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.

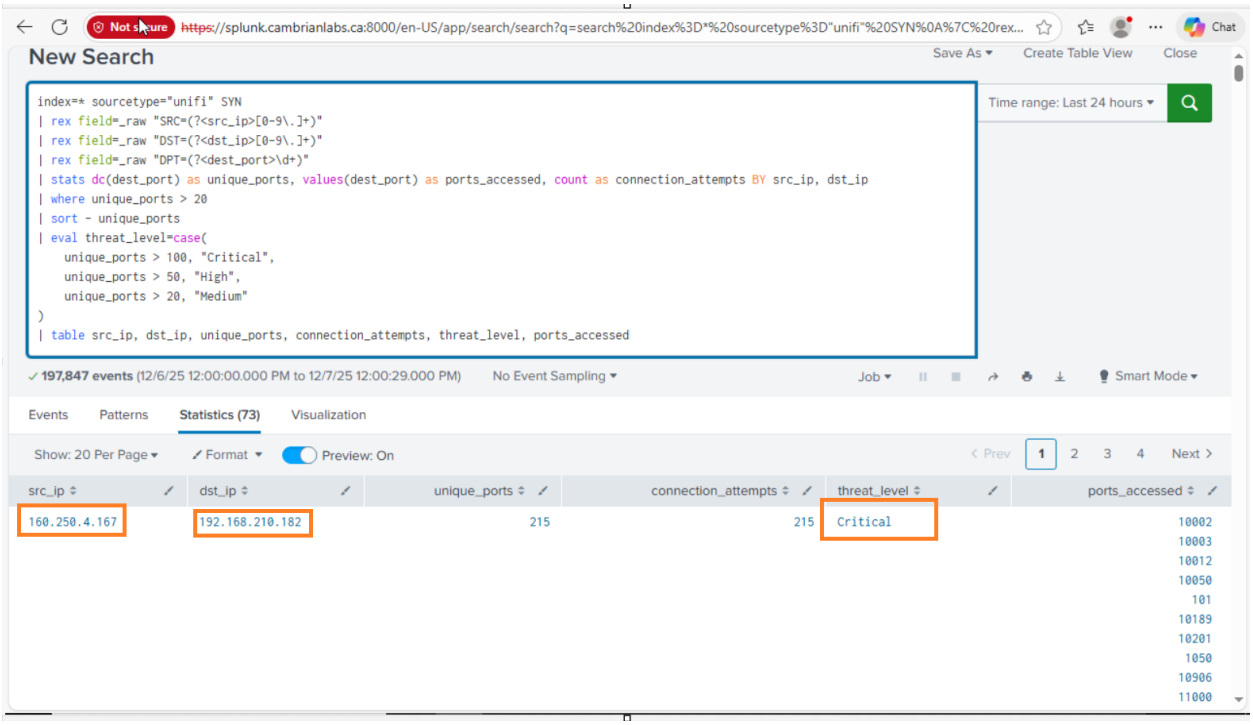
At this point, it became clear that the issue wasn’t something we could fix ourselves. it was likely related to limitations within the Netlab VM environment, including storage restrictions, broken parsing, or indexing constraints.

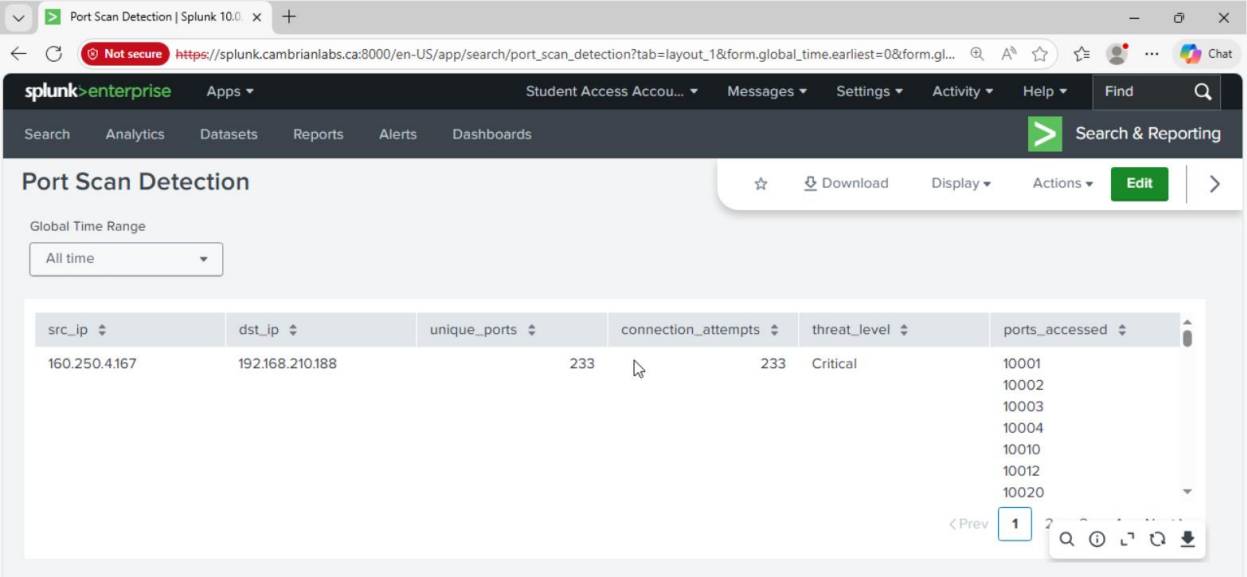
We tried different file types, created new indexes, and repeated the process multiple times, but no method successfully import the attack data into our Splunk instance.

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)



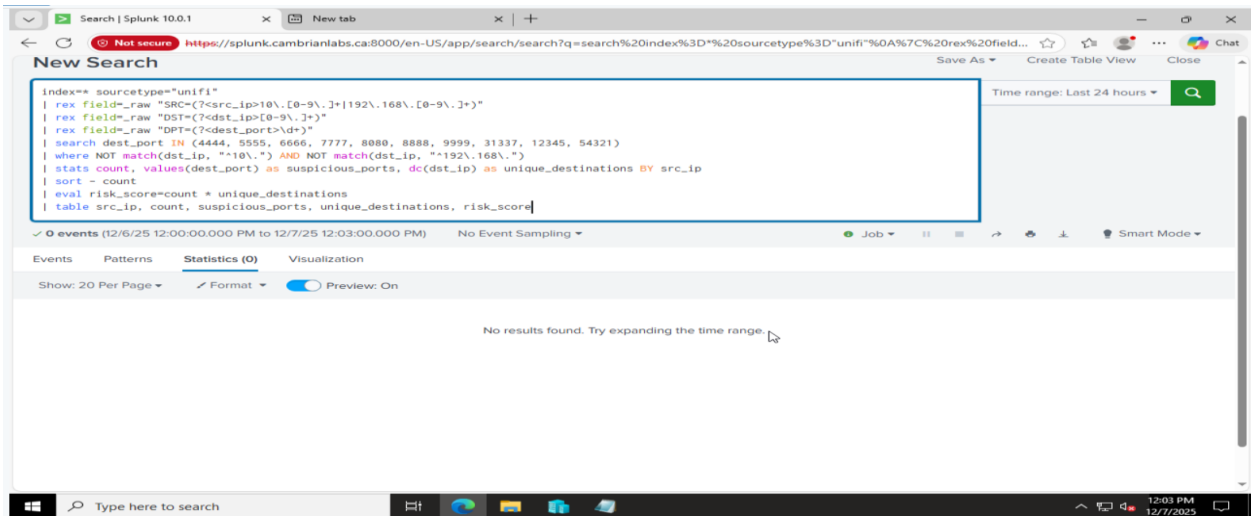


Query 2: 2. SUSPICIOUS OUTBOUND CONNECTIONS TO NON-STANDARD PORTS

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

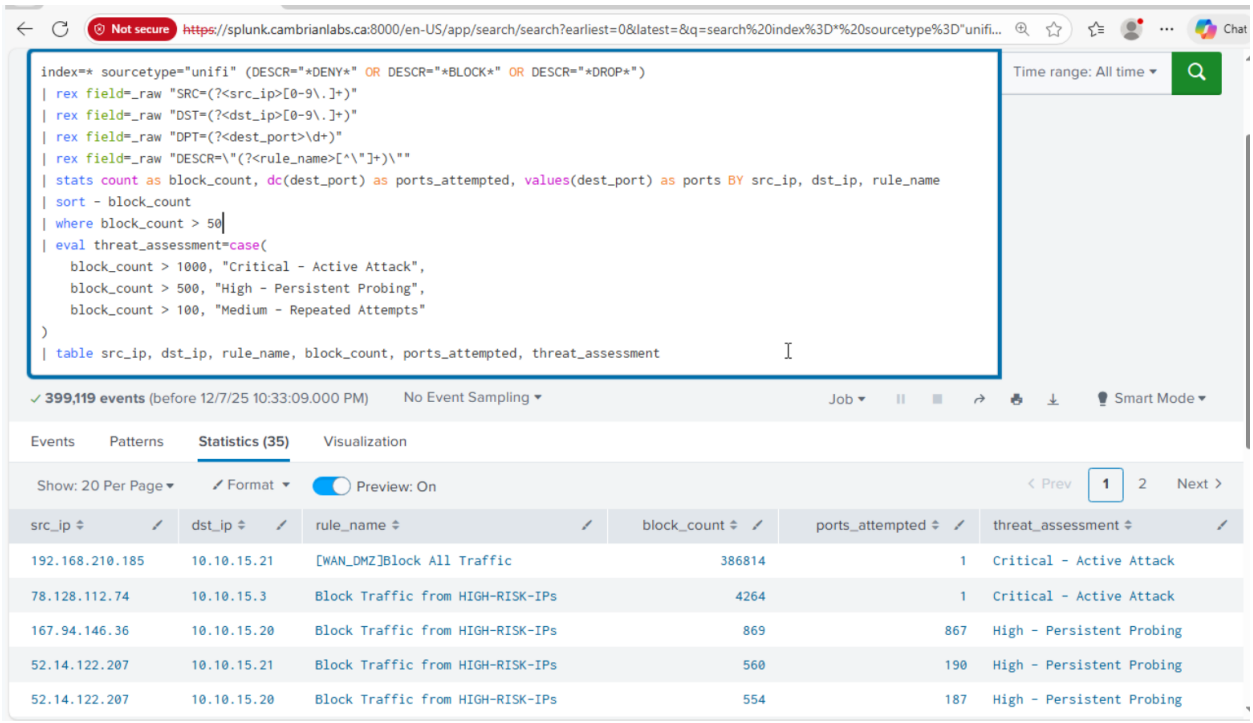
Focuses on ports commonly used by malware: 4444, 5555, 6666, 8080, 8888, etc

