, we opened the Virtual Switch Manager on the host and created a new External Virtual Switch, which bridges the VM to the network. Without this switch, the VM could not get its own IP address.

Once the switch was created, we attached it to the Windows Server VM and rebooted. After running ipconfig, we confirmed that the VM finally had a real IP address, which meant it could access the internet and download software.

However, we ran into another practical issue at this stage: downloads were extremely slow inside the Netlab environment. Even downloading the Splunk .msi installer took much longer than expected, and we had to retry multiple times because the connection would drop or freeze.

Eventually, after waiting and troubleshooting, we managed to download Splunk Enterprise and complete the installation inside the VM.

When Splunk finally installed successfully, we logged in through Splunk Web and then moved on to the next part of the project i.e. importing the attack dataset. We downloaded the attack\_data files from GitHub, but the download speed was again very slow, and extracting the files inside the VM took additional time.

Once everything was ready, we tried to upload the dataset into Splunk using the “Add Data” option. This is where we faced the biggest challenge: Splunk was unable to index many of the files.

At this point, it became clear that the issue wasn’t something we could fix ourselves. It was likely related to limitations within the Netlab VM environment, including storage restrictions, broken parsing, or indexing constraints.

We tried different file types, created new indexes, and repeated the process multiple times, but no method successfully import the attack data into our Splunk instance.

After we explained the situation, Professor decided to give us access to the college’s pre-configured Splunk server with some limitations as an alternative. This server already handles the attack dataset properly, allowing us to continue the analysis, dashboards, and reporting without being blocked by technical problems.

## Query 1: PORT SCAN DETECTION

Explanation: Detects sources attempting to connect to multiple ports (potential scanners)

The screenshot shows a Splunk search interface with the following details:

**Search Bar:** index== sourcetype="unifi" SYN  
| rex field=\_raw "SRC=(?<src\_ip>[0-9\.]\*)"  
| rex field=\_raw "DST=(?<dst\_ip>[0-9\.]\*)"  
| rex field=\_raw "DPT=(?<dest\_port>\d+)"  
| stats dc(dest\_port) as unique\_ports, values(dest\_port) as ports\_accessed, count as connection\_attempts BY src\_ip, dst\_ip  
| where unique\_ports > 20  
| sort - unique\_ports  
| eval threat\_level=case(  
 unique\_ports > 100, "Critical",  
 unique\_ports > 50, "High",  
 unique\_ports > 20, "Medium"  
)  
| table src\_ip, dst\_ip, unique\_ports, connection\_attempts, threat\_level, ports\_accessed

**Results Table:**

src_ip	dst_ip	unique_ports	connection_attempts	threat_level	ports_accessed
160.250.4.167	192.168.210.182	215	215	Critical	10002 10003 10012 10050 101 10189 10201 1050 10906 11000

Port Scan Detection | Splunk 10.0

Not secure https://splunk.cambrianlabs.ca:8000/en-US/app/search/port\_scan\_detection?tab=layout\_1&form.global\_time.earliest=0&form.glo...

splunk>enterprise Apps Student Access Accou... Messages Settings Activity Help Find Search

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

## Port Scan Detection

Global Time Range

All time

src\_ip dst\_ip unique\_ports connection\_attempts threat\_level ports\_accessed

src_ip	dst_ip	unique_ports	connection_attempts	threat_level	ports_accessed
160.250.4.167	192.168.210.188	233	233	Critical	10001 10002 10003 10004 10010 10012 10020

1 / 2

## Query 2: 2. SUSPICIOUS OUTBOUND CONNECTIONS TO NON-STANDARD PORTS

Identifies internal hosts connecting to unusual high ports (potential C2)

Focuses on ports commonly used by malware: 4444, 5555, 6666, 8080, 8888, etc

**NO RESULT** meaning that no internal host makes outbound connections to unusual ports

```

index=* sourcetype="unifi"
| rex field=_raw "SRC=(?<src_ip>10\.[0-9\.]+|192\.168\.[0-9\.]+)" 
| rex field=_raw "DST=(?<dst_ip>[0-9\.]+)" 
| rex field=_raw "DPT=(?<dest_port>\d+)" 
| search dest_port IN {4444, 5555, 6666, 7777, 8888, 8888, 9999, 31337, 12345, 54321}
| where NOT match(dst_ip, "10\.\.") AND NOT match(dst_ip, "192\.168\.\.")
| stats count, values(dest_port) as suspicious_ports, dc(dst_ip) as unique_destinations BY src_ip
| sort - count
| eval risk_score=count * unique_destinations
| table src_ip, count, suspicious_ports, unique_destinations, risk_score|

```

No results found. Try expanding the time range.

#### Query 4.4. BLOCKED TRAFFIC ANALYSIS (FIREWALL DENIALS)

Analyzes traffic blocked by firewall rules to identify attack patterns. High block counts indicate persistent attack attempts

```

index=* sourcetype="unifi" (DESCR="*DENY*" OR DESCRIPTOR="BLOCK" OR DESCRIPTOR="DROP")
| rex field=_raw "SRC=(?<src_ip>[0-9\.]+)"
| rex field=_raw "DST=(?<dst_ip>[0-9\.]+)"
| rex field=_raw "DPT=(?<dest_port>\d+)"
| rex field=_raw "DESCR=\"(?<rule_name>[^"]+)\\""
| stats count as block_count, dc(dest_port) as ports_attempted, values(dest_port) as ports BY src_ip, dst_ip, rule_name
| sort - block_count
| where block_count > 50
| eval threat_assessment=case(
    block_count > 1000, "Critical - Active Attack",
    block_count > 500, "High - Persistent Probing",
    block_count > 100, "Medium - Repeated Attempts"
)
| table src_ip, dst_ip, rule_name, block_count, ports_attempted, threat_assessment

