TROLL TRACE

Agenda

1. Meet The Team
2. Challenge Overview
3. Objectives & Actions
4. Splunk Alert Queries
5. Follow The Trail
6. Q&A

Omar Ardid

- Cybersecurity Professional
- Enjoy building gaming computers and playing video games
- Passionate on helping others

TROLL TRACE

Gilbert Collado

- Cybersecurity Professional

- 9 Year Navy Veteran

- Proficient in Building PC Systems, Soldering Components & Troubleshooting

Steve Cherewaty

- Cybersecurity professional

- Background in aerospace and startups

- Passion for building

Challenge Overview

- Suffered a data breach earlier this year
- Requested a threat emulation exercise

- Evaluate SimCorp's VPC network
- Hunt threats during adversarial action

Objectives & Actions

Objectives:	***Actions:***
Observe adversarial actions and collect evidence on movement and actions	*Implement network monitoring tools*

Objectives & Actions

Objectives:	Actions:
Observe adversarial actions and collect evidence on movement and actions	Design/configure network monitoring tools
Discover gaps & vulnerabilities in the current architecture	Monitor real-time events and sort through logs using Splunk, Nmap NES and AWS resources

TROLL TRACE

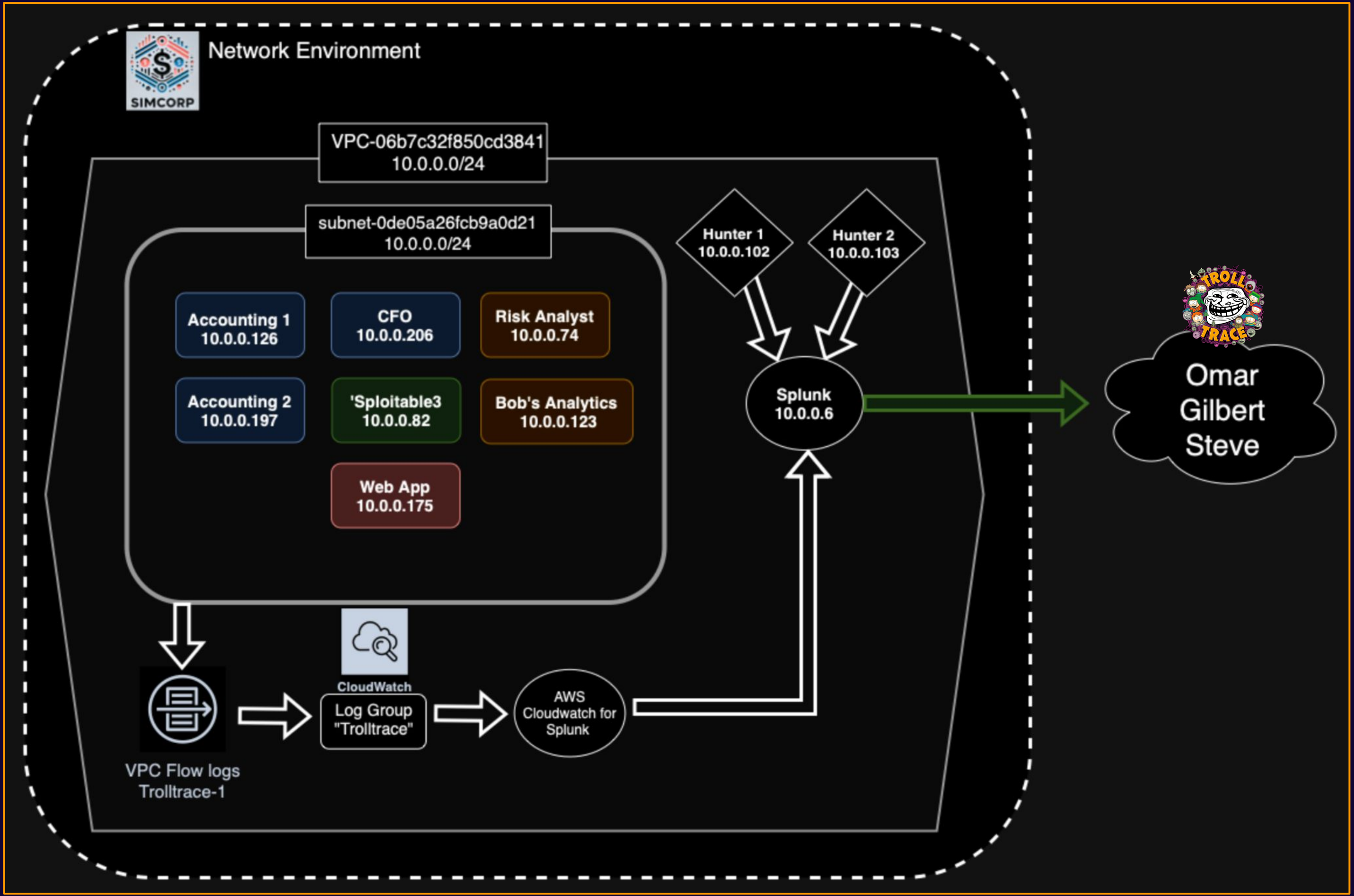
Objectives & Actions

Objectives:	Actions:
Observe adversarial actions and collect evidence on movement and actions	Design/configure network monitoring tools
Discover gaps & vulnerabilities in the current architecture	Monitor real-time events and sort through logs using Splunk, Nmap NES and AWS resources
Introduce automated components to enable more efficient monitoring/responses	Configure IDS rules for greater detection capabilities