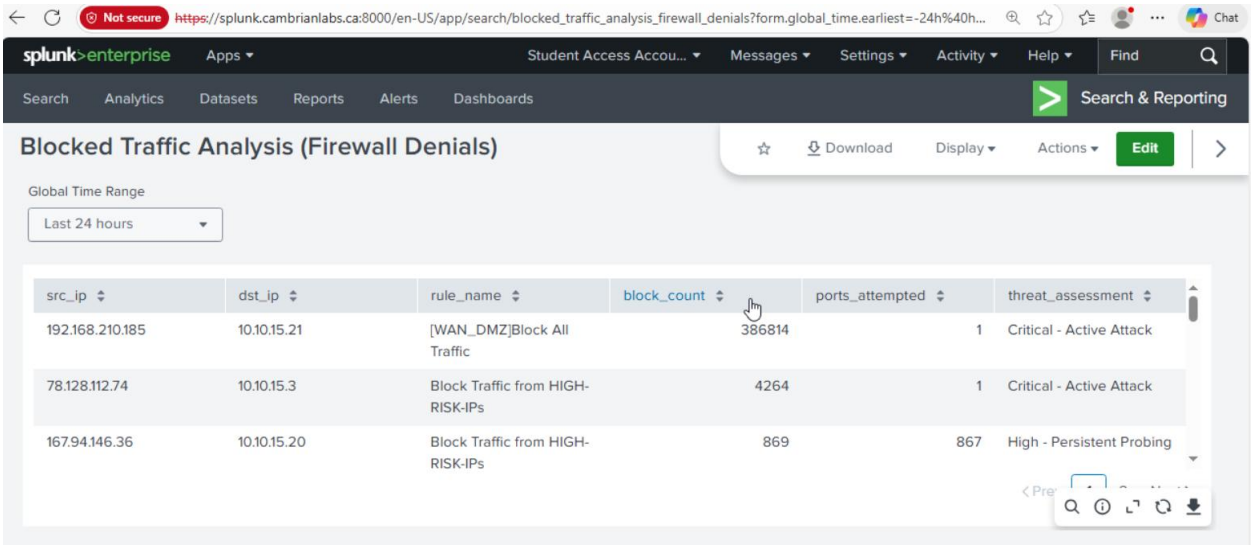
NO RESULT meaning that no internal host makes outbound connections to unusual ports



Query 4.4. BLOCKED TRAFFIC ANALYSIS (FIREWALL DENIALS)

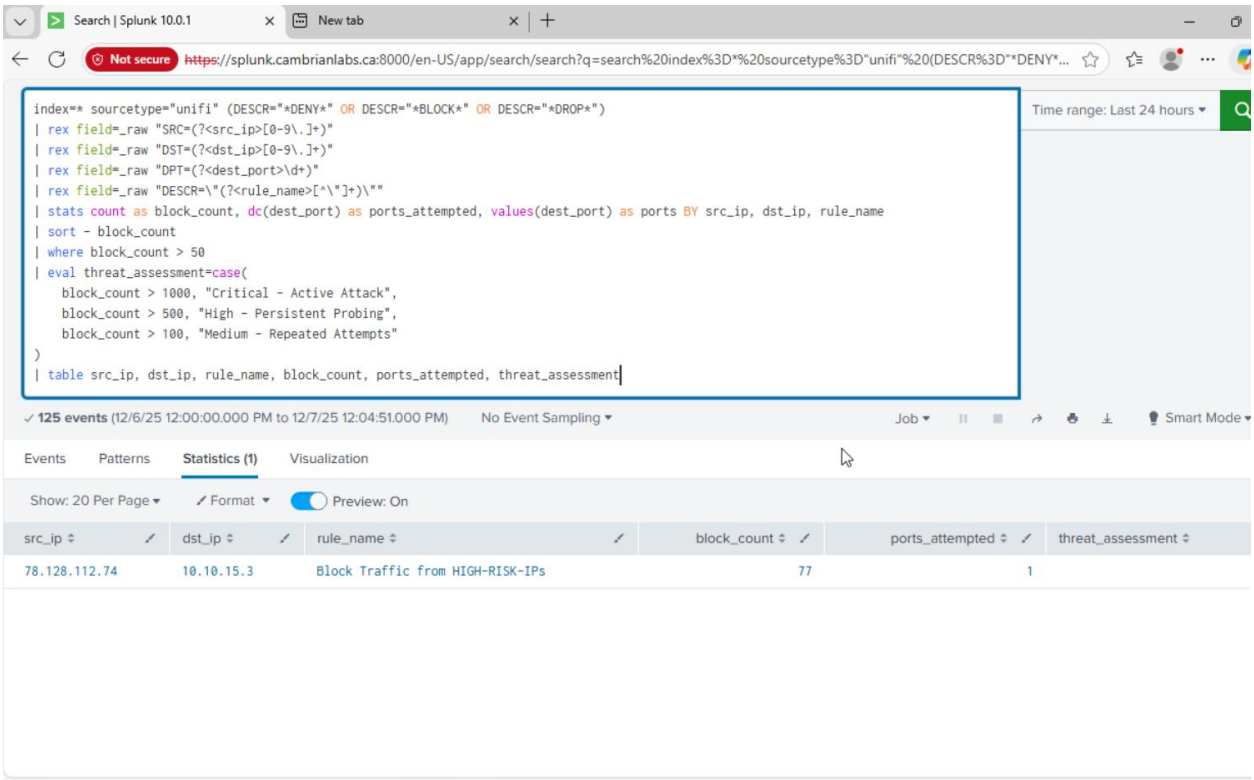
Analyzes traffic blocked by firewall rules to identify attack patterns. High block counts indicate persistent attack attempts





Query 6 ABNORMAL PROTOCOL USAGE

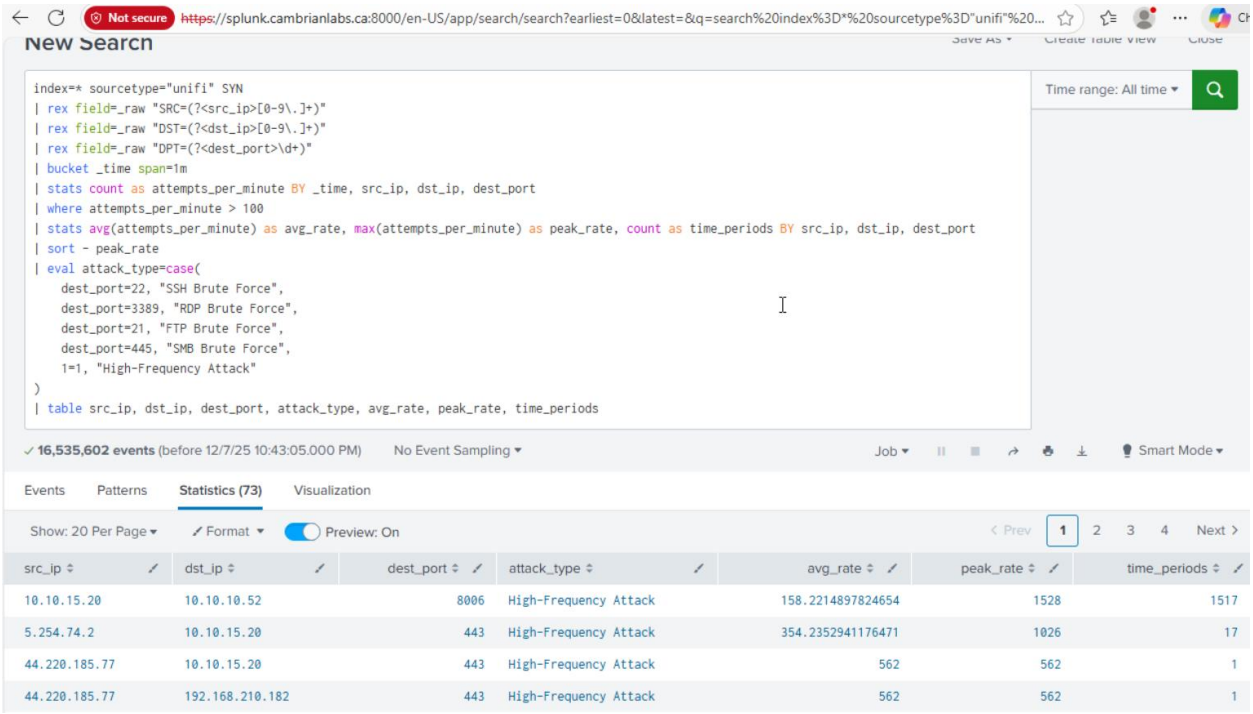
Detects use of protocols that shouldn't be present in normal traffic. Focus on GRE tunnels, unusual encapsulation that may hide malicious traffic

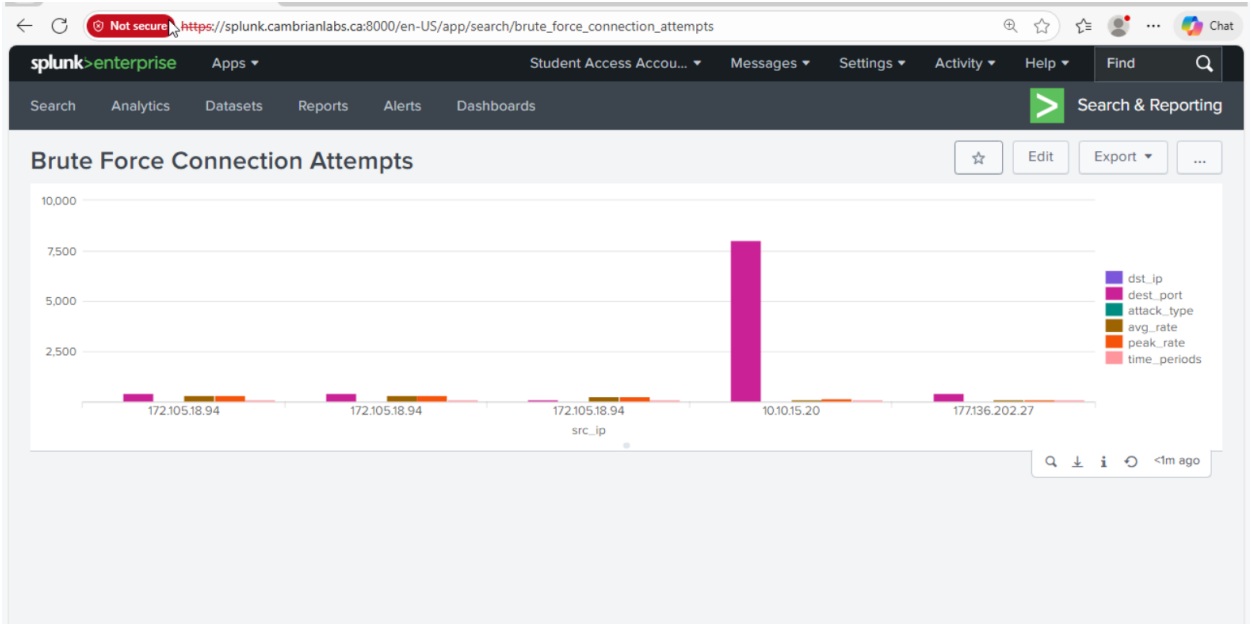


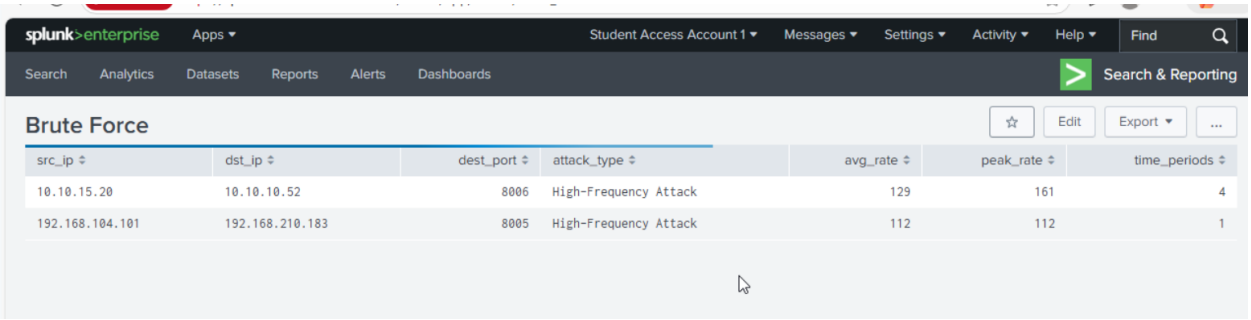
Query 7: BRUTE FORCE CONNECTION ATTEMPTS