```

src_ip	dst_ip	rule_name	block_count	ports_attempted	threat_assessment
192.168.210.185	10.10.15.21	[WAN_DMZ]Block All Traffic	386814	1	Critical - Active Attack
78.128.112.74	10.10.15.3	Block Traffic from HIGH-RISK-IPs	4264	1	Critical - Active Attack
167.94.146.36	10.10.15.20	Block Traffic from HIGH-RISK-IPs	869	867	High - Persistent Probing
52.14.122.207	10.10.15.21	Block Traffic from HIGH-RISK-IPs	560	190	High - Persistent Probing
52.14.122.207	10.10.15.20	Block Traffic from HIGH-RISK-IPs	554	187	High - Persistent Probing

## Query 6 ABNORMAL PROTOCOL USAGE

# Detects use of protocols that shouldn't be present in normal traffic. Focus on GRE tunnels, unusual encapsulation that may hide malicious traffic

```

index=* sourcetype="unifi" (DESCR=*DENY* OR DESCRIPTOR=*BLOCK* OR DESCRIPTOR=*DROP*)
| rex field=_raw "SRC=(?<src_ip>[0-9\.\.]+)"
| rex field=_raw "DST=(?<dst_ip>[0-9\.\.]+)"
| rex field=_raw "DPT=(?<dest_port>\d+)"
| rex field=_raw "DESCR=(?<rule_name>[^"]+)"
| stats count as block_count, dc(dest_port) as ports_attempted, values(dest_port) as ports BY src_ip, dst_ip, rule_name
| sort -block_count
| where block_count > 50
| eval threat_assessment=case(
    block_count > 1000, "Critical - Active Attack",
    block_count > 500, "High - Persistent Probing",
    block_count > 100, "Medium - Repeated Attempts"
)
| table src_ip, dst_ip, rule_name, block_count, ports_attempted, threat_assessment

```

125 events (12/6/25 12:00:00.000 PM to 12/7/25 12:04:51.000 PM) No Event Sampling

## Query 7: BRUTE FORCE CONNECTION ATTEMPTS

Identifies sources making rapid repeated connection attempts

High frequency to same destination/port suggests brute force or DoS

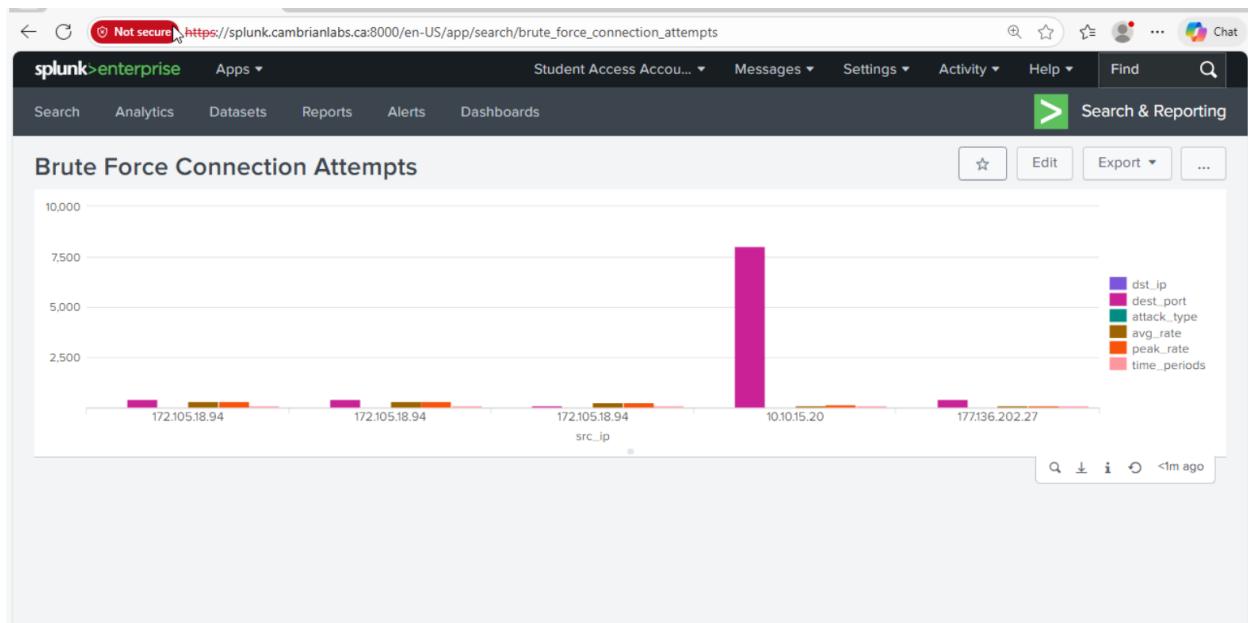
The screenshot shows a Splunk search interface with the following details:

Search bar: index== sourcetype="unifi" SYN  
| rex field=\_raw "SRC=(?<src\_ip>[0-9\.]+)"  
| rex field=\_raw "DST=(?<dst\_ip>[0-9\.]+)"  
| rex field=\_raw "DPT=(?<dest\_port>\d+)"  
| bucket \_time span=1m  
| stats count as attempts\_per\_minute BY \_time, src\_ip, dst\_ip, dest\_port  
| where attempts\_per\_minute > 100  
| stats avg(attempts\_per\_minute) as avg\_rate, max(attempts\_per\_minute) as peak\_rate, count as time\_periods BY src\_ip, dst\_ip, dest\_port  
| sort - peak\_rate  
| eval attack\_type=case(  
 dest\_port=22, "SSH Brute Force",  
 dest\_port=3389, "RDP Brute Force",  
 dest\_port=21, "FTP Brute Force",  
 dest\_port=445, "SMB Brute Force",  
 1=1, "High-Frequency Attack"  
)  
| table src\_ip, dst\_ip, dest\_port, attack\_type, avg\_rate, peak\_rate, time\_periods

