CWL
CyberWarFare Labs

CYBERWARFARE LABS

Blue Team Fundamentals

Foundations of Defense: Step into the Blue Team Realm

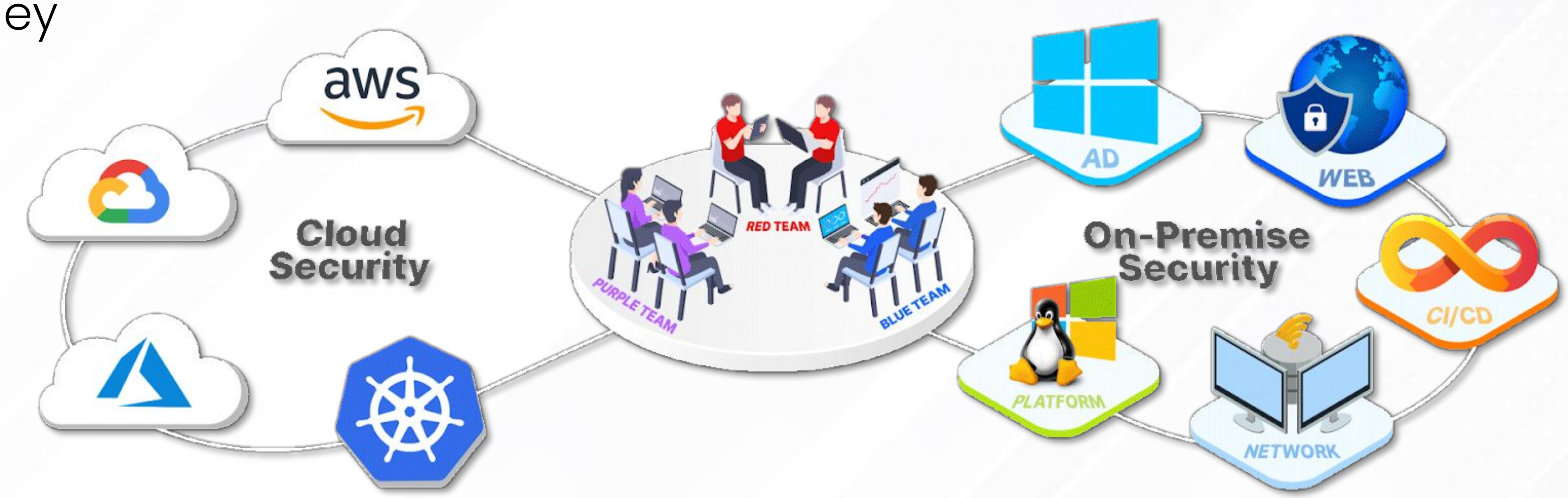
Blue Team Fundamentals [BTF]

About CyberWarFare Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions :

1. Cyber Range Labs

2. Up-Skilling Platform

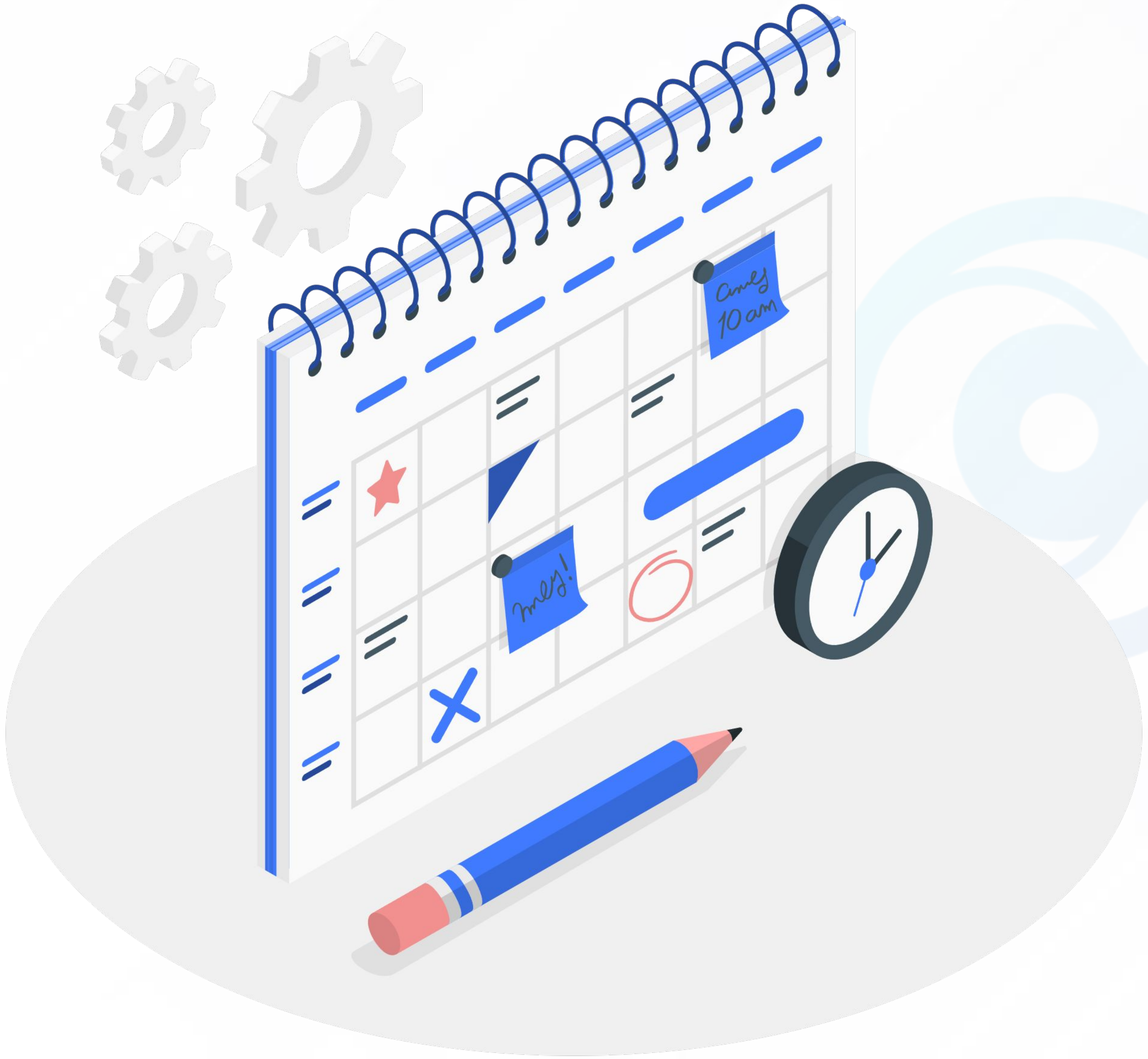


INFINITE LEARNING EXPERIENCE

About Speaker :

Harisuthan S
(Senior Security Engineer)

Is a Blue Team Security researcher, bringing over 3+ years of experience in cyber defence. possesses a deep understanding of Blue Team methodologies including investigation and detection over cyber attacks,



Agenda

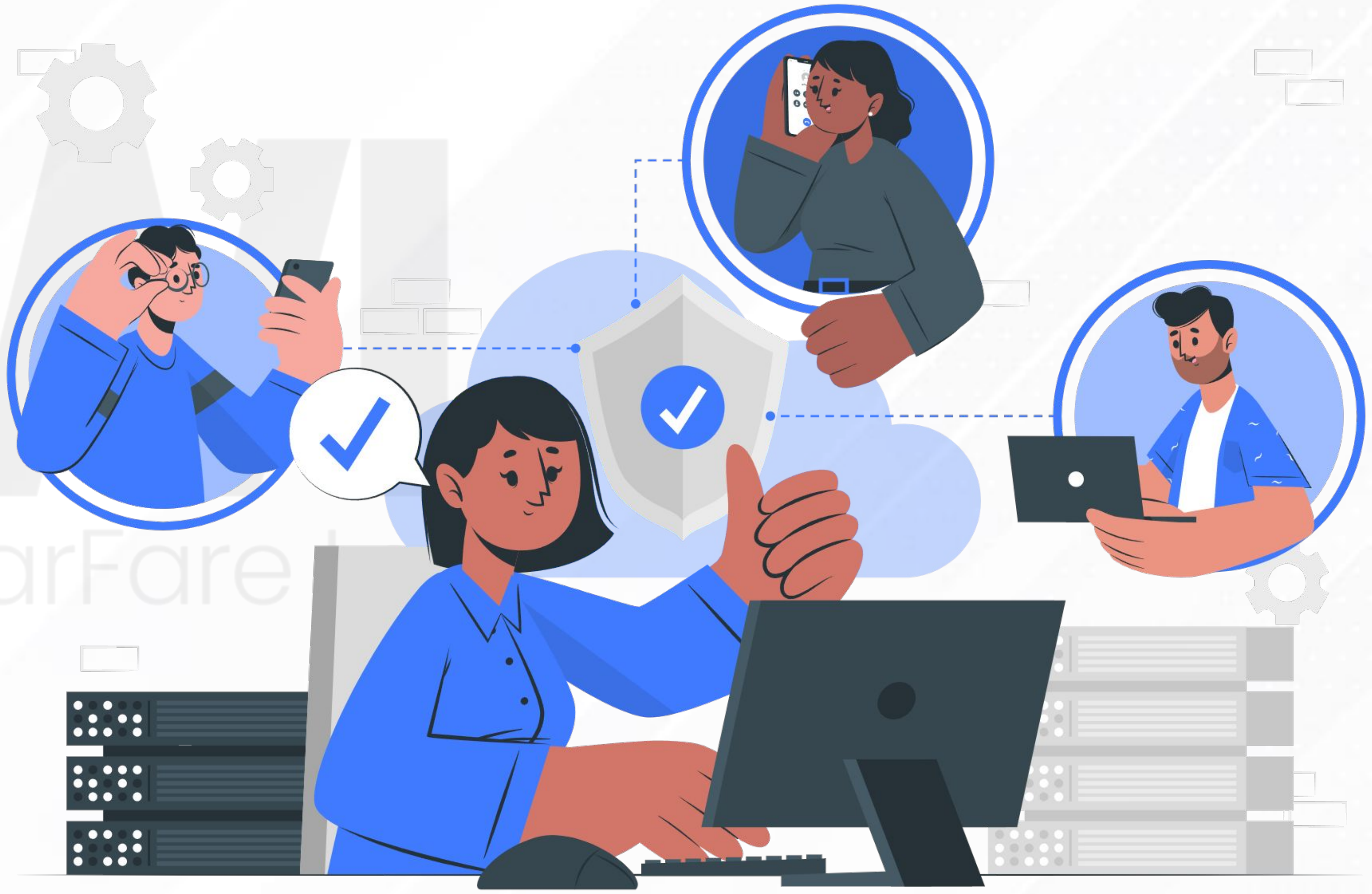
- Introduction to Cyber Defence
- Key Component of Cyber Defense
- Various Phases of Cyber Defence
- Chained Incident Investigation : Demo
- Blue Team Fundamentals : BTF
- Certification Procedure