Identifies sources making rapid repeated connection attempts

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



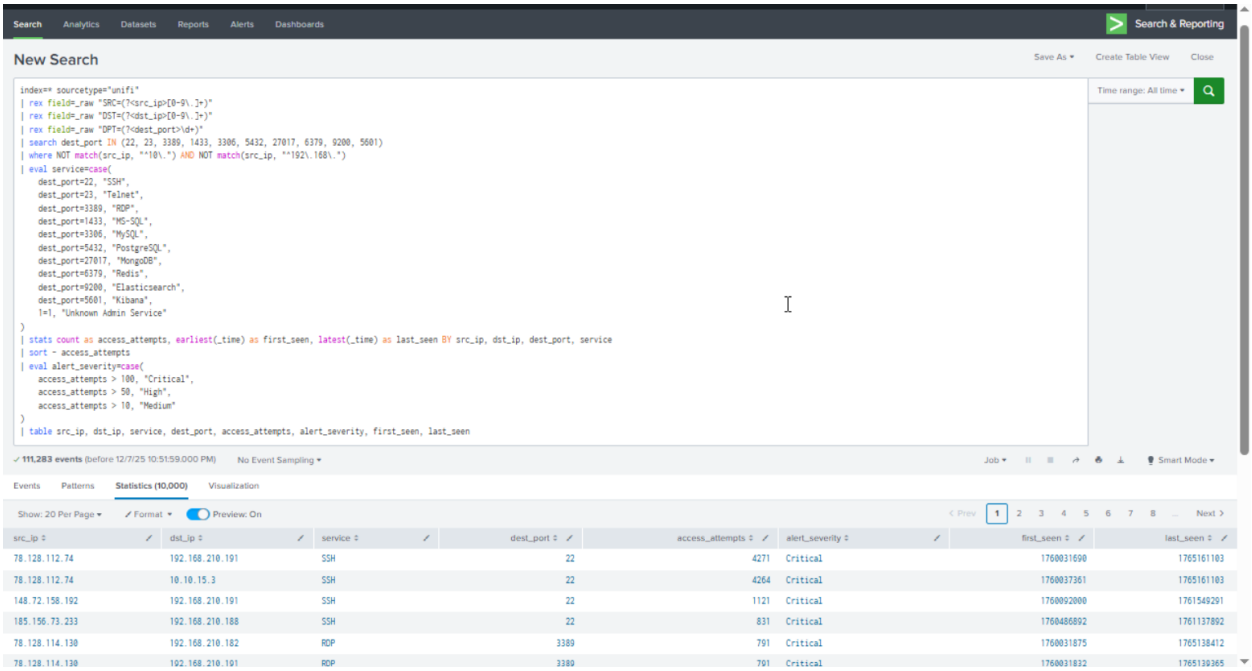




src_ip	dst_ip	dest_port	attack_type	avg_rate	peak_rate	time_periods
10.10.15.20	10.10.10.52	8006	High-Frequency Attack	129	161	4
192.168.104.101	192.168.210.183	8005	High-Frequency Attack	112	112	1

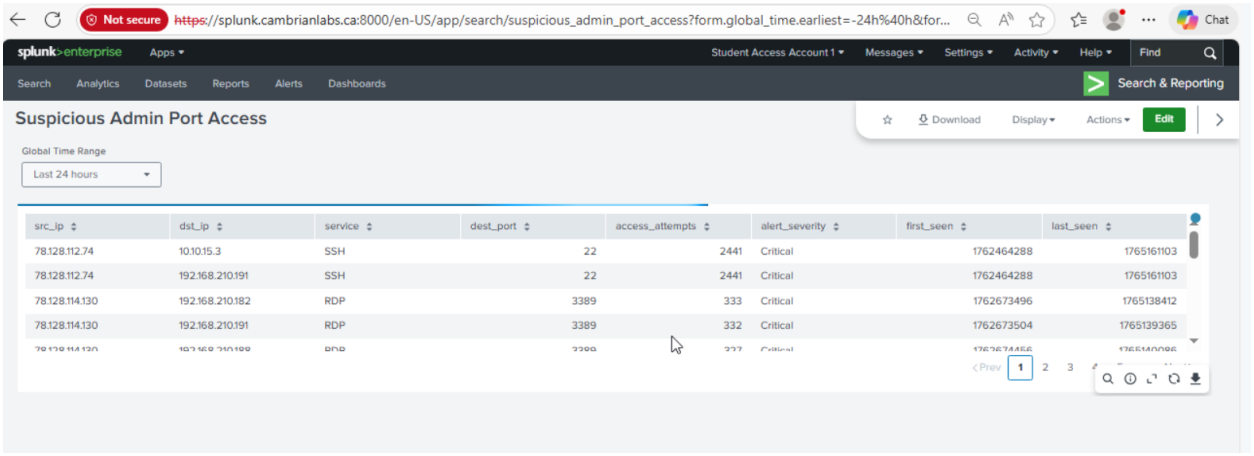
Query: 8. SUSPICIOUS ADMIN PORT ACCESS

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



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	1760031690	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	1761549291
185.156.73.233	192.168.210.188	SSH	22	831	Critical	1760486892	1761137892
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

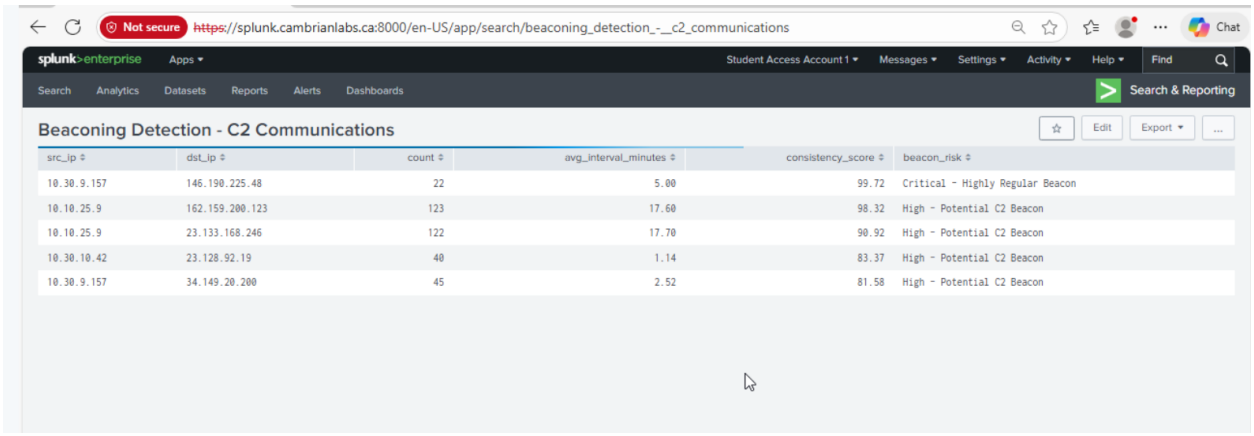
src_ip	dst_ip	service	dest_port	access_attempts	alert_severity	first_seen	last_seen
78.128.112.74	192.168.210.191	SSH	22	4271	Critical	1760031690	1765161103
78.128.112.74	10.10.15.3	SSH	22	4264	Critical	1760037361	1765161103
148.72.158.192	192.168.210.191	SSH	22	1121	Critical	1760092000	1761549291
185.156.73.233	192.168.210.188	SSH	22	831	Critical	1760486892	1761137892
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	1765140086
78.128.114.126	192.168.210.188	RDP	3389	577	Critical	1760031690	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	1760031690	1765114716
79.124.49.90	192.168.210.182	RDP	3389	507	Critical	1760034479	1763412222
79.124.49.90	192.168.210.191	RDP	3389	507	Critical	1760031690	1763409732
79.124.49.90	192.168.210.188	RDP	3389	504	Critical	1760034451	1763410216
161.35.152.142	192.168.210.188	SSH	22	345	Critical	1760443514	1760455802
194.0.234.19	192.168.210.188	SSH	22	308	Critical	1760486573	1761134257
146.190.225.91	192.168.210.188	SSH	22	295	Critical	1760443258	1760454208
194.180.48.63	192.168.210.182	SSH	22	262	Critical	1760051095	1765153757
194.180.48.63	192.168.210.188	SSH	22	262	Critical	1760051079	1765153771



Query 9: BEACONING DETECTION (C2 COMMUNICATION)