Results: ✓ 16,535,602 events (before 12/7/25 10:43:05.000 PM)

Statistics (73) tab selected.

src_ip	dst_ip	dest_port	attack_type	avg_rate	peak_rate	time_periods
10.10.15.20	10.10.10.52	8006	High-Frequency Attack	158.2214897824654	1528	1517
5.254.74.2	10.10.15.20	443	High-Frequency Attack	354.2352941176471	1026	17
44.220.185.77	10.10.15.20	443	High-Frequency Attack	562	562	1
44.220.185.77	192.168.210.182	443	High-Frequency Attack	562	562	1



The screenshot shows a Splunk search interface with the title 'Brute Force'. The table has columns: src\_ip, dst\_ip, dest\_port, attack\_type, avg\_rate, peak\_rate, and time\_periods. Two rows are visible:

src_ip	dst_ip	dest_port	attack_type	avg_rate	peak_rate	time_periods
10.10.15.20	10.10.10.52	8006	High-Frequency Attack	129	161	4
192.168.104.101	192.168.210.183	8005	High-Frequency Attack	112	112	1

## Query: 8. SUSPICIOUS ADMIN PORT ACCESS

Monitors access to administrative ports from unexpected sources Ports: SSH(22), RDP(3389), Telnet(23), SQL(1433,3306), etc.

The screenshot shows a Splunk search interface with the title 'New Search'. The search query is displayed in the search bar:

```

index=sourceType:unifi
| rex fields:raw "SRC=(?src_ip:[0-9.]+)"
| rex fields:raw "DST=(?dst_ip:[0-9.]+)"
| rex fields:raw "DPT=(?dest_port:[0-9]+)"
| search dest_port IN [22, 23, 3389, 1433, 3306, 5432, 27017, 6379, 9200, 5601]
| where NOT match(src_ip, '^10\.\.') AND NOT match(src_ip, '^192\.\.168\.\.')
| eval service=case(
    dest_port=22, "SSH",
    dest_port=23, "Telnet",
    dest_port=3389, "RDP",
    dest_port=1433, "MS SQL",
    dest_port=3306, "MySQL",
    dest_port=5432, "PostgreSQL",
    dest_port=27017, "MongoDB",
    dest_port=6379, "Redis",
    dest_port=9200, "Elasticsearch",
    dest_port=5000, "Kibana",
    !+, "Unknown Admin Service"
)
| stats count as access_attempts, earliest(_time) as first_seen, latest(_time) as last_seen BY src_ip, dst_ip, dest_port, service
| sort - access_attempts
| eval alert_severity(case(
    access_attempts > 100, "Critical",
    access_attempts > 50, "High",
    access_attempts > 10, "Medium"
))
| table src_ip, dst_ip, service, dest_port, access_attempts, alert_severity, first_seen, last_seen

```

The table shows 111,283 events. The columns are: src\_ip, dst\_ip, service, dest\_port, access\_attempts, alert\_severity, first\_seen, and last\_seen. A preview of the data is shown below:

src_ip	dst_ip	service	dest_port	access_attempts	alert_severity	first_seen	last_seen
78.128.112.74	192.168.210.191	SSH	22	4271	Critical	1760031600	1765161103
78.128.112.74	10.10.15.3	SSH	22	4264	Critical	1760037361	1765161103
148.72.158.192	192.168.210.191	SSH	22	1121	Critical	1760092000	1765149201
185.156.73.233	192.168.210.188	SSH	22	831	Critical	1760486892	1765137892
78.128.114.138	192.168.210.182	RDP	3389	791	Critical	1760031875	1765138412
78.128.114.138	192.168.210.191	RDP	3389	791	Critical	1760031832	1765139365

src_ip	dst_ip	service	dest_port	access_attempts	alert_severity	first_seen	last_seen
78.128.112.74	192.168.210.191	SSH	22	4271	Critical	1760031600	1765161103
78.128.112.74	10.10.15.3	SSH	22	4264	Critical	1760037361	1765161103
148.72.158.192	192.168.210.191	SSH	22	1121	Critical	1760092000	1765145201
185.156.73.233	192.168.210.188	SSH	22	831	Critical	1760466892	17611327892
78.128.114.130	192.168.210.182	RDP	3389	791	Critical	1760031875	1765138412
78.128.114.130	192.168.210.191	RDP	3389	791	Critical	1760031832	1765139365
78.128.114.130	192.168.210.188	RDP	3389	784	Critical	1760031875	1765140066
78.128.114.126	192.168.210.188	RDP	3389	577	Critical	1760031600	1765116207
78.128.114.126	192.168.210.191	RDP	3389	572	Critical	1760081846	1765114713
78.128.114.126	192.168.210.182	RDP	3389	568	Critical	1760031600	1765114716
79.124.49.98	192.168.210.182	RDP	3389	507	Critical	1760034479	1763412222
79.124.49.98	192.168.210.191	RDP	3389	507	Critical	1760031600	1763409732
79.124.49.98	192.168.210.188	RDP	3389	504	Critical	1760034451	1763410216
161.35.152.142	192.168.210.188	SSH	22	345	Critical	1760443514	1760455802
184.0.234.19	192.168.210.188	SSH	22	308	Critical	176046573	1761134257
146.190.225.91	192.168.210.188	SSH	22	295	Critical	1760443258	1760454208
184.180.48.63	192.168.210.182	SSH	22	262	Critical	1760051095	1765133757
194.180.48.63	192.168.210.188	SSH	22	262	Critical	1760051079	1765153771

Not secure https://splunk.cambrianlabs.ca:8000/en-US/app/search/suspicious\_admin\_port\_access?form.global\_time.earliest=-24h%40h&for...