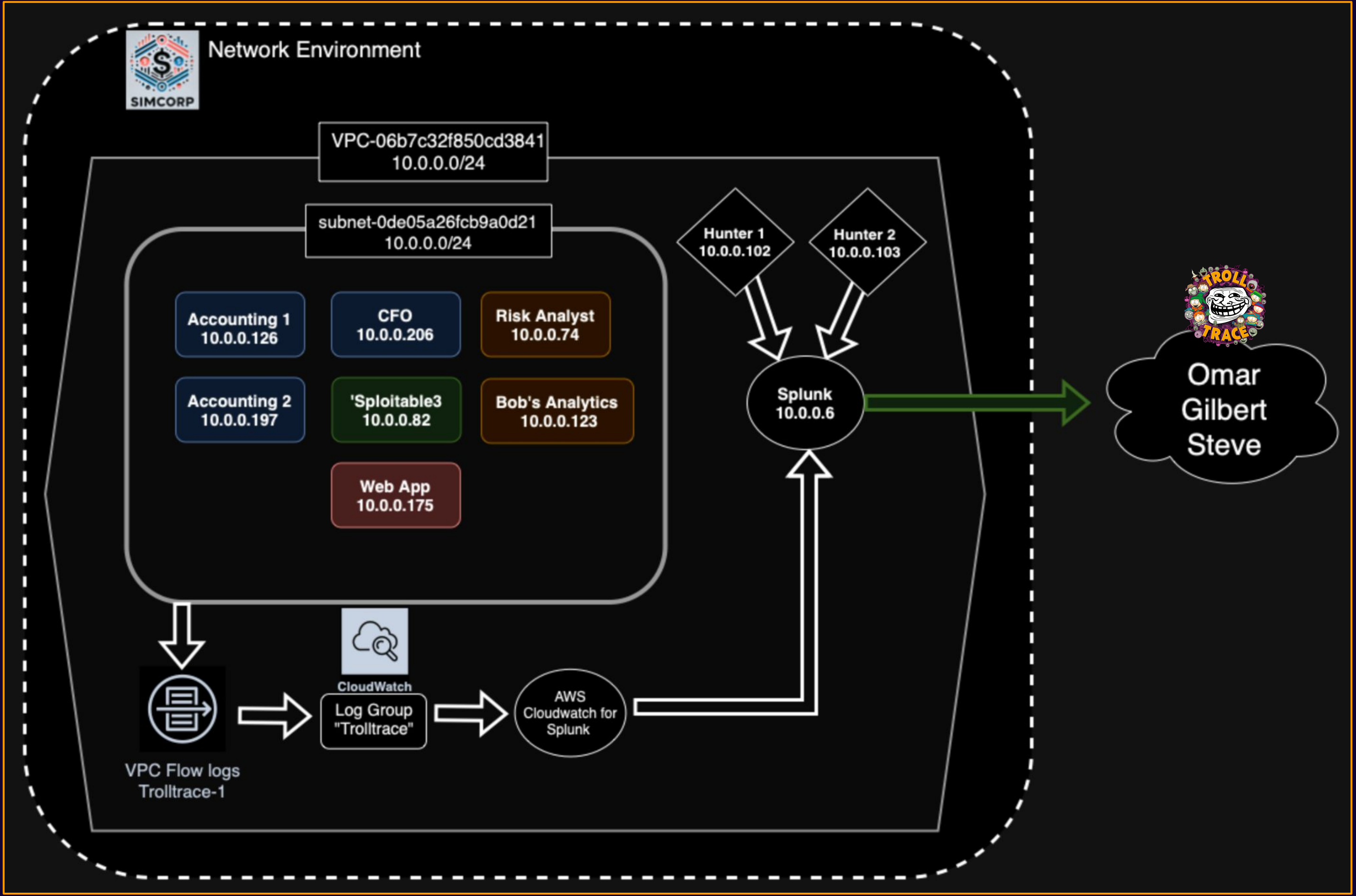
Objectives & Actions

Objectives:	Actions:
Observe adversarial actions and collect evidence on movement and actions	Design/configure network monitoring tools
Discover gaps & vulnerabilities in the current architecture	Monitor real-time events and sort through logs using Splunk, Nmap NES and AWS resources
Introduce automated components to enable more efficient monitoring/responses	Configure IDS rules for greater detection capabilities
Compile a report on the findings of the exercise	Perform a STRIDE analysis