Identifies regular, periodic connections that may indicate malware beaconing

Looks for consistent time intervals between connections

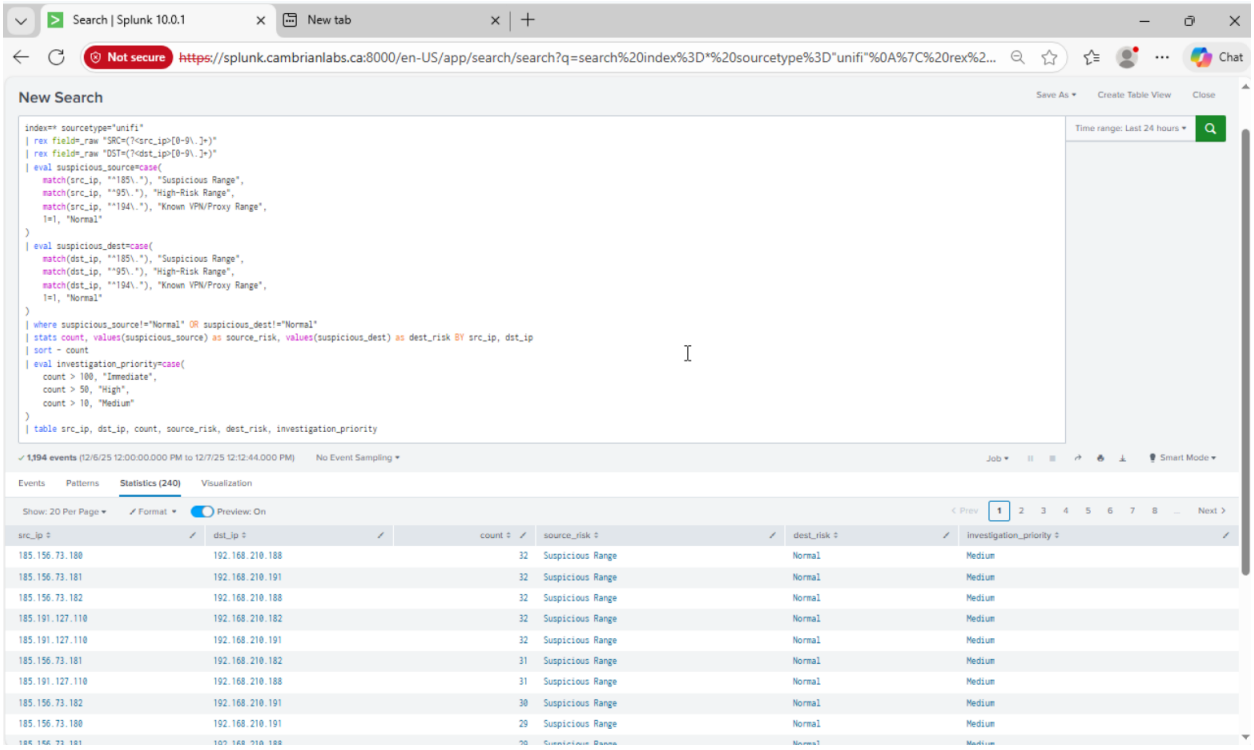


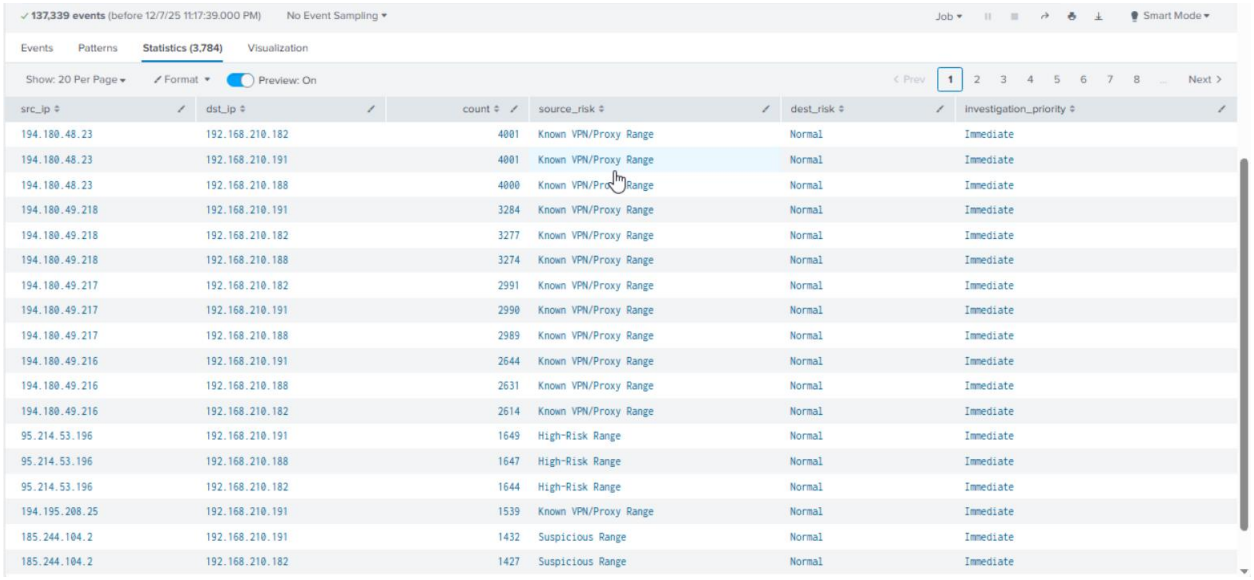
Query 10: GEOGRAPHIC ANOMALY DETECTION (CONNECTIONS TO SUSPICIOUS COUNTRIES)

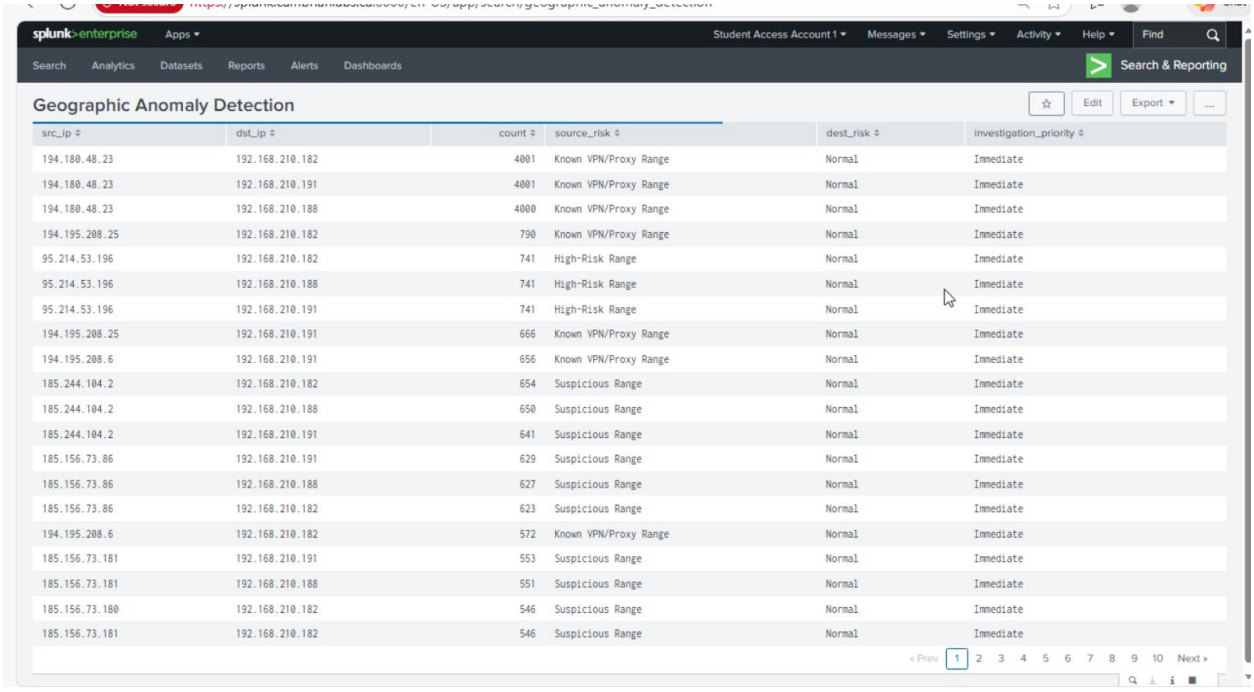
Identifies connections to/from high-risk geographic locations

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

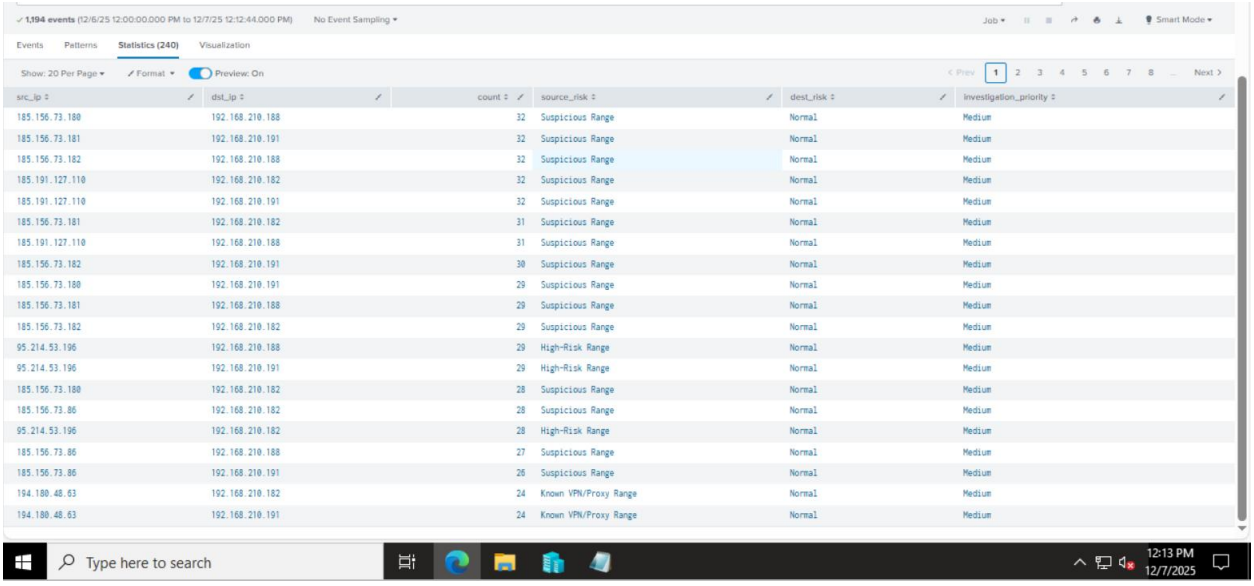
Alternative approach: Focus on known suspicious IP ranges


Search | Splunk 10.0.1
New tab
Not secure
https://splunk.cambrianlabs.ca:8000/en-US/app/search/search?q=search%20index%3D*%20sourcetype%3D"unifi"%0A%7C%20rex%2...
Chat
New Search
Save As
Create Table View
Close
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=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=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
Time range: Last 24 hours
1,194 events (12/6/25 12:00:00.000 PM to 12/7/25 12:12:44.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (240)
Visualization
Show: 20 Per Page
Format
Preview: On
Prev
1
2
3
4
5
6
7
8
Next
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