Splunk > enterprise Apps ▾

Student Access Account ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Search & Reporting ▾

Suspicious Admin Port Access

Global Time Range ▾ List 24 hours

src\_ip dst\_ip service dest\_port access\_attempts alert\_severity first\_seen last\_seen

78.128.112.74	10.10.15.3	SSH	22	2441	Critical	1762464288	1765161103
78.128.112.74	192.168.210.191	SSH	22	2441	Critical	1762464288	1765161103
78.128.114.130	192.168.210.182	RDP	3389	333	Critical	1762673496	1765138412
78.128.114.130	192.168.210.191	RDP	3389	332	Critical	1762673504	1765139365
79.124.114.130	192.168.210.190	RDP	3389	2777	Critical	1762673504	1765140096

1 Prev 1 2 3 ... 1765140096

## Query 9: BEACONING DETECTION (C2 COMMUNICATION)

Identifies regular, periodic connections that may indicate malware beaconing

Looks for consistent time intervals between connections

Search & Reporting

```

index=_ sourceType="unifi"
| rex field=_raw "SRCIP=(?>src_ip>10.(0|9)\.2|192\.168\.[0-9]\.)"
| rex field=_raw "DSTIP=(?>dst_ip>0-9\.)"
| rex field=_raw "TIME=(?>time>[0-9]{10}\.0)" AND NOT match(dst_ip, "192.168.*")
| sort src_ip, dst_ip, _time
| streamstats current=_ last(_time) as last_time BY src_ip, dst_ip
| eval consistency_score=last(_time)-_time
| where isnotnull(_time_delta)
| stats count, avg(_time_delta) as avg_interval, stdev(_time_delta) as stdev_interval, min(_time_delta) as min_interval, max(_time_delta) as max_interval BY src_ip, dst_ip
| eval consistency_score=round((avg_interval/stdev_interval)*100, 2)
| eval consistency_score=round(((stdev_interval/avg_interval)*100, 2))
| sort - consistency_score
| eval consistency_score=case
    when consistency_score > 90 AND avg_interval < 600, "Critical - Highly Regular Beacon"
    when consistency_score > 80, "High - Potential C2 Beacon"
    when consistency_score > 70, "Medium - Regular Pattern Detected"
    otherwise "Low - No Pattern Detected"
| table src_ip, dst_ip, count, avg_interval_minutes, consistency_score, beacon_risk

```

**9,947 events (Before 12/7/25 11:04:02.000 PM)** No Event Sampling \*

Events Patterns Statistics (2) Visualization

src_ip	dst_ip	count	avg_interval_minutes	consistency_score	beacon_risk
10.10.25.9	23.133.168.247	570	17.60	98.19	High - Potential C2 Beacon
10.10.25.9	23.133.168.246	122	17.70	98.92	High - Potential C2 Beacon

Not secure [https://splunk.cambrianlabs.ca:8000/en-US/app/search/beaconing\\_detection\\_-\\_\\_c2\\_communications](https://splunk.cambrianlabs.ca:8000/en-US/app/search/beaconing_detection_-__c2_communications)

Student Access Account 1 Messages Settings Activity Help Find Q

Beaconing Detection - C2 Communications

src_ip	dst_ip	count	avg_interval_minutes	consistency_score	beacon_risk
10.30.9.157	146.190.225.48	22	5.00	99.72	Critical - Highly Regular Beacon
10.10.25.9	162.159.200.123	123	17.60	98.32	High - Potential C2 Beacon
10.10.25.9	23.133.168.246	122	17.70	90.92	High - Potential C2 Beacon
10.30.10.42	23.128.92.19	40	1.14	83.37	High - Potential C2 Beacon
10.30.9.157	34.149.20.200	45	2.52	81.58	High - Potential C2 Beacon

## Query 10: GEOGRAPHIC ANOMALY DETECTION (CONNECTIONS TO SUSPICIOUS COUNTRIES)

Identifies connections to/from high-risk geographic locations

Note: Requires iplocation command (may need external lookup tables)

Alternative approach: Focus on known suspicious IP ranges

Search | Splunk 10.0.1

New tab

Not secure https://splunk.cambrianlabs.ca:8000/en-US/app/search/search?q=search%20index%3D%20sourcetype%3Dunifi%0A%7C%20rex%2...