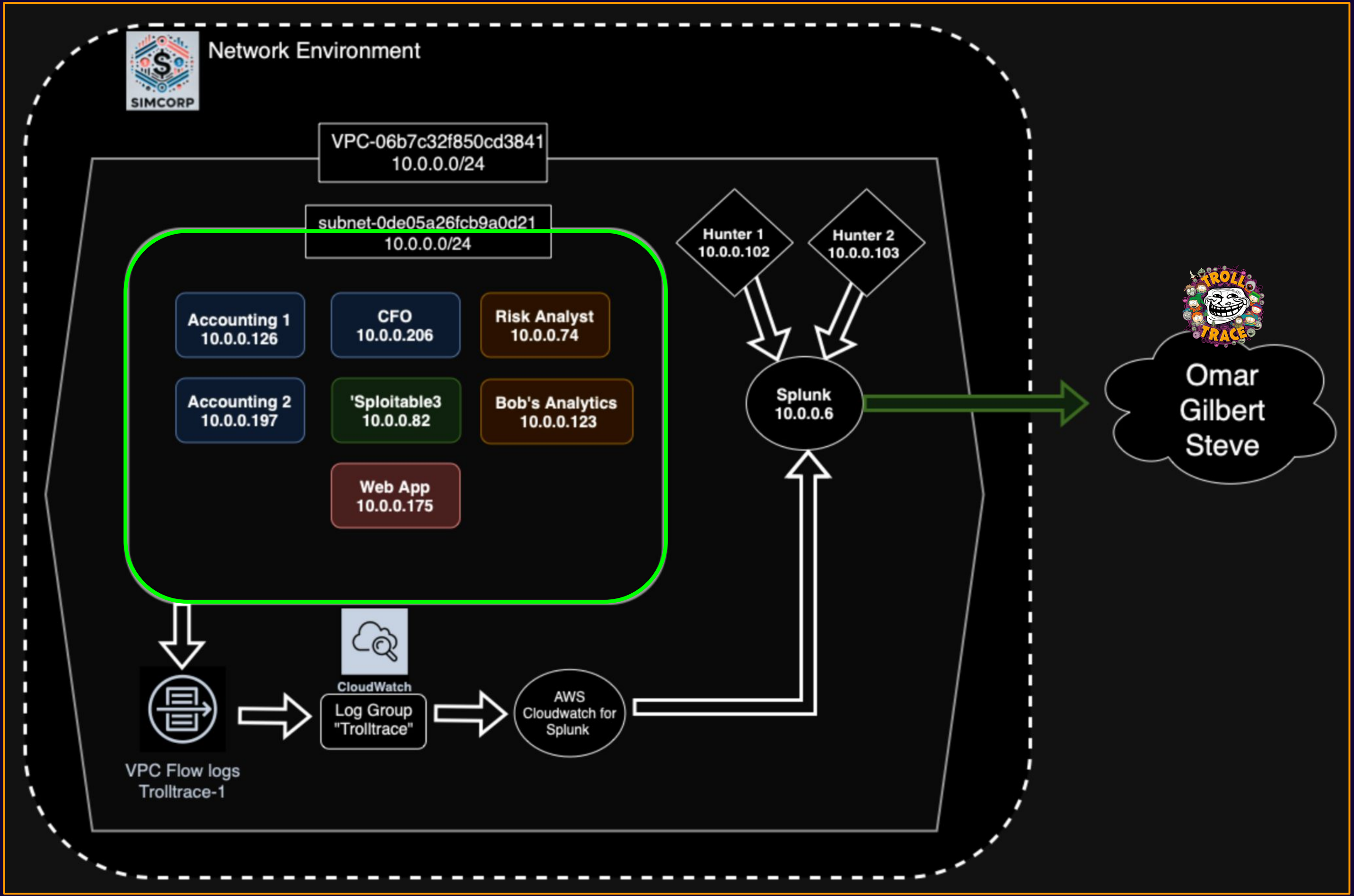
SimCorp Network Topology



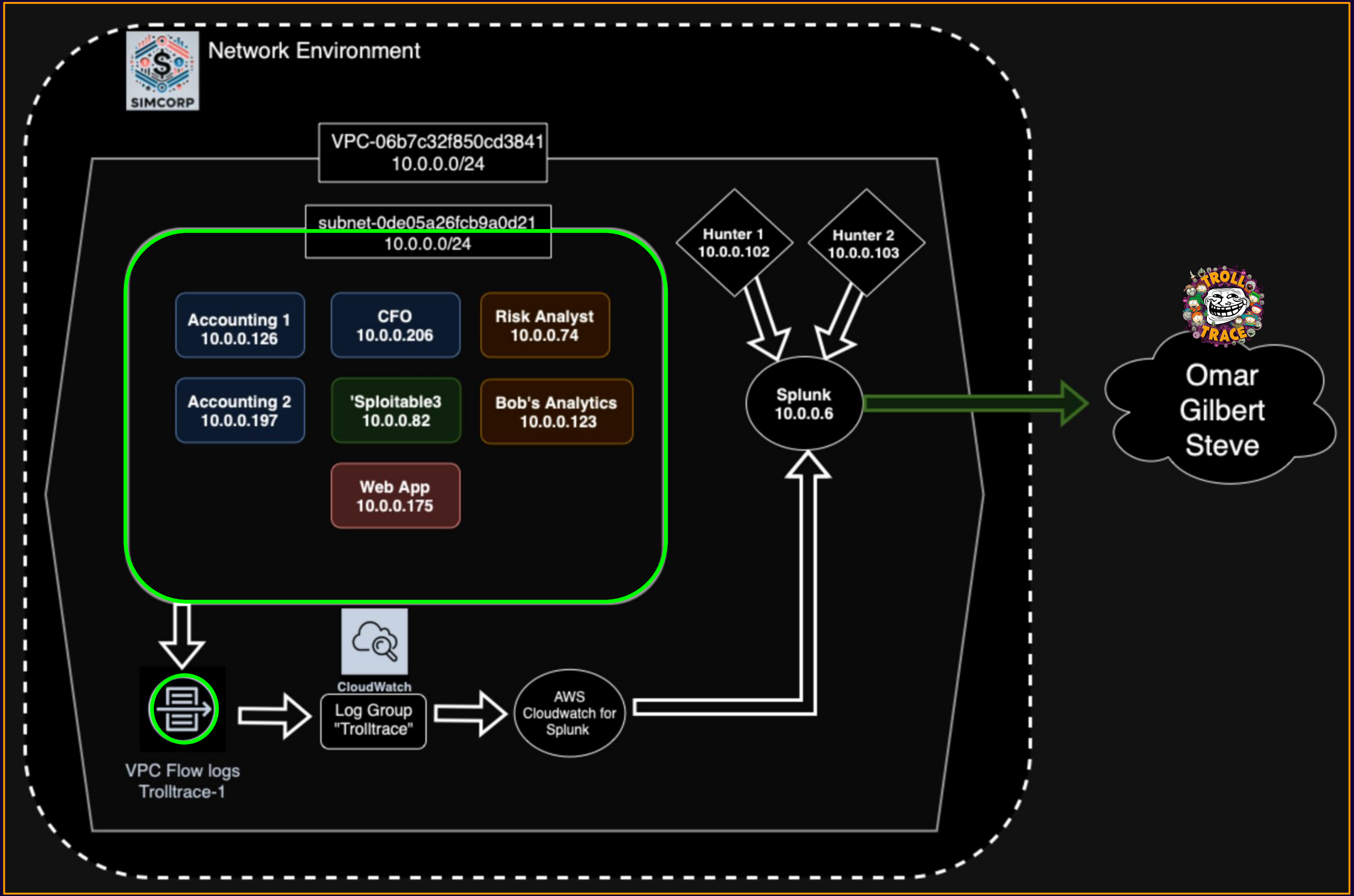
SimCorp Network Topology



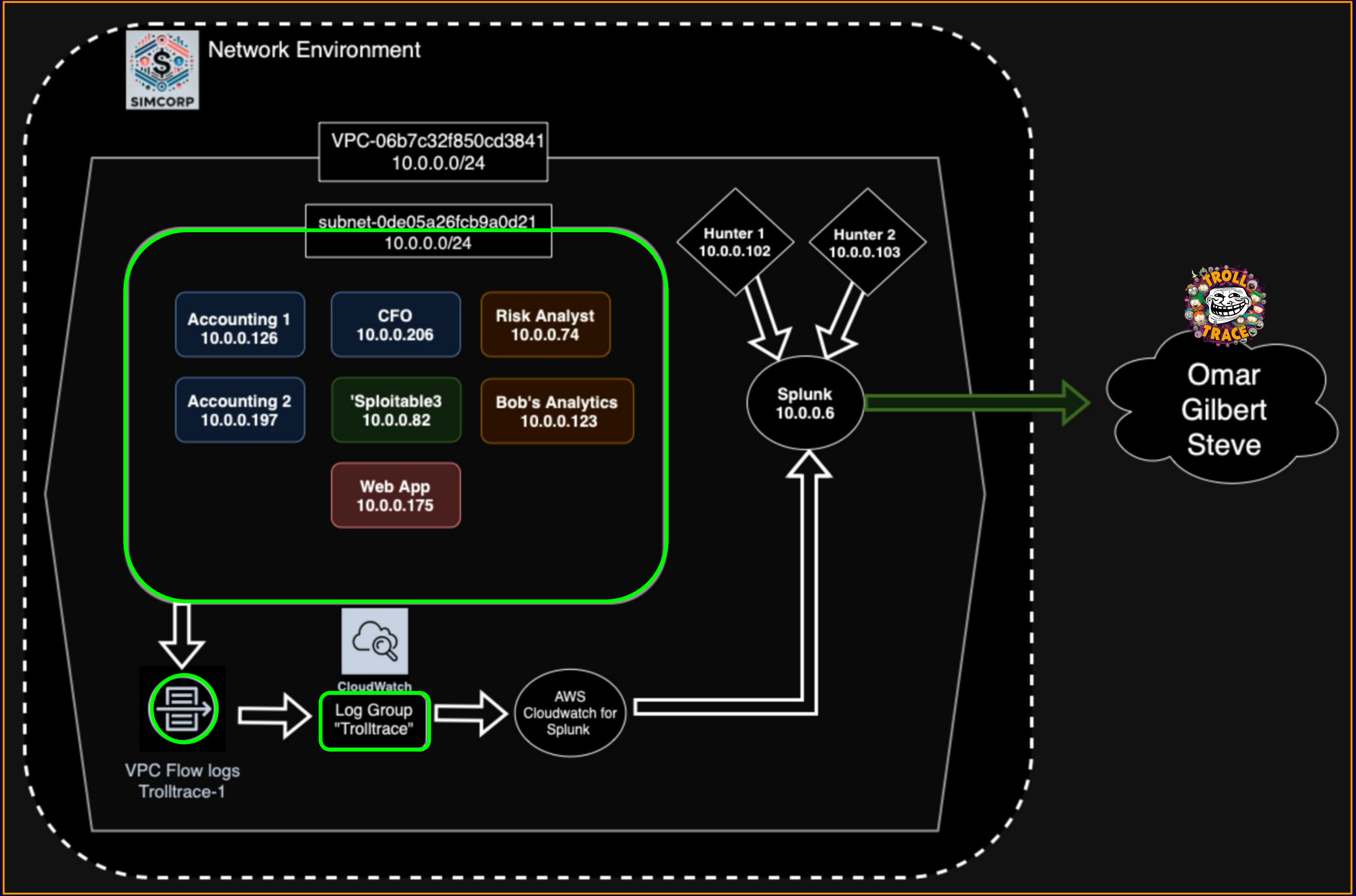
SimCorp Network Topology



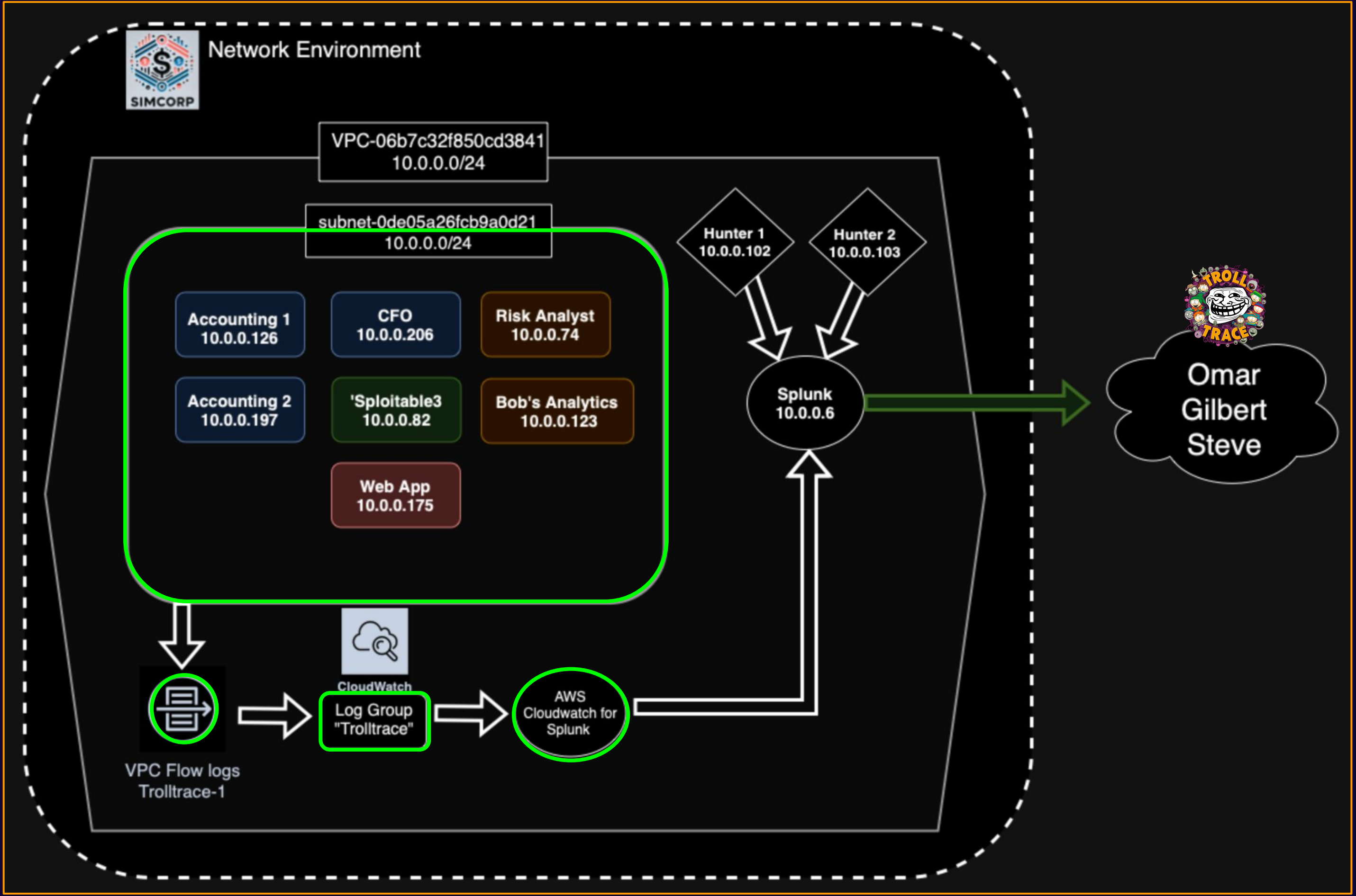
SimCorp Network Topology



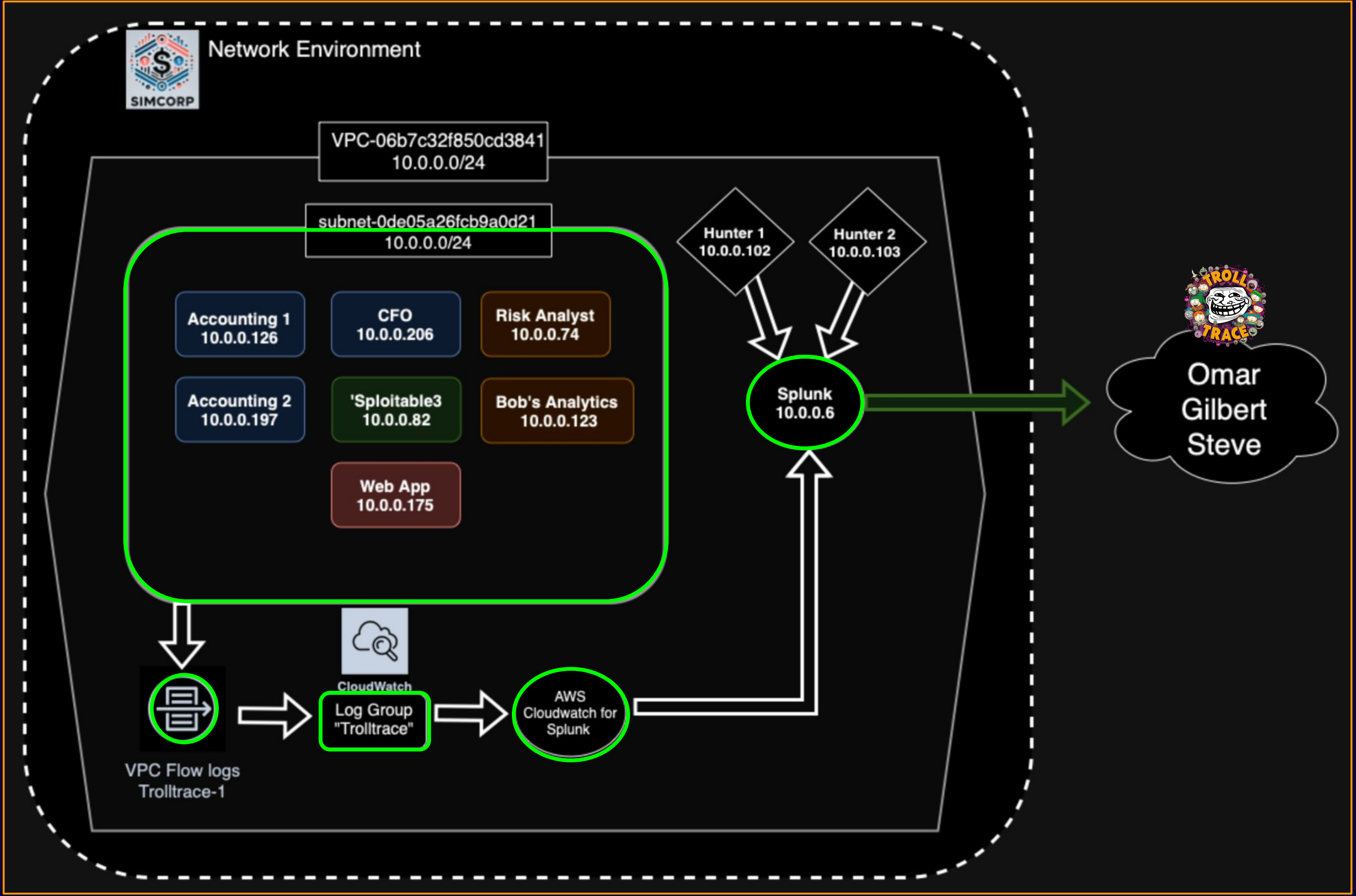
SimCorp Network Topology



SimCorp Network Topology

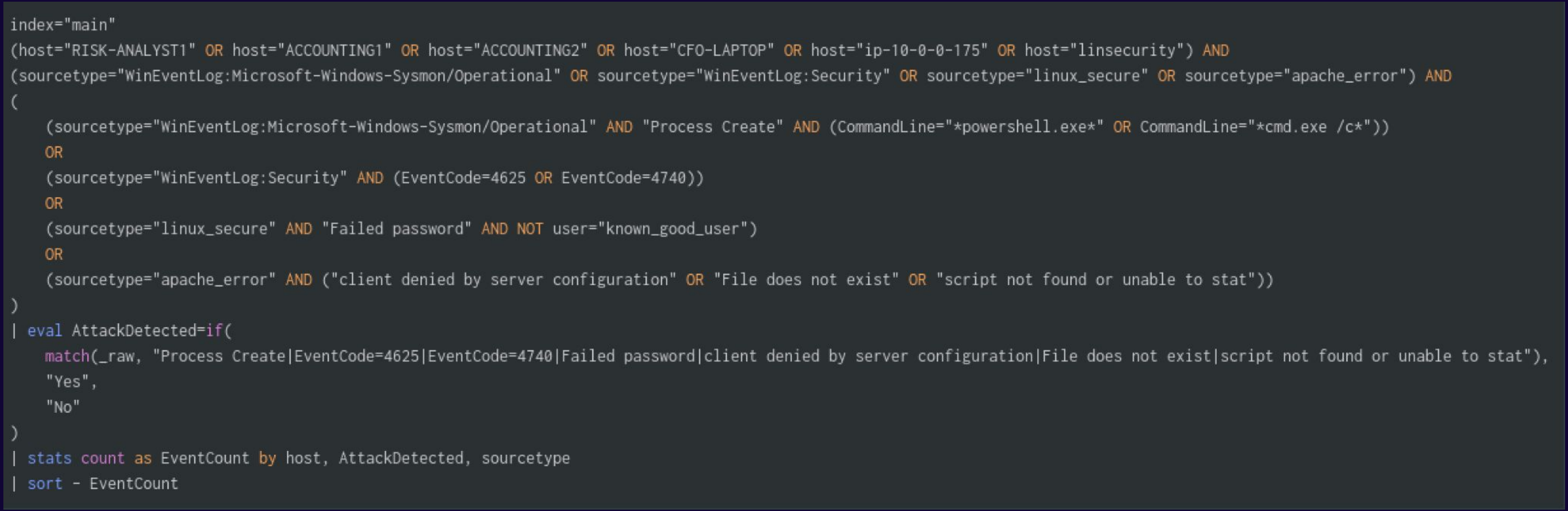


SimCorp Network Topology

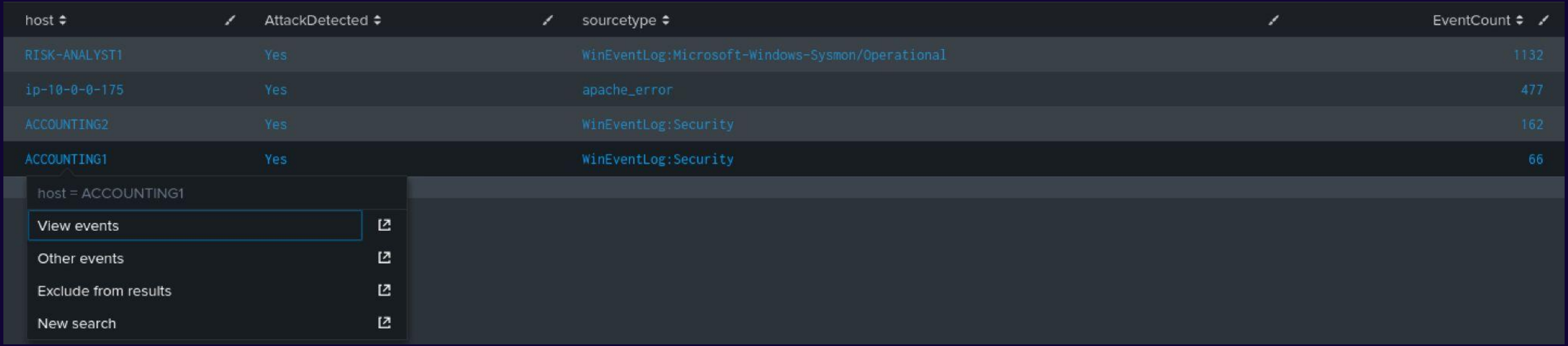