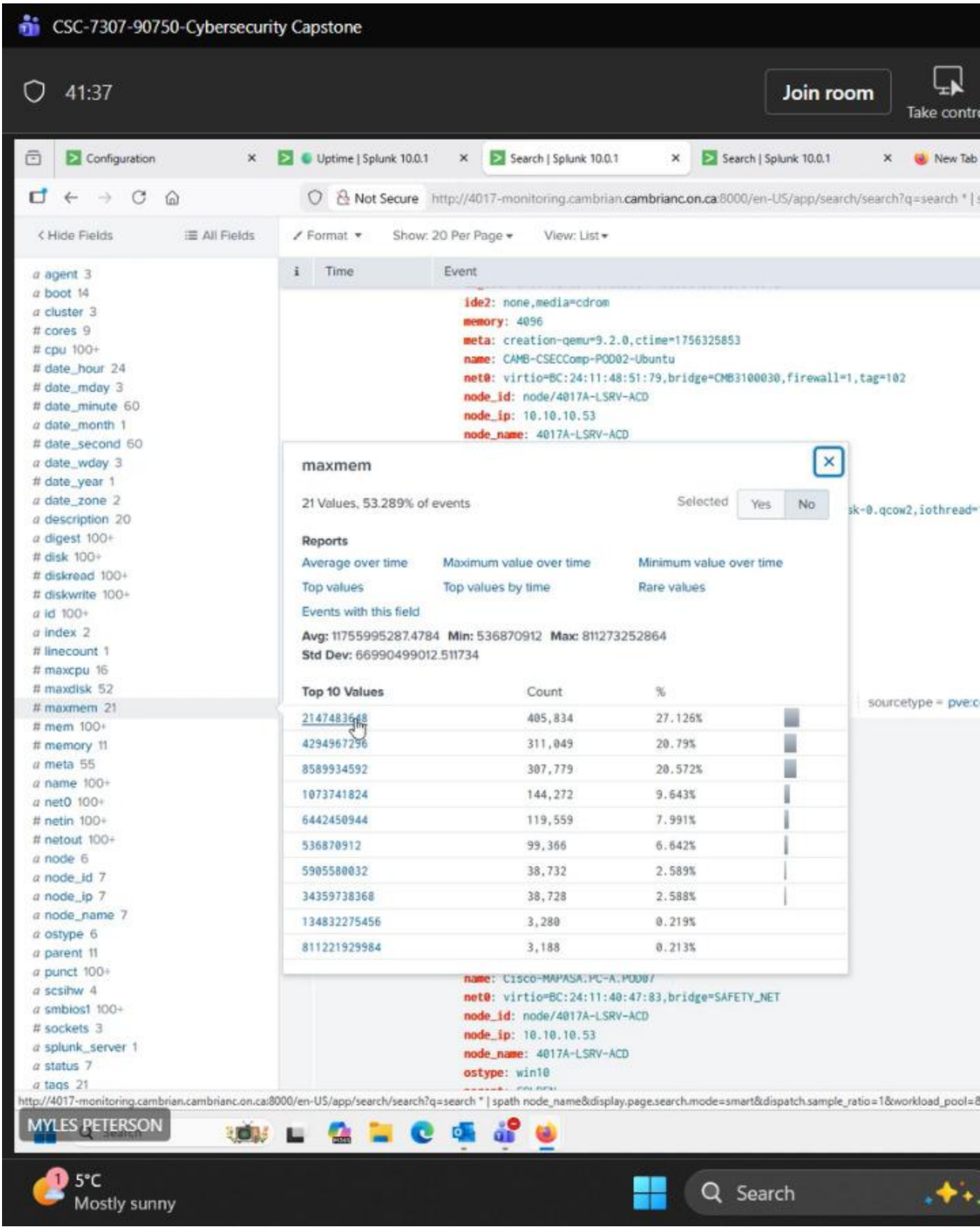

137,339 events (before 12/7/25 11:17:39.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (3,784)
Visualization
Show: 20 Per Page
Format
Preview: On
Prev
1
2
3
4
5
6
7
8
Next
src_ip
dst_ip
count
source_risk
dest_risk
investigation_priority
194.180.48.23 192.168.210.182 4001 Known VPN/Proxy 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

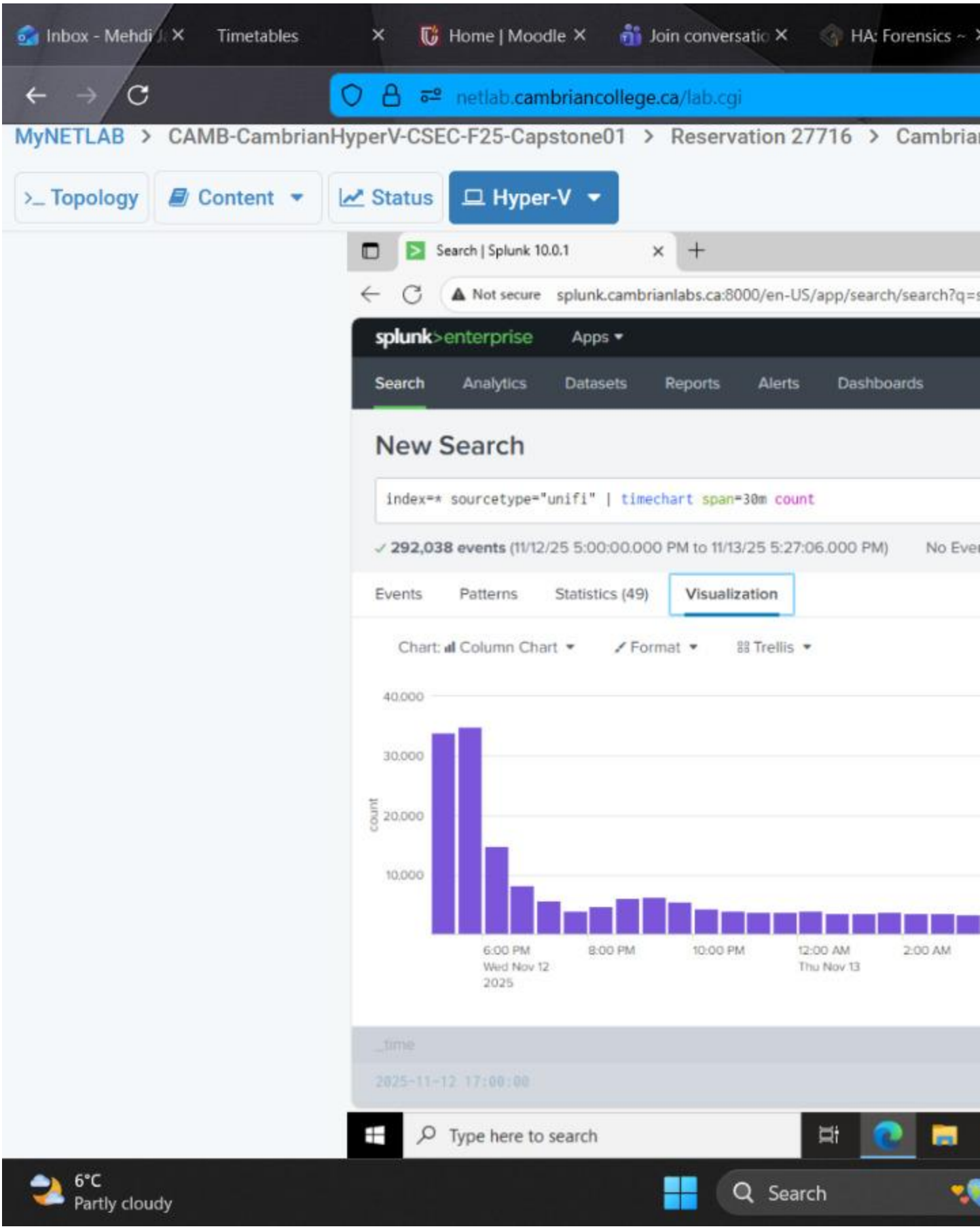


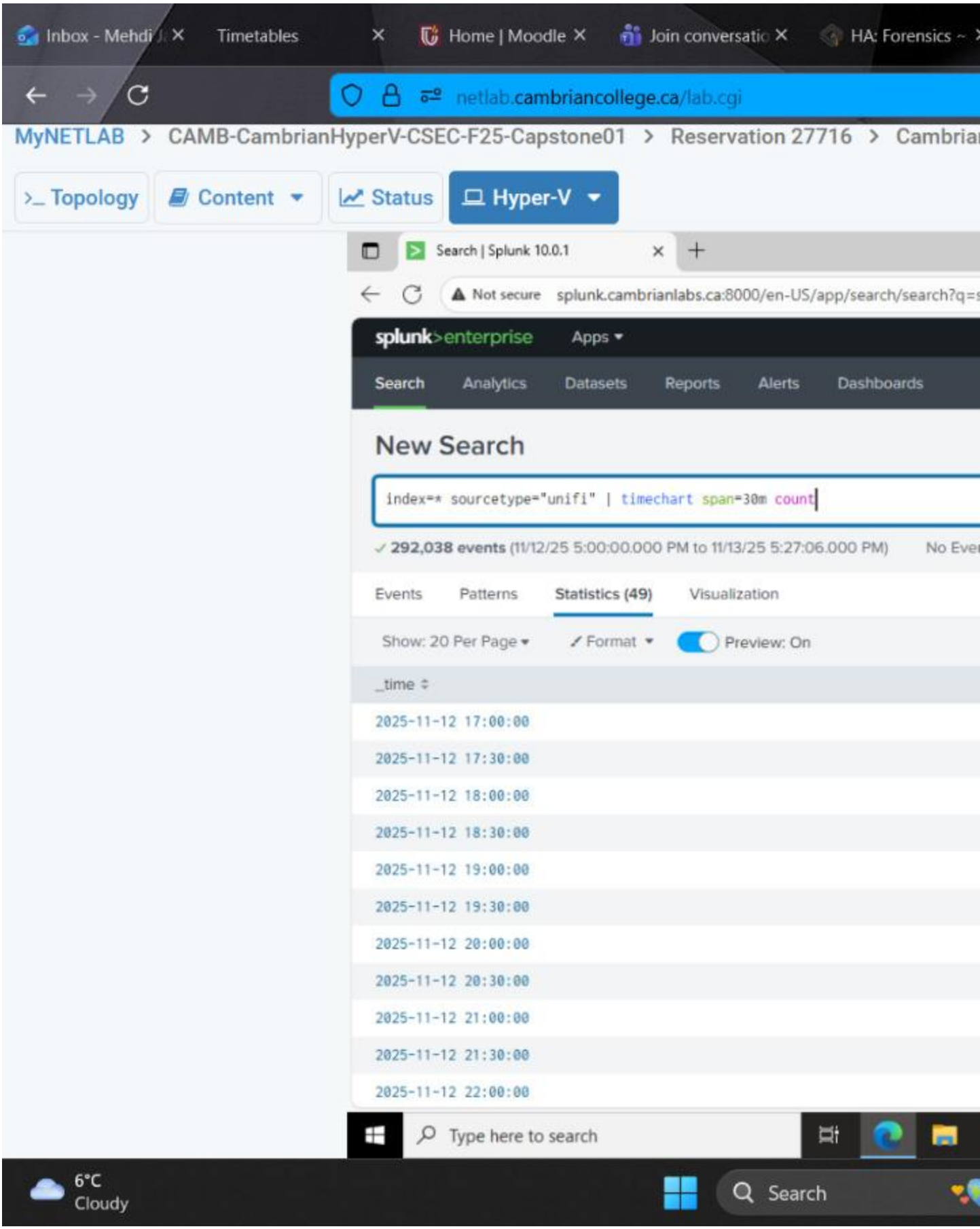
src_ip	dst_ip	count	source_risk	dest_risk	investigation_priority
194.180.48.23	192.168.210.182	4001	Known VPN/Proxy Range	Normal	Immediate
194.180.48.23	192.168.210.191	4001	Known VPN/Proxy Range	Normal	Immediate
194.180.48.23	192.168.210.188	4000	Known VPN/Proxy Range	Normal	Immediate
194.195.208.25	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