Save As ▾ Create Table View Close

Time range: Last 24 hours

New Search

```

index== sourcetype="unifi"
| rex field=_raw "SRC=(?<src_ip>[0-9\.]+)"
| rex field=_raw "DST=(?<dst_ip>[0-9\.]+)"
| eval suspicious_source=case(
    match(src_ip, '^185\.'), "Suspicious Range",
    match(src_ip, '^95\.'), "High-Risk Range",
    match(src_ip, '^194\.'), "Known VPN/Proxy Range",
    !1, "Normal"
)
| eval suspicious_dest=case(
    match(dst_ip, '^185\.'), "Suspicious Range",
    match(dst_ip, '^95\.'), "High-Risk Range",
    match(dst_ip, '^194\.'), "Known VPN/Proxy Range",
    !1, "Normal"
)
| where suspicious_source!="Normal" OR suspicious_dest!="Normal"
| stats count, values(suspicious_source) as source_risk, values(suspicious_dest) as dest_risk BY src_ip, dst_ip
| sort - count
| eval investigation_priority=case(
    count > 100, "Immediate",
    count > 50, "High",
    count > 10, "Medium"
)
| table src_ip, dst_ip, count, source_risk, dest_risk, investigation_priority

```

1,394 events (12/6/25 12:00:00 PM to 12/7/25 12:12:44 PM) No Event Sampling

Events Patterns Statistics (240) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

src_ip	dst_ip	count	source_risk	dest_risk	investigation_priority
185.156.73.180	192.168.210.188	32	Suspicious Range	Normal	Medium
185.156.73.181	192.168.210.191	32	Suspicious Range	Normal	Medium
185.156.73.182	192.168.210.188	32	Suspicious Range	Normal	Medium
185.191.127.110	192.168.210.182	32	Suspicious Range	Normal	Medium
185.191.127.110	192.168.210.191	32	Suspicious Range	Normal	Medium
185.156.73.181	192.168.210.182	31	Suspicious Range	Normal	Medium
185.191.127.110	192.168.210.188	31	Suspicious Range	Normal	Medium
185.156.73.182	192.168.210.191	30	Suspicious Range	Normal	Medium
185.156.73.180	192.168.210.191	29	Suspicious Range	Normal	Medium
185.156.73.181	192.168.210.188	28	Suspicious Range	Normal	Medium

✓ 137,339 events (before 12/7/25 11:17:39 PM) No Event Sampling

Events Patterns Statistics (3,784) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

src_ip	dst_ip	count	source_risk	dest_risk	investigation_priority
194.180.48.23	192.168.210.182	4001	Known VPN/Proxy Range	Normal	Immediate
194.180.48.23	192.168.210.191	4001	Known VPN/Proxy Range	Normal	Immediate
194.180.48.23	192.168.210.188	4000	Known VPN/Proxy Range	Normal	Immediate
194.180.49.218	192.168.210.191	3284	Known VPN/Proxy Range	Normal	Immediate
194.180.49.218	192.168.210.182	3277	Known VPN/Proxy Range	Normal	Immediate
194.180.49.218	192.168.210.188	3274	Known VPN/Proxy Range	Normal	Immediate
194.180.49.217	192.168.210.182	2991	Known VPN/Proxy Range	Normal	Immediate
194.180.49.217	192.168.210.191	2990	Known VPN/Proxy Range	Normal	Immediate
194.180.49.217	192.168.210.188	2989	Known VPN/Proxy Range	Normal	Immediate
194.180.49.216	192.168.210.191	2644	Known VPN/Proxy Range	Normal	Immediate
194.180.49.216	192.168.210.188	2631	Known VPN/Proxy Range	Normal	Immediate
194.180.49.216	192.168.210.182	2614	Known VPN/Proxy Range	Normal	Immediate
95.214.53.196	192.168.210.191	1649	High-Risk Range	Normal	Immediate
95.214.53.196	192.168.210.188	1647	High-Risk Range	Normal	Immediate
95.214.53.196	192.168.210.182	1644	High-Risk Range	Normal	Immediate
194.195.208.25	192.168.210.191	1539	Known VPN/Proxy Range	Normal	Immediate
185.244.104.2	192.168.210.191	1432	Suspicious Range	Normal	Immediate
185.244.104.2	192.168.210.182	1427	Suspicious Range	Normal	Immediate

Splunk Enterprise - Geographic Anomaly Detection

Search Analytics Datasets Reports Alerts Dashboards

Student Access Account 1 Messages Settings Activity Help Find Search & Reporting

Geographic Anomaly Detection

src\_ip \$ dst\_ip \$ count \$ source\_risk \$ dest\_risk \$ investigation\_priority \$

src_ip \$	dst_ip \$	count \$	source_risk \$	dest_risk \$	investigation_priority \$
194.180.48.23	192.168.210.182	4001	Known VPN/Proxy Range	Normal	Immediate
194.180.48.23	192.168.210.191	4001	Known VPN/Proxy Range	Normal	Immediate
194.180.48.23	192.168.210.188	4000	Known VPN/Proxy Range	Normal	Immediate
194.195.208.25	192.168.210.182	790	Known VPN/Proxy Range	Normal	Immediate
95.214.53.196	192.168.210.182	741	High-Risk Range	Normal	Immediate
95.214.53.196	192.168.210.188	741	High-Risk Range	Normal	Immediate
95.214.53.196	192.168.210.191	741	High-Risk Range	Normal	Immediate
194.195.208.25	192.168.210.191	666	Known VPN/Proxy Range	Normal	Immediate
194.195.208.6	192.168.210.191	656	Known VPN/Proxy Range	Normal	Immediate
185.244.104.2	192.168.210.182	654	Suspicious Range	Normal	Immediate
185.244.104.2	192.168.210.188	650	Suspicious Range	Normal	Immediate
185.244.104.2	192.168.210.191	641	Suspicious Range	Normal	Immediate
185.156.73.86	192.168.210.191	629	Suspicious Range	Normal	Immediate
185.156.73.86	192.168.210.188	627	Suspicious Range	Normal	Immediate
185.156.73.86	192.168.210.182	623	Suspicious Range	Normal	Immediate
194.195.208.6	192.168.210.182	572	Known VPN/Proxy Range	Normal	Immediate
185.156.73.181	192.168.210.191	553	Suspicious Range	Normal	Immediate
185.156.73.181	192.168.210.188	551	Suspicious Range	Normal	Immediate
185.156.73.180	192.168.210.182	546	Suspicious Range	Normal	Immediate
185.156.73.181	192.168.210.182	546	Suspicious Range	Normal	Immediate