Introduction to Cyber Defence

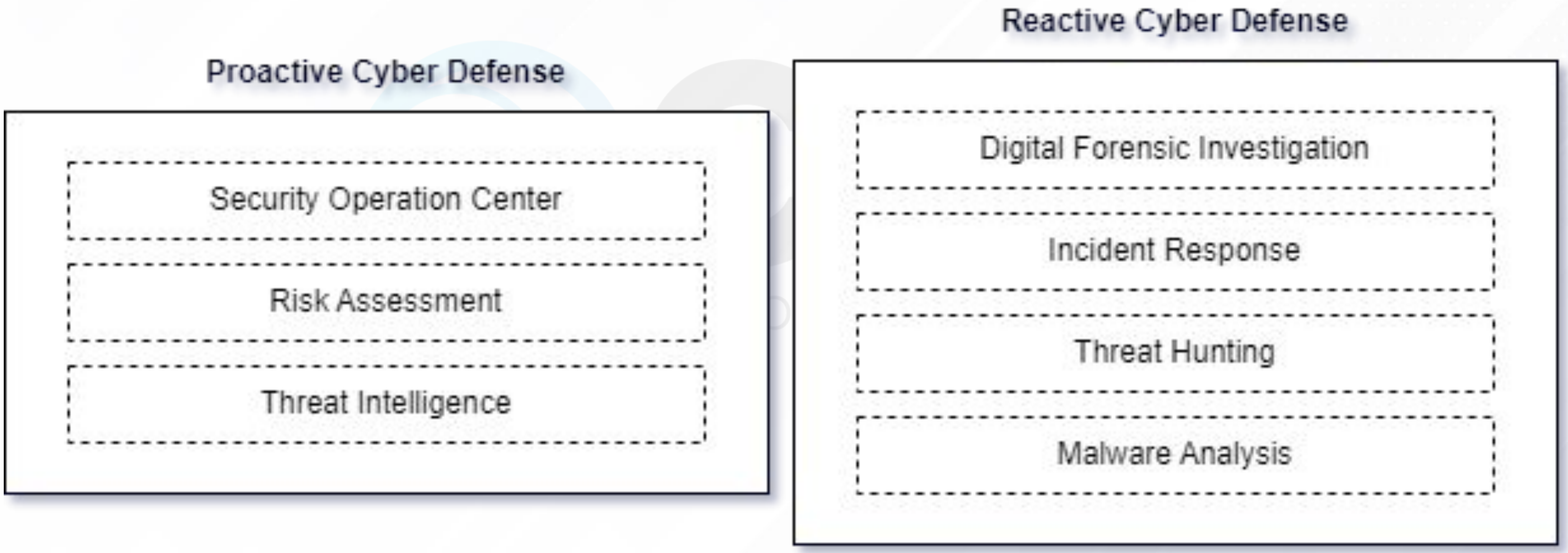
General overview of Cyber Defence

- **Cyber defense** is the strategy or a practice of protecting IT infrastructure from an malicious intrusions.