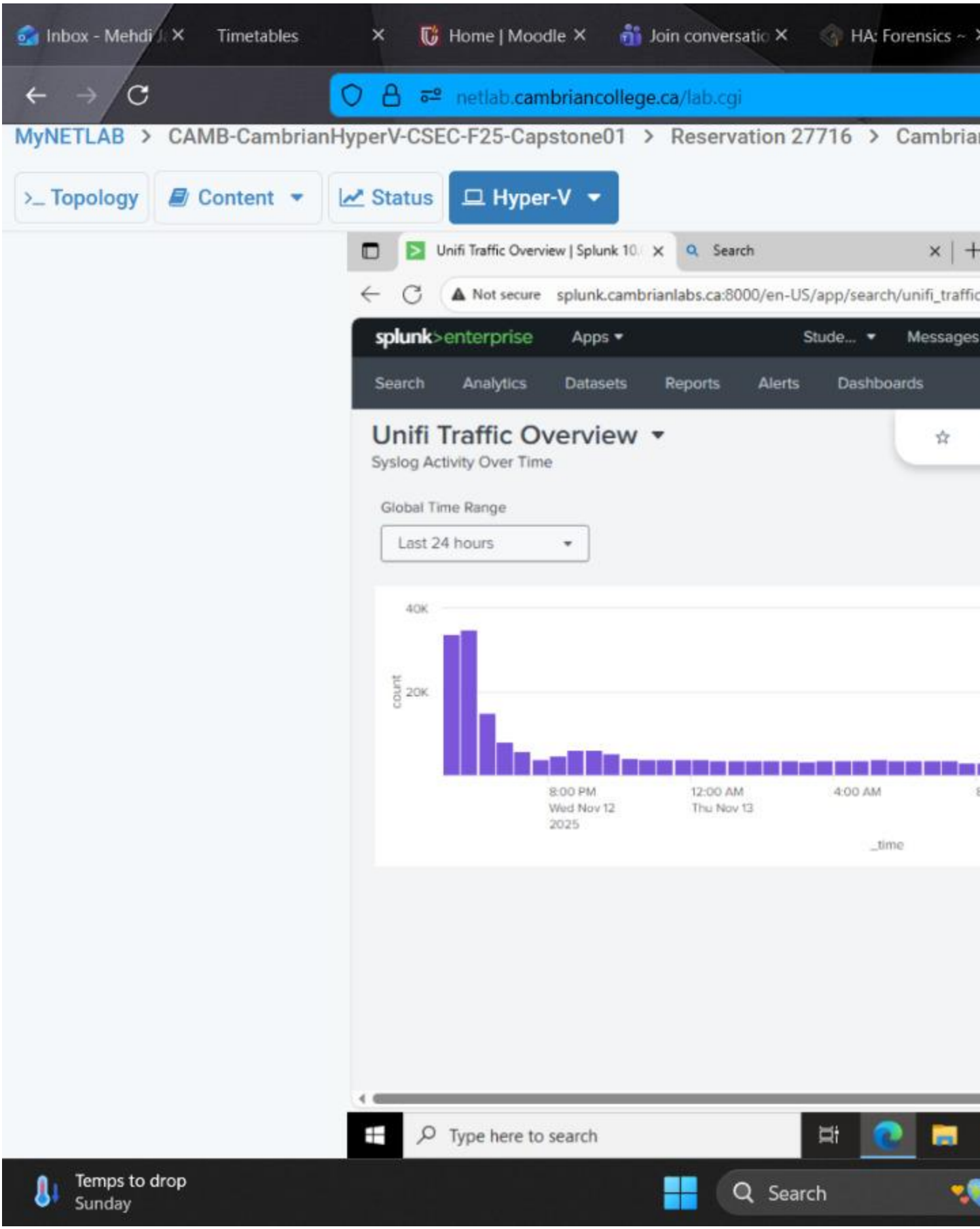


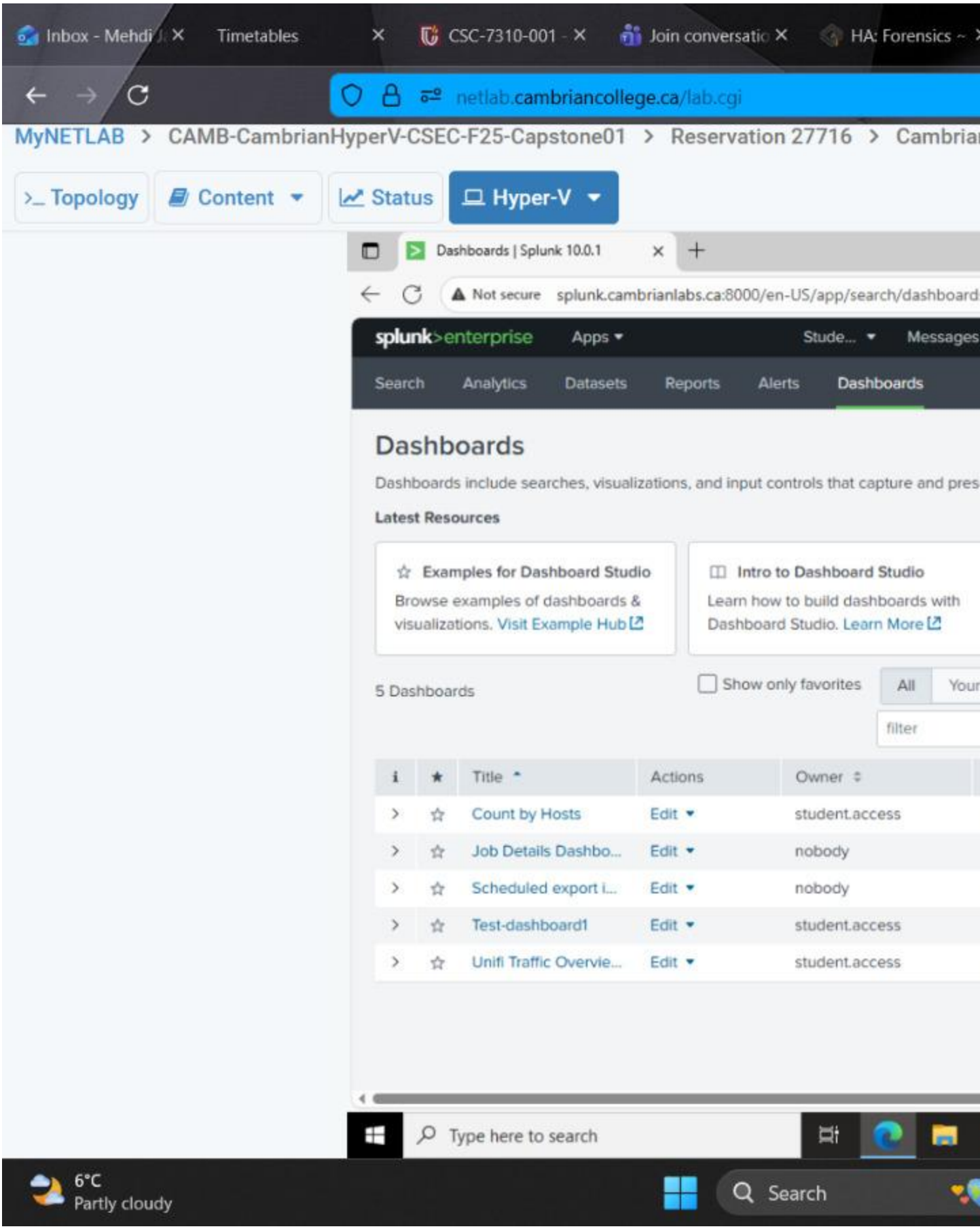
src_ip	dst_ip	count	source_risk	dest_risk	investigation_priority
185.156.73.180	192.168.210.188	32	Suspicious Range	Normal	Medium
185.156.73.181	192.168.210.191	32	Suspicious Range	Normal	Medium
185.156.73.182	192.168.210.188	32	Suspicious Range	Normal	Medium
185.191.127.110	192.168.210.182	32	Suspicious 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	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
185.156.73.180	192.168.210.182	28	Suspicious Range	Normal	Medium
185.156.73.86	192.168.210.182	28	Suspicious Range	Normal	Medium
95.214.53.196	192.168.210.182	28	High-Risk Range	Normal	Medium
185.156.73.86	192.168.210.188	27	Suspicious Range	Normal	Medium
185.156.73.86	192.168.210.191	26	Suspicious 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