< Prev 1 2 3 4 5 6 7 8 9 10 Next >

1,194 events (12/6/25 12:00:00,000 PM to 12/7/25 12:12:44,000 PM) No Event Sampling ▾

Events Patterns Statistics (240) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

src_ip \$	dst_ip \$	count \$	source_risk \$	dest_risk \$	investigation_priority \$
185.156.73.180	192.168.210.188	32	Suspicious Range	Normal	Medium
185.156.73.181	192.168.210.191	32	Suspicious Range	Normal	Medium
185.156.73.182	192.168.210.188	32	Suspicious Range	Normal	Medium
185.191.127.110	192.168.210.182	32	Suspicious Range	Normal	Medium
185.191.127.110	192.168.210.191	32	Suspicious Range	Normal	Medium
185.156.73.181	192.168.210.182	31	Suspicious Range	Normal	Medium
185.191.127.110	192.168.210.188	31	Suspicious Range	Normal	Medium
185.156.73.182	192.168.210.191	30	Suspicious Range	Normal	Medium
185.156.73.188	192.168.210.191	29	Suspicious Range	Normal	Medium
185.156.73.181	192.168.210.188	29	Suspicious Range	Normal	Medium
185.156.73.182	192.168.210.182	29	Suspicious Range	Normal	Medium
95.214.53.196	192.168.210.188	29	High-Risk Range	Normal	Medium
95.214.53.196	192.168.210.191	29	High-Risk Range	Normal	Medium
185.156.73.188	192.168.210.182	28	Suspicious Range	Normal	Medium
185.156.73.86	192.168.210.188	28	Suspicious Range	Normal	Medium
185.156.73.86	192.168.210.191	27	Suspicious Range	Normal	Medium
185.156.73.86	192.168.210.182	26	Suspicious Range	Normal	Medium
185.156.73.86	192.168.210.182	24	Known VPN/Proxy Range	Normal	Medium
194.180.48.63	192.168.210.182	24	Known VPN/Proxy Range	Normal	Medium
194.180.48.63	192.168.210.191	24	Known VPN/Proxy Range	Normal	Medium

< Prev 1 2 3 4 5 6 7 8 9 10 Next >

Windows Type here to search 12:13 PM 12/7/2025

Configuration    Uptime | Splunk 10.0.1    Search | Splunk 10.0.1    Search | Splunk 10.0.1    New Tab

Not Secure http://4017-monitoring.cambrian.cambrianc.on.ca:8000/en-US/app/search/search?q=search%20node\_name&display.page.search.mode=smart&dispatch.sample\_ratio=1&workload\_pool=8

Hide Fields All Fields Format Show: 20 Per Page View: List

	Time	Event
a agent	3	ide2: none,media=cdrom memory: 4096 meta: creation-qemu=9.2.0,ctime=1756325853 name: CAMB-CSECComp-P002-Ubuntu net0: virtio=BC:24:11:48:51:79,bridge=CMB3100030,firewall=1,tag=102 node_id: node/4017A-LSRV-ACD node_ip: 10.10.10.53 node_name: 4017A-LSRV-ACD
a boot	14	
a cluster	3	
# cores	9	
# cpu	100+	
# date_hour	24	
# date_mday	3	
# date_minute	60	
a date_month	1	
# date_second	60	
a date_wday	3	
# date_year	1	
a date_zone	2	
a description	20	
a digest	100+	
# disk	100+	
# diskread	100+	
# diskwrite	100+	
a id	100+	
a index	2	
# linecount	1	
# maxcpu	16	
# maxdisk	52	
# maxmem	21	
# mem	100+	
# memory	11	
a meta	55	
a name	100+	
a net0	100+	
# netin	100+	
# netout	100+	
a node	6	
a node_id	7	
a node_ip	7	
a node_name	7	
a ostype	6	
a parent	11	
a punct	100+	
a scsihw	4	
a smbios1	100+	
# sockets	3	
a splunk_server	1	
a status	7	
a tags	21	

maxmem

21 Values, 53.289% of events Selected Yes No

Reports

Average over time Maximum value over time Minimum value over time

Top values Top values by time Rare values

Events with this field

Avg: 11755995287.4784 Min: 536870912 Max: 811273252864  
Std Dev: 66990499012.511734

Top 10 Values	Count	%
2147483648	405,834	27.126%
4294967296	311,049	20.79%
8589934592	307,779	20.572%
1073741824	144,272	9.643%
6442450944	119,559	7.991%
536870912	99,366	6.642%
5905588032	38,732	2.589%
34359738368	38,728	2.588%
134832275456	3,280	0.219%
811221929984	3,188	0.213%

name: C15c0-MAPASA-PC-A-POOB/  
net0: virtio=BC:24:11:48:47:83,bridge=SAFETY\_NET  
node\_id: node/4017A-LSRV-ACD  
node\_ip: 10.10.10.53  
node\_name: 4017A-LSRV-ACD  
ostype: win10

MYLES PETERSON

1 5°C Mostly sunny

Search

Inbox - Mehdi X Timetables X Home | Moodle X Join conversation X HA: Forensics X

← → ↻ netlab.cambriancollege.ca/lab.cgi

MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambrian

> Topology Content Status Hyper-V

Search | Splunk 10.0.1

Not secure splunk.cambriancollege.ca:8000/en-US/app/search/search?q=splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