Splunk Alert Queries

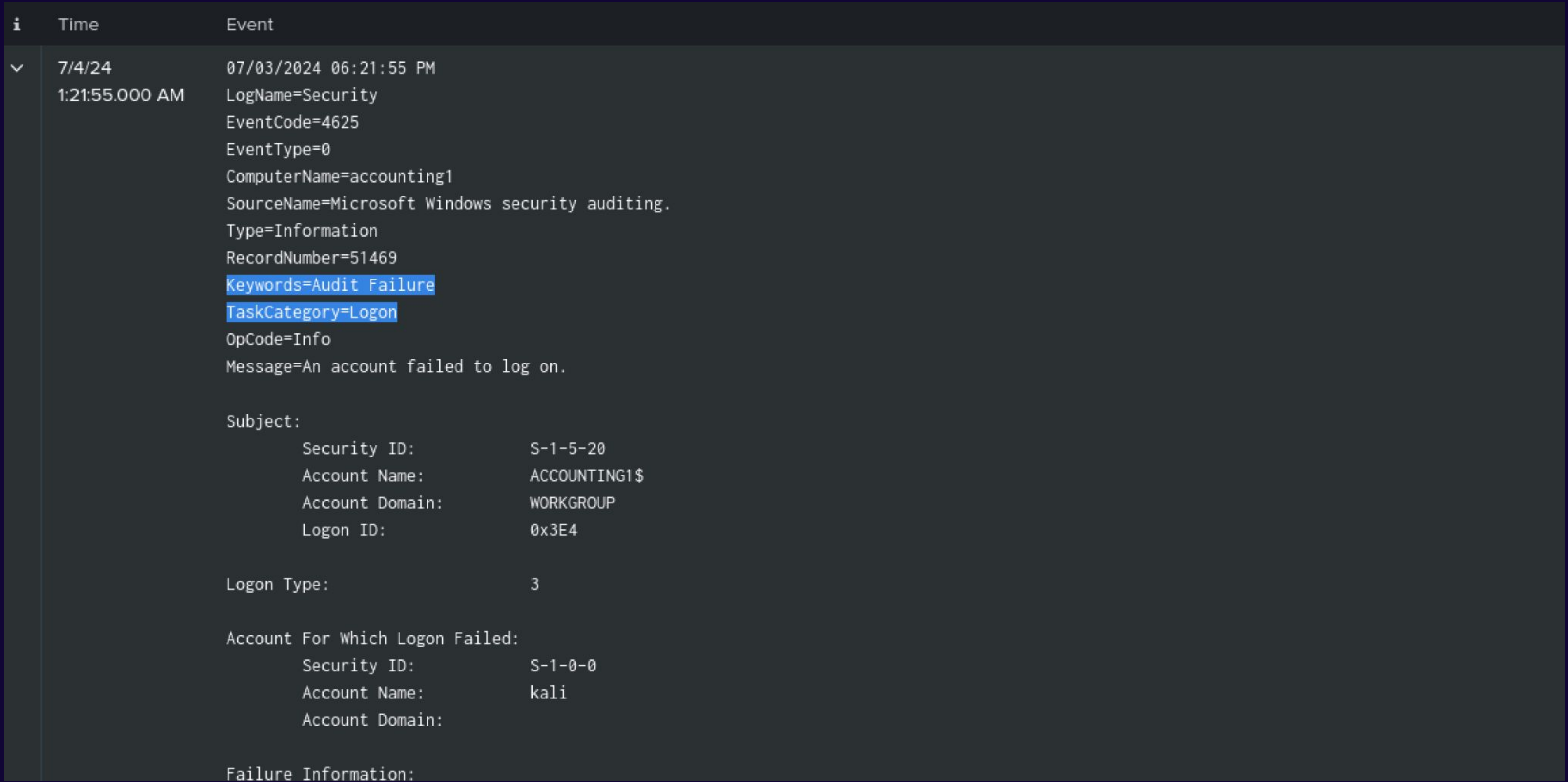
1. Search Query
2. Source and Event Filtering
3. Attack Detection Logic



```
index="main"
(host="RISK-ANALYST1" OR host="ACCOUNTING1" OR host="ACCOUNTING2" OR host="CFO-LAPTOP" OR host="ip-10-0-0-175" OR host="linsecurity") AND
(sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" OR sourcetype="WinEventLog:Security" OR sourcetype="linux_secure" OR sourcetype="apache_error") AND
(
    (sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND "Process Create" AND (CommandLine="*powershell.exe*" OR CommandLine="*cmd.exe /c*"))
    OR
    (sourcetype="WinEventLog:Security" AND (EventCode=4625 OR EventCode=4740))
    OR
    (sourcetype="linux_secure" AND "Failed password" AND NOT user="known_good_user")
    OR
    (sourcetype="apache_error" AND ("client denied by server configuration" OR "File does not exist" OR "script not found or unable to stat"))
)
| eval AttackDetected=if(
    match(_raw, "Process Create|EventCode=4625|EventCode=4740|Failed password|client denied by server configuration|File does not exist|script not found or unable to stat"),
    "Yes",
    "No"
)
| stats count as EventCount by host, AttackDetected, sourcetype
| sort - EventCount
```



host	AttackDetected	sourcetype	EventCount
RISK-ANALYST1	Yes	WinEventLog:Microsoft-Windows-Sysmon/Operational	1132
ip-10-0-0-175	Yes	apache_error	477
ACCOUNTING2	Yes	WinEventLog:Security	162
ACCOUNTING1	Yes	WinEventLog:Security	66