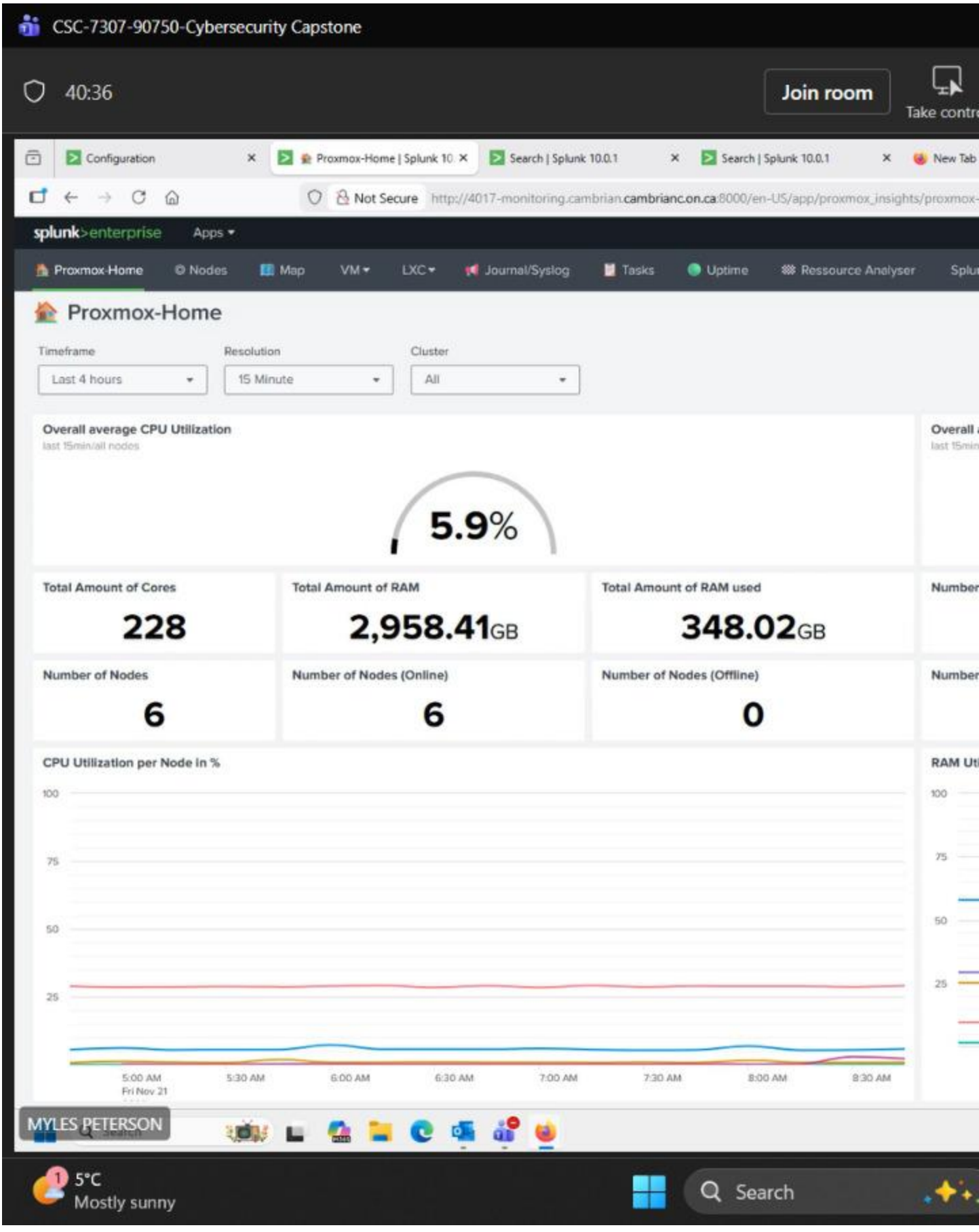

CSC-7307-90750-Cybersecurity Capstone
41:37
Join room
Take contr
Configuration
Uptime | Splunk 10.0.1
Search | Splunk 10.0.1
Search | Splunk 10.0.1
New Tab
Not Secure
http://4017-monitoring.cambrian.cambrianc.on.ca:8000/en-US/app/search/search?q=search * |
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Time
Event
a agent 3
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
ide2: none,media=cdrom
memory: 4096
meta: creation-qemu=9.2.0,ctime=1756325853
name: CAMB-CSECComp-POD02-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
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%
5905580032 38,732 2.589%
34359738368 38,728 2.588%
134832275456 3,280 0.219%
811221929984 3,188 0.213%
sourcetype = pve:c
name: Cisco-MAPASA-PC-A-POD07
net0: virtio=BC:24:11:40:47:83,bridge=SAFETY_NET
node_id: node/4017A-LSRV-ACD
node_ip: 10.10.10.53
node_name: 4017A-LSRV-ACD
ostype: win10
http://4017-monitoring.cambrian.cambrianc.on.ca:8000/en-US/app/search/search?q=search * | spath node_name&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=
MYLES PETERSON
5°C
Mostly sunny
Search

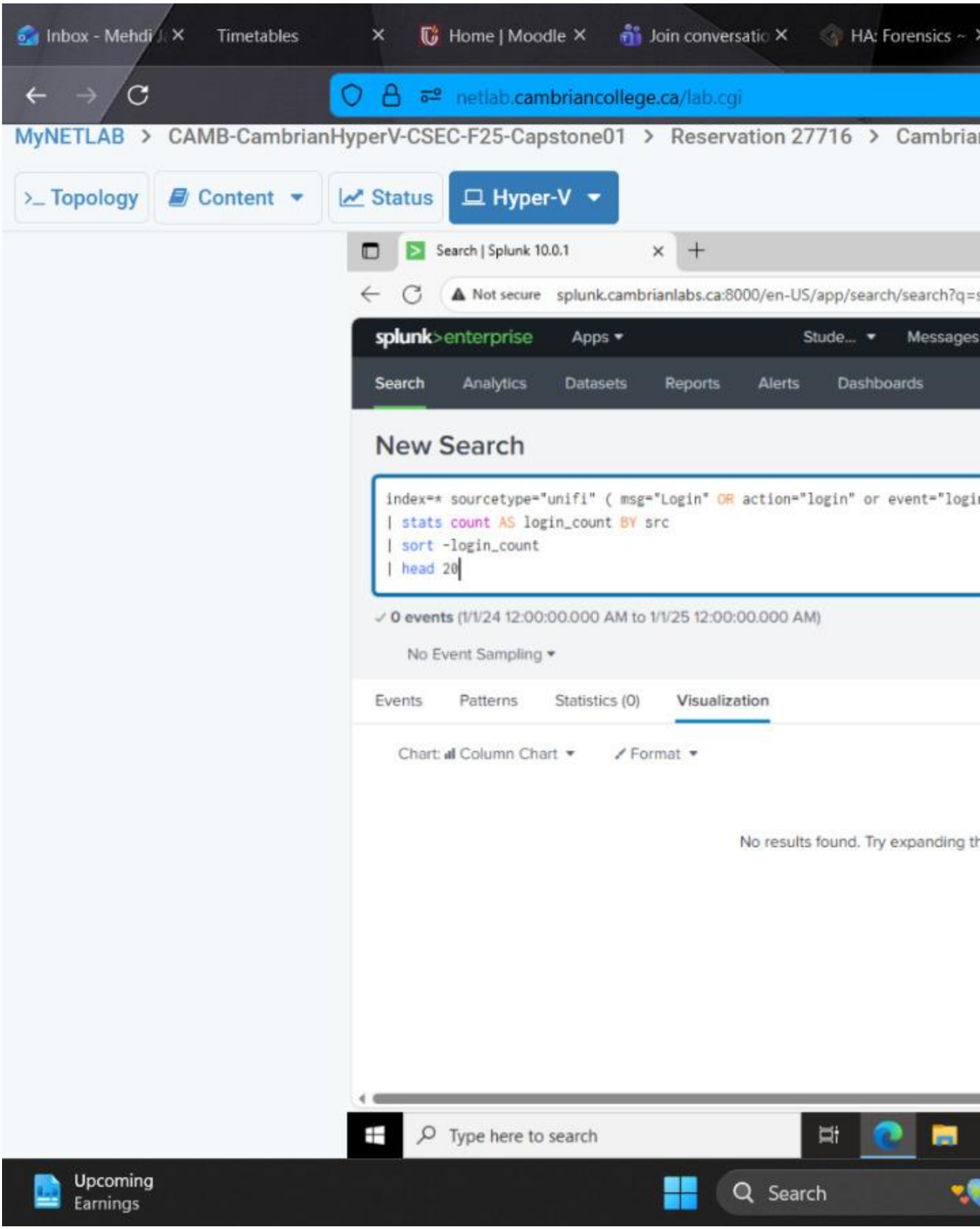

Inbox - Mehdi
Timetables
Home | Moodle
Join conversatio
HA: Forensics
netlab.cambriancollege.ca/lab.cgi
MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambria
Topology
Content
Status
Hyper-V
Search | Splunk 10.0.1
Not secure
splunk.cambrianlabs.ca:8000/en-US/app/search/search?q=
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 Eve
Events
Patterns
Statistics (49)
Visualization
Chart: Column Chart
Format
Trellis
40.000
30.000
20.000
10.000
count
6:00 PM
Wed Nov 12
2025
8:00 PM
10:00 PM
12:00 AM
Thu Nov 13
2:00 AM
_time
2025-11-12 17:00:00
Type here to search
6°C
Partly cloudy
Search

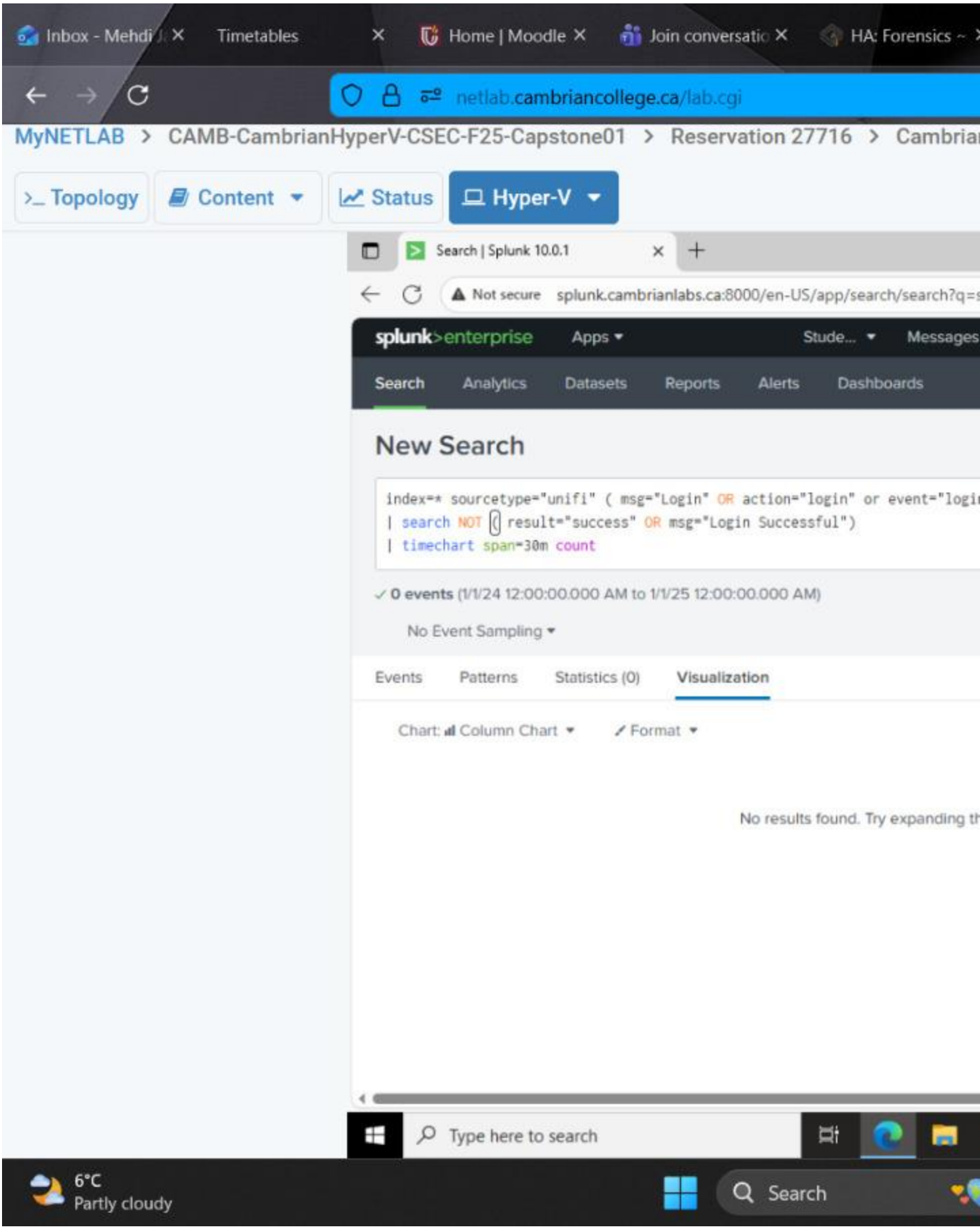

Inbox - Mehdi
Timetables
Home | Moodle
Join conversatio
HA: Forensics
netlab.cambriancollege.ca/lab.cgi
MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambria
Topology
Content
Status
Hyper-V
Search | Splunk 10.0.1
Not secure
splunk.cambrianlabs.ca:8000/en-US/app/search/search?q=
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 Eve
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
Type here to search
6°C
Cloudy
Search