## New Search

```
index=* sourcetype="unifi" | timechart span=30m count
```

✓ 292,038 events (11/12/25 5:00:00.000 PM to 11/13/25 5:27:06.000 PM) No Events

Events Patterns Statistics (49) Visualization

Chart: all Column Chart Format Trellis

Time Period	Count
6:00 PM - 6:30 PM	~33,000
6:30 PM - 7:00 PM	~34,000
7:00 PM - 7:30 PM	~15,000
7:30 PM - 8:00 PM	~8,000
8:00 PM - 8:30 PM	~7,000
8:30 PM - 9:00 PM	~7,000
9:00 PM - 9:30 PM	~7,000
9:30 PM - 10:00 PM	~6,000
10:00 PM - 10:30 PM	~6,000
10:30 PM - 11:00 PM	~6,000
11:00 PM - 11:30 PM	~6,000
11:30 PM - 12:00 AM	~6,000
12:00 AM - 12:30 AM	~6,000
12:30 AM - 1:00 AM	~6,000
1:00 AM - 1:30 AM	~6,000
1:30 AM - 2:00 AM	~6,000

\_time  
2025-11-12 17:00:00

Type here to search

6°C Partly cloudy

Search

Inbox - Mehdi X Timetables X Home | Moodle X Join conversation X HA: Forensics ~

← → ↻ netlab.cambriancollege.ca/lab.cgi

MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambria

> Topology Content Status Hyper-V

Search | Splunk 10.0.1

Not secure splunk.cambriancollege.ca:8000/en-US/app/search/search?q=splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

## New Search

```
index=* sourcetype="unifi" | timechart span=30m count
```

✓ 292,038 events (11/12/25 5:00:00.000 PM to 11/13/25 5:27:06.000 PM) No Events

Events Patterns Statistics (49) Visualization

Show: 20 Per Page Format Preview: On

\_time :

2025-11-12 17:00:00
2025-11-12 17:30:00
2025-11-12 18:00:00
2025-11-12 18:30:00
2025-11-12 19:00:00
2025-11-12 19:30:00
2025-11-12 20:00:00
2025-11-12 20:30:00
2025-11-12 21:00:00
2025-11-12 21:30:00
2025-11-12 22:00:00

Windows Type here to search

Cloudy 6°C

Search

Inbox - Mehdi X Timetables X Home | Moodle X Join conversation X HA: Forensics X

← → ↻ netlab.cambriancollege.ca/lab.cgi

MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambria

> Topology Content Status Hyper-V

Unifi Traffic Overview | Splunk 10.0.2.10 X Search

Not secure splunk.cambriancollege.ca:8000/en-US/app/search/unifi\_traffic\_overview

splunk>enterprise Apps Stud... Messages

Search Analytics Datasets Reports Alerts Dashboards

## Unifi Traffic Overview ▾

Syslog Activity Over Time

Global Time Range

Last 24 hours

COUNT

40K  
20K

8:00 PM  
Wed Nov 12  
2025

12:00 AM  
Thu Nov 13

4:00 AM

8:00 AM

\_time

Type here to search

Temps to drop Sunday

Search

Inbox - Mehdi X Timetables X CSC-7310-001 - X Join conversation X HA: Forensics ~

← → ↻ netlab.cambriancollege.ca/lab.cgi

MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambria

> Topology Content Status Hyper-V

Dashboards | Splunk 10.0.1

Not secure splunk.cambrianlabs.ca:8000/en-US/app/search/dashboard

splunk>enterprise Apps Student Messages

Search Analytics Datasets Reports Alerts Dashboards

## Dashboards

Dashboards include searches, visualizations, and input controls that capture and present data from multiple sources.

### Latest Resources

★ Examples for Dashboard Studio  
Browse examples of dashboards & visualizations. Visit Example Hub ↗

Intro to Dashboard Studio  
Learn how to build dashboards with Dashboard Studio. Learn More ↗

5 Dashboards  Show only favorites All Your filter

i	★	Title	Actions	Owner
>	★	Count by Hosts	Edit	student.access
>	★	Job Details Dashbo...	Edit	nobody
>	★	Scheduled export i...	Edit	nobody
>	★	Test-dashboard1	Edit	student.access
>	★	Unifi Traffic Overvie...	Edit	student.access

6°C Partly cloudy Type here to search Search



40:36

[Join room](#)

Take control

[Configuration](#)[Proxmox-Home | Splunk 10.0.1](#)[Search | Splunk 10.0.1](#)[Search | Splunk 10.0.1](#)[New Tab](#)

Not Secure

http://4017-monitoring.cambrian.cambrianc.on.ca:8000/en-US/app/proxmox\_insights/proxmox-

[splunk>enterprise](#)

Apps ▾

[Proxmox-Home](#)[Nodes](#)[Map](#)[VM ▾](#)[Journal/Syslog](#)[Tasks](#)[Uptime](#)[Ressource Analyser](#)[Splunk](#)

## Proxmox-Home

Timeframe

Resolution

Cluster

Last 4 hours

15 Minute

All

Overall average CPU Utilization

last 15min/all nodes

Overall

last 15min



Total Amount of Cores

**228**

Total Amount of RAM

**2,958.41GB**

Total Amount of RAM used

**348.02GB**

Number of Nodes

**6**

Number of Nodes (Online)

**6**

Number of Nodes (Offline)