7/4/24
1:21:55.000 AM

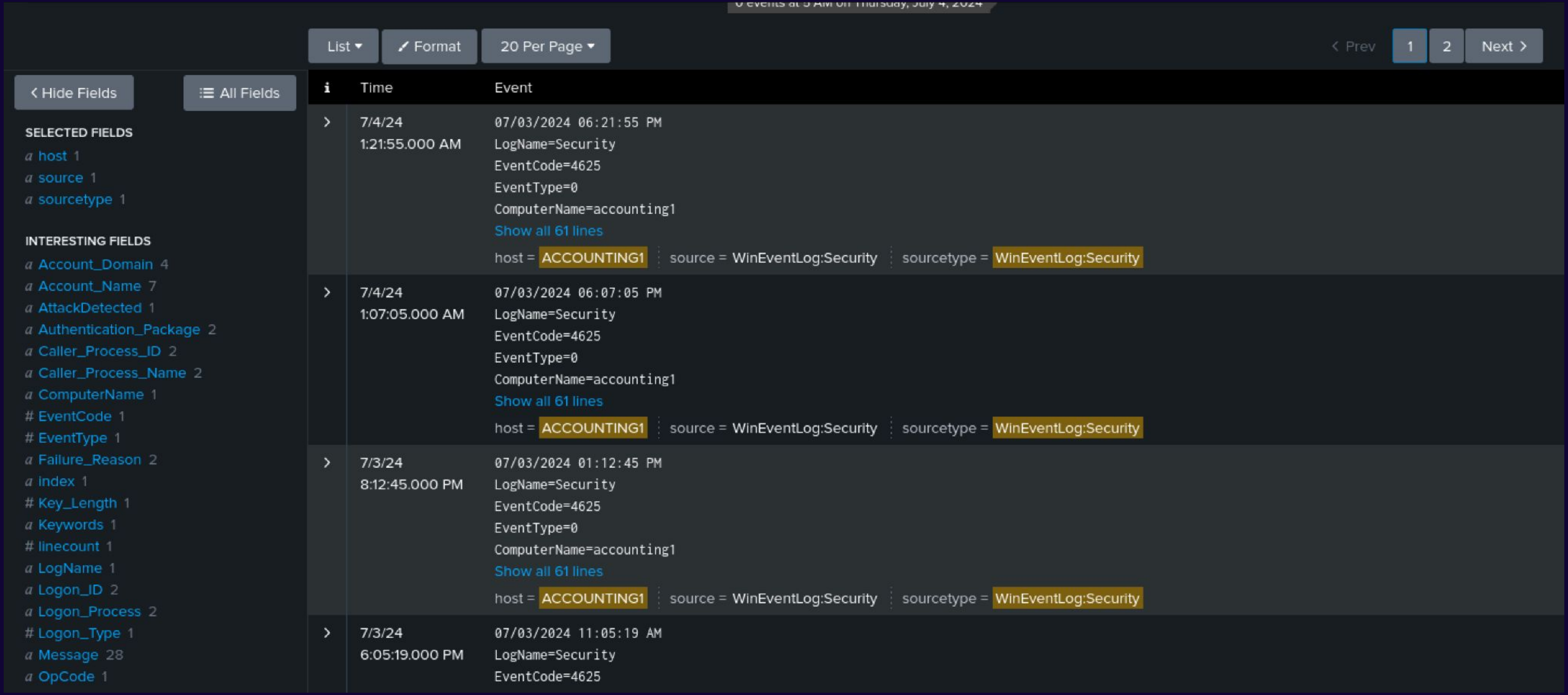
```
07/03/2024 06:21:55 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=accounting1
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=51469
Keywords=Audit Failure
TaskCategory=Logon
OpCode=Info
Message=An account failed to log on.

Subject:
        Security ID:            S-1-5-20
        Account Name:           ACCOUNTING1$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E4

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:           kali
        Account Domain:

Failure Information:
```



SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Account_Domain 4
- a Account_Name 7
- a AttackDetected 1
- a Authentication_Package 2
- a Caller_Process_ID 2
- a Caller_Process_Name 2
- a ComputerName 1
- # EventCode 1
- # EventType 1
- a Failure_Reason 2
- a index 1
- # Key_Length 1
- a Keywords 1
- # linecount 1
- a LogName 1
- a Logon_ID 2
- a Logon_Process 2
- # Logon_Type 1
- a Message 28
- a OpCode 1

Time	Event

7/4/24
1:21:55.000 AM
	07/03/2024 06:21:55 PM
	LogName=Security
	EventCode=4625
	EventType=0
	ComputerName=accounting1
	Show all 61 lines
	host = ACCOUNTING1 source = WinEventLog:Security sourcetype = WinEventLog:Security