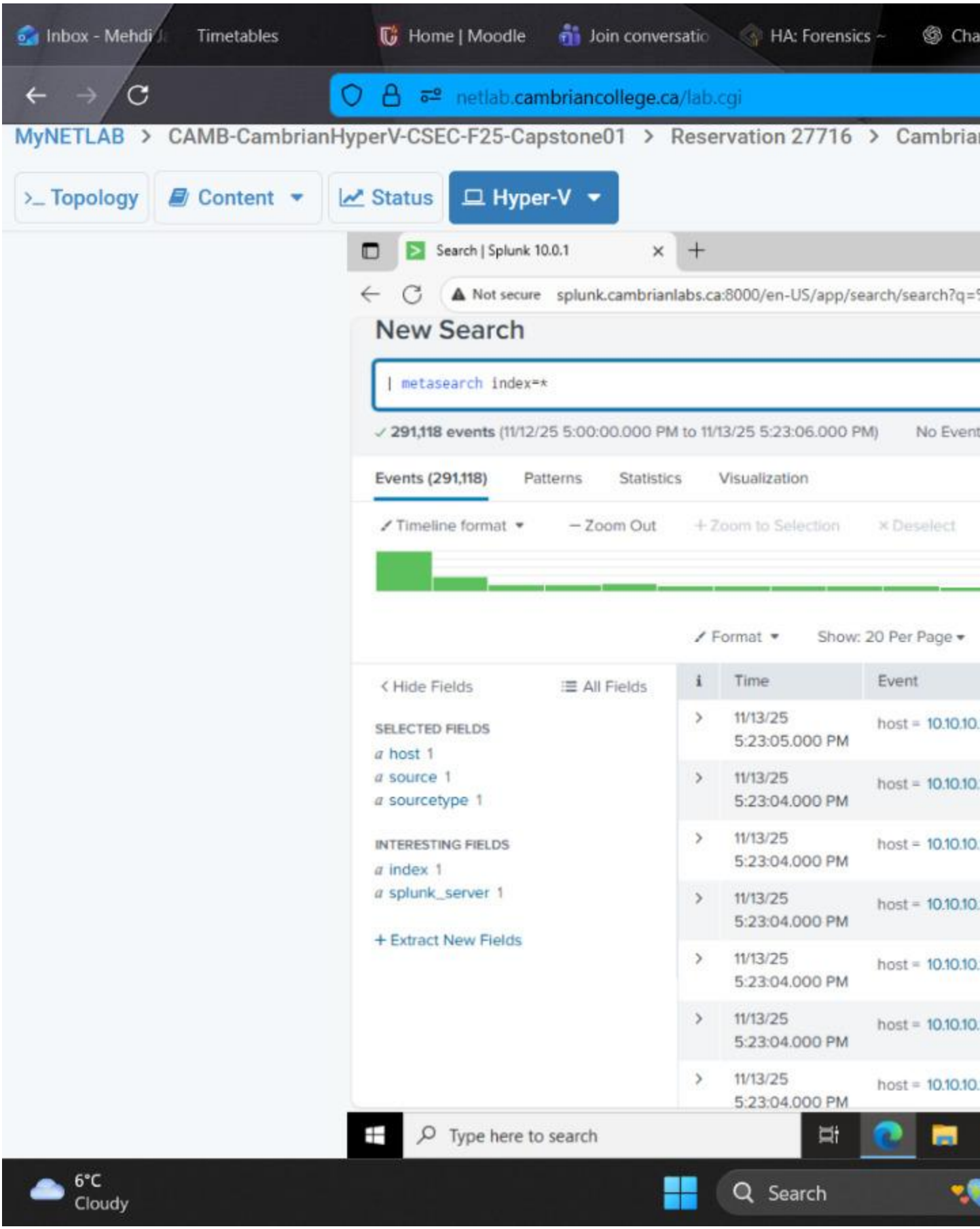

Inbox - Mehdi
Timetables
Home | Moodle
Join conversatio
HA: Forensics
netlab.cambriancollege.ca/lab.cgi
MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambria
Topology
Content
Status
Hyper-V
Unifi Traffic Overview | Splunk 10
Search
Not secure
splunk.cambrianlabs.ca:8000/en-US/app/search/unifi_traffic
splunk>enterprise
Apps
Stude...
Messages
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Unifi Traffic Overview
Syslog Activity Over Time
Global Time Range
Last 24 hours
40K
20K
count
8:00 PM
Wed Nov 12
2025
12:00 AM
Thu Nov 13
4:00 AM
_time
Type here to search
Temps to drop
Sunday
Search

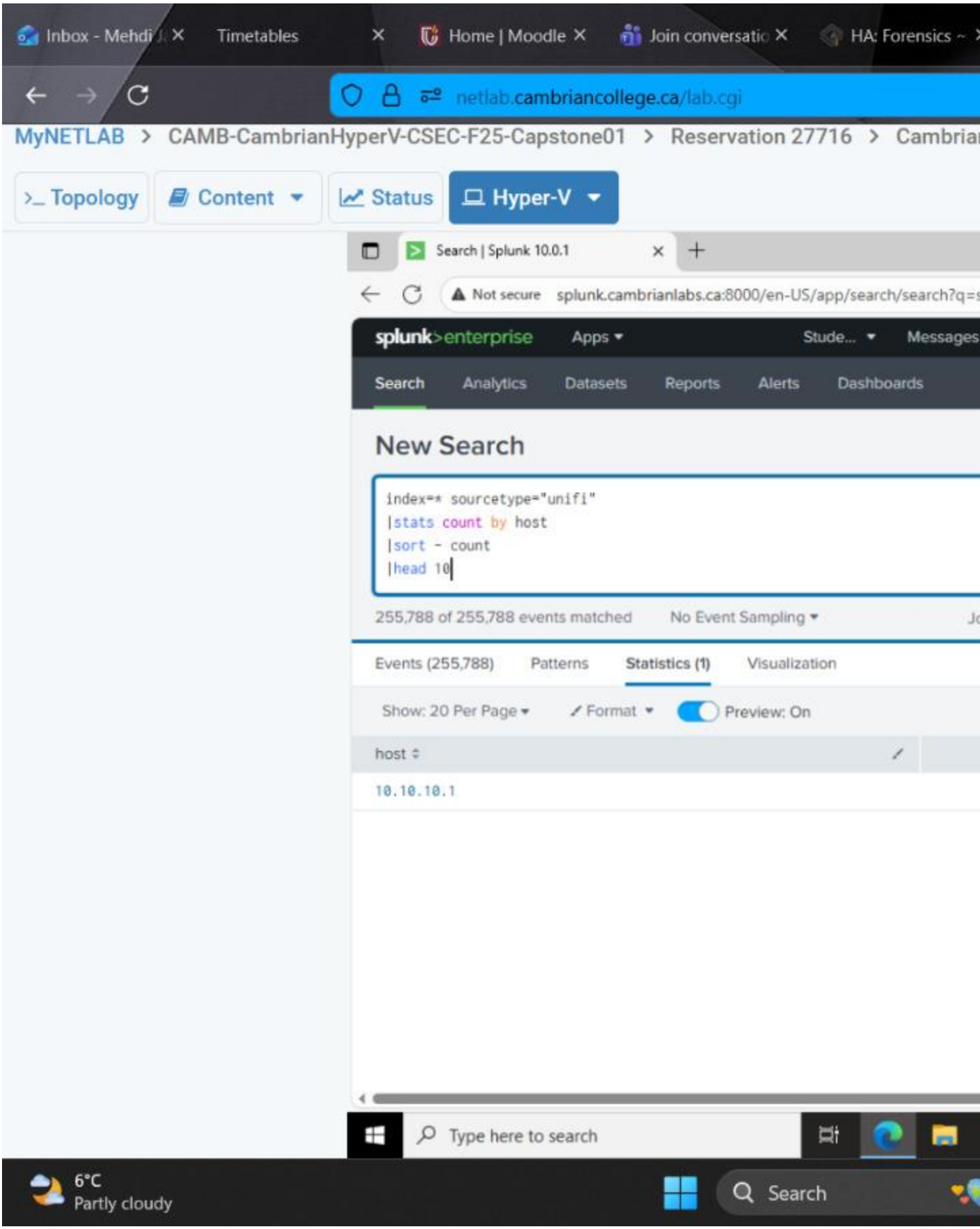

Inbox - Mehdi
Timetables
CSC-7310-001
Join conversatio
HA: Forensics
netlab.cambriancollege.ca/lab.cgi
MyNETLAB > CAMB-CambrianHyperV-CSEC-F25-Capstone01 > Reservation 27716 > Cambria
Topology
Content
Status
Hyper-V
Dashboards | Splunk 10.0.1
Not secure
splunk.cambrianlabs.ca:8000/en-US/app/search/dashboard
splunk>enterprise
Apps
Stude...
Messages
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Dashboards
Dashboards include searches, visualizations, and input controls that capture and pres
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
filter
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
Type here to search
6°C
Partly cloudy
Search


CSC-7307-90750-Cybersecurity Capstone
40:36
Join room
Take contr
Configuration
Proxmox-Home | Splunk 10
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
LXC
Journal/Syslog
Tasks
Uptime
Ressource Analyser
Proxmox-Home
Timeframe
Last 4 hours
Resolution
15 Minute
Cluster
All
Overall average CPU Utilization
last 15min/all nodes
5.9%
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
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
Timetables
Home | Moodle
Join conversatio
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.cambrianlabs.ca:8000/en-US/app/search/search?q=
splunk>enterprise
Apps
Stude...
Messages
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=* sourcetype="unifi" (msg="Login" OR action="login" or event="logi
| 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: Column Chart
Format
No results found. Try expanding th
Type here to search
Upcoming
Earnings
Search


Inbox - Mehdi
Timetables
Home | Moodle
Join conversatio
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.cambrianlabs.ca:8000/en-US/app/search/search?q=
splunk>enterprise
Apps
Stude...
Messages
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=* sourcetype="unifi" (msg="Login" OR action="login" or event="logi
| search NOT (result="success" OR msg="Login Successful")
| timechart span=30m count
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: Column Chart
Format
No results found. Try expanding th
Type here to search
6°C
Partly cloudy
Search


Inbox - Mehdi
Timetables
Home | Moodle
Join conversatio
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.cambrianlabs.ca:8000/en-US/app/search/search?q=
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
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a index 1
a splunk_server 1
+ Extract New Fields
Time
Event
11/13/25 5:23:05.000 PM
11/13/25 5:23:04.000 PM
host = 10.10.10.
Type here to search
6°C
Cloudy
Search


Inbox - Mehdi
Timetables
Home | Moodle
Join conversatio
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.cambrianlabs.ca:8000/en-US/app/search/search?q=
splunk>enterprise
Apps
Stude...
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
Search

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.