**0**

CPU Utilization per Node in %

100

75

50

25

RAM Ut

100

75

50

25

5:00 AM  
Fri Nov 21

5:30 AM

6:00 AM

6:30 AM

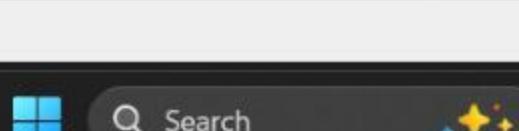
7:00 AM

7:30 AM

8:00 AM

8:30 AM

MYLES PETERSON



5°C

Mostly sunny



Search



Inbox - Mehdi X Timetables X Home | Moodle X Join conversation X HA: Forensics ~

← → ↻ netlab.cambriancollege.ca/lab.cgi

MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambrian

> Topology Content Status Hyper-V

Search | Splunk 10.0.1

Not secure splunk.cambriancollege.ca:8000/en-US/app/search/search?q=splunk>enterprise

splunk>enterprise Apps Stud... Messages

Search Analytics Datasets Reports Alerts Dashboards

## New Search

```
index=* sourcetype="unifi" ( msg="Login" OR action="login" or event="login" )  
| stats count AS login_count BY src  
| sort -login_count  
| head 20
```

✓ 0 events (1/1/24 12:00:00.000 AM to 1/1/25 12:00:00.000 AM)  
No Event Sampling ▾

Events Patterns Statistics (0) Visualization

Chart: all Column Chart ▾ Format ▾

No results found. Try expanding the search.

Type here to search

Upcoming Earnings

Search

Inbox - Mehdi X Timetables X Home | Moodle X Join conversation X HA: Forensics ~

← → ↻ netlab.cambriancollege.ca/lab.cgi

MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambrian

> Topology Content Status Hyper-V

Search | Splunk 10.0.1

Not secure splunk.cambriancollege.ca:8000/en-US/app/search/search?q=splunk>enterprise

splunk>enterprise Apps Stud... Messages

Search Analytics Datasets Reports Alerts Dashboards

## New Search

```
index=* sourcetype="unifi" ( msg="Login" OR action="login" or event="login" )  
| search NOT @ result="success" OR msg="Login Successful"  
| timechart span=30m count
```

✓ 0 events (1/24 12:00:00.000 AM to 1/25 12:00:00.000 AM)  
No Event Sampling ▾

Events Patterns Statistics (0) Visualization

Chart: all Column Chart ▾ Format ▾

No results found. Try expanding the search.

Type here to search

6°C Partly cloudy

Inbox - Mehdi Timetables Home | Moodle Join conversation HA: Forensics Chat

← → ↻ netlab.cambriancollege.ca/lab.cgi

MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambria

> Topology Content Status Hyper-V

Search | Splunk 10.0.1

New Search

| metasearch index=\*

✓ 291,118 events (11/12/25 5:00:00.000 PM to 11/13/25 5:23:06.000 PM) No Event

Events (291,118) Patterns Statistics Visualization

✓ Timeline format ▾ – Zoom Out + Zoom to Selection × Deselect

Format ▾ Show: 20 Per Page ▾

	i	Time	Event
◀ Hide Fields	☰ All Fields		
SELECTED FIELDS			
a host 1	>	11/13/25 5:23:05.000 PM	host = 10.10.10.
a source 1	>	11/13/25 5:23:04.000 PM	host = 10.10.10.
a sourcetype 1	>	11/13/25 5:23:04.000 PM	host = 10.10.10.
INTERESTING FIELDS			
a index 1	>	11/13/25 5:23:04.000 PM	host = 10.10.10.
a splunk_server 1	>	11/13/25 5:23:04.000 PM	host = 10.10.10.
+ Extract New Fields	>	11/13/25 5:23:04.000 PM	host = 10.10.10.
	>	11/13/25 5:23:04.000 PM	host = 10.10.10.
	>	11/13/25 5:23:04.000 PM	host = 10.10.10.
	>	11/13/25 5:23:04.000 PM	host = 10.10.10.

Windows Type here to search

Cloudy 6°C Search

Inbox - Mehdi X Timetables X Home | Moodle X Join conversation X HA: Forensics X

← → ↻ netlab.cambriancollege.ca/lab.cgi

MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambrian

> Topology Content Status Hyper-V

Search | Splunk 10.0.1

Not secure splunk.cambriancollege.ca:8000/en-US/app/search/search?q=splunk>enterprise

splunk>enterprise Apps Stud... Messages

Search Analytics Datasets Reports Alerts Dashboards

## New Search

```
index=* sourcetype="unifi"
|stats count by host
|sort - count
|head 10
```

255,788 of 255,788 events matched No Event Sampling ▾

Events (255,788) Patterns Statistics (1) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

host ▾

10.10.10.1

Type here to search

6°C Partly cloudy

## **Conclusion**

*Splunk proved to be an essential tool in our project for understanding how modern organizations manage, analyze, and respond to machine-generated data. Through hands-on configuration, indexing, and query analysis, we gained practical experience with key SOC functions such as threat detection, event correlation, visualization, and anomaly monitoring. Although we encountered technical constraints within the Netlab environment, these challenges enhanced our troubleshooting skills and deepened our understanding of Splunk's operational requirements.*

*Accessing the college's pre-configured Splunk server allowed us to complete our investigation and successfully run advanced security queries, including port-scan detection, beaconing analysis, suspicious outbound traffic monitoring, and geographic anomaly detection. These exercises demonstrated Splunk's value in real-world cybersecurity operations, where rapid insights and automated responses are crucial for defending systems.*

*Overall, this project strengthened our technical expertise, collaboration, and problem-solving capabilities. It also highlighted the importance of scalable log analytics platforms in modern security operations. Splunk remains one of the most powerful tools available for transforming raw machine data into actionable intelligence, making it a critical asset for cybersecurity teams and organizations striving to maintain strong security posture in an evolving threat landscape.*