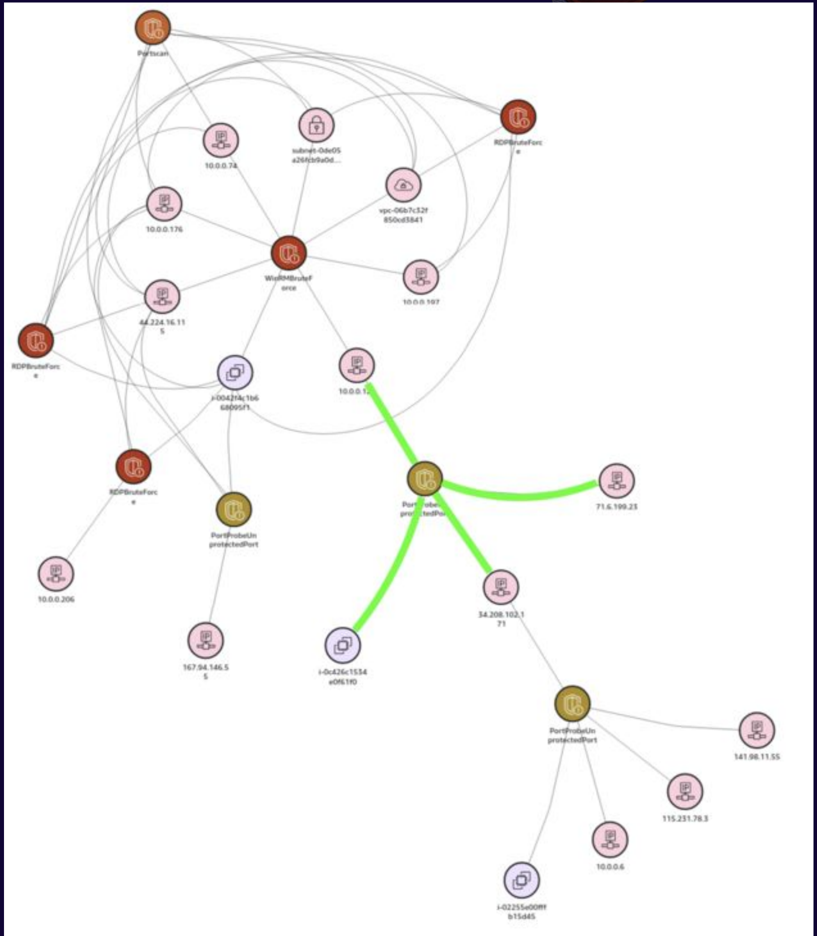
7/4/24
1:07:05.000 AM
	07/03/2024 06:07:05 PM
	LogName=Security
	EventCode=4625
	EventType=0
	ComputerName=accounting1
	Show all 61 lines
	host = ACCOUNTING1 source = WinEventLog:Security sourcetype = WinEventLog:Security

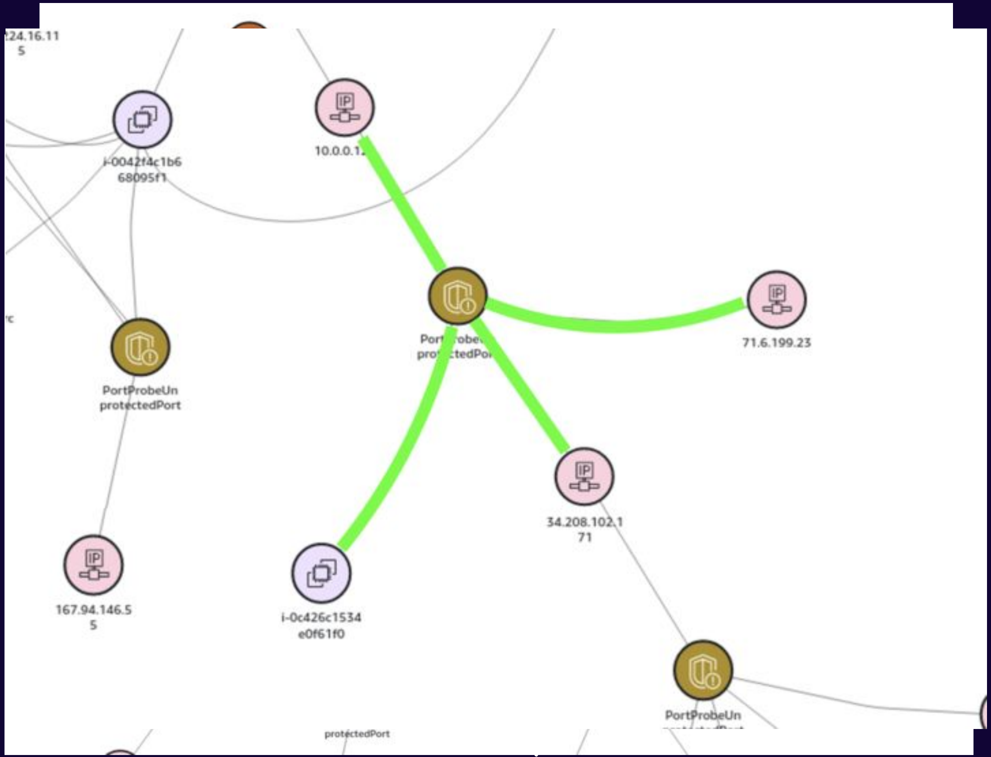
7/3/24
8:12:45.000 PM
	07/03/2024 01:12:45 PM
	LogName=Security
	EventCode=4625
	EventType=0
	ComputerName=accounting1
	Show all 61 lines
	host = ACCOUNTING1 source = WinEventLog:Security sourcetype = WinEventLog:Security

7/3/24
6:05:19.000 PM
	07/03/2024 11:05:19 AM
	LogName=Security
	EventCode=4625

]

Follow The Trail

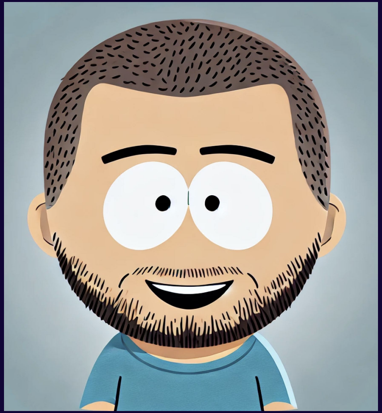




= [illegible]

Big Thank You to Code Fellows & All of our instructors:

Roger Huba

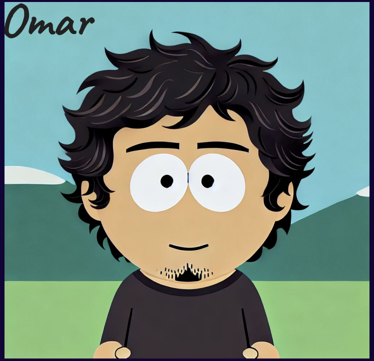


Marco Vazquez

Ethan Denny

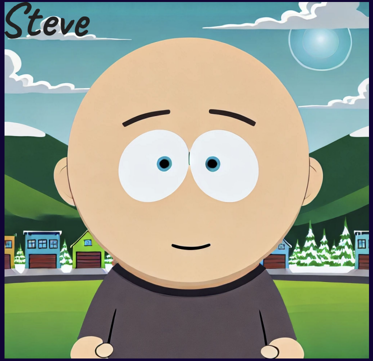
Resources & Thanks. Questions?

LinkedIn



GitHub

LinkedIn



GitHub

LinkedIn

GitHub