- It encompasses with a variety of practices, technologies, and processes which are designed to safeguard digital assets against cyber threats.



Proactive & Reactive Approach



Proactive Cyber Defense

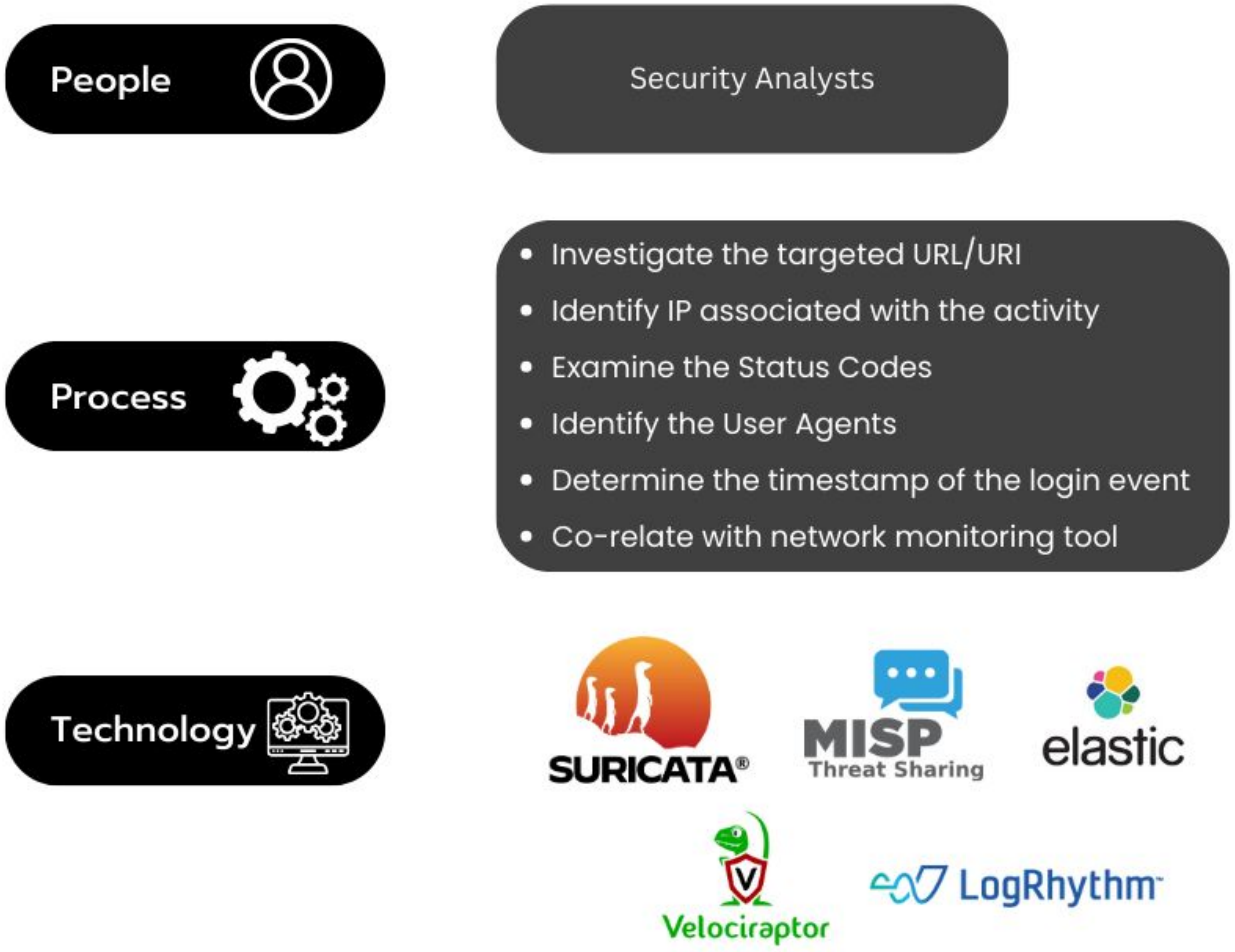
- Security Operation Center
- Risk Assessment
- Threat Intelligence

Reactive Cyber Defense

- Digital Forensic Investigation
- Incident Response
- Threat Hunting
- Malware Analysis

Key Component of Cyber Defense

The illustrated image provides a clear grasp of the whole fundamental component of cyber defence.



People

Security Analysts

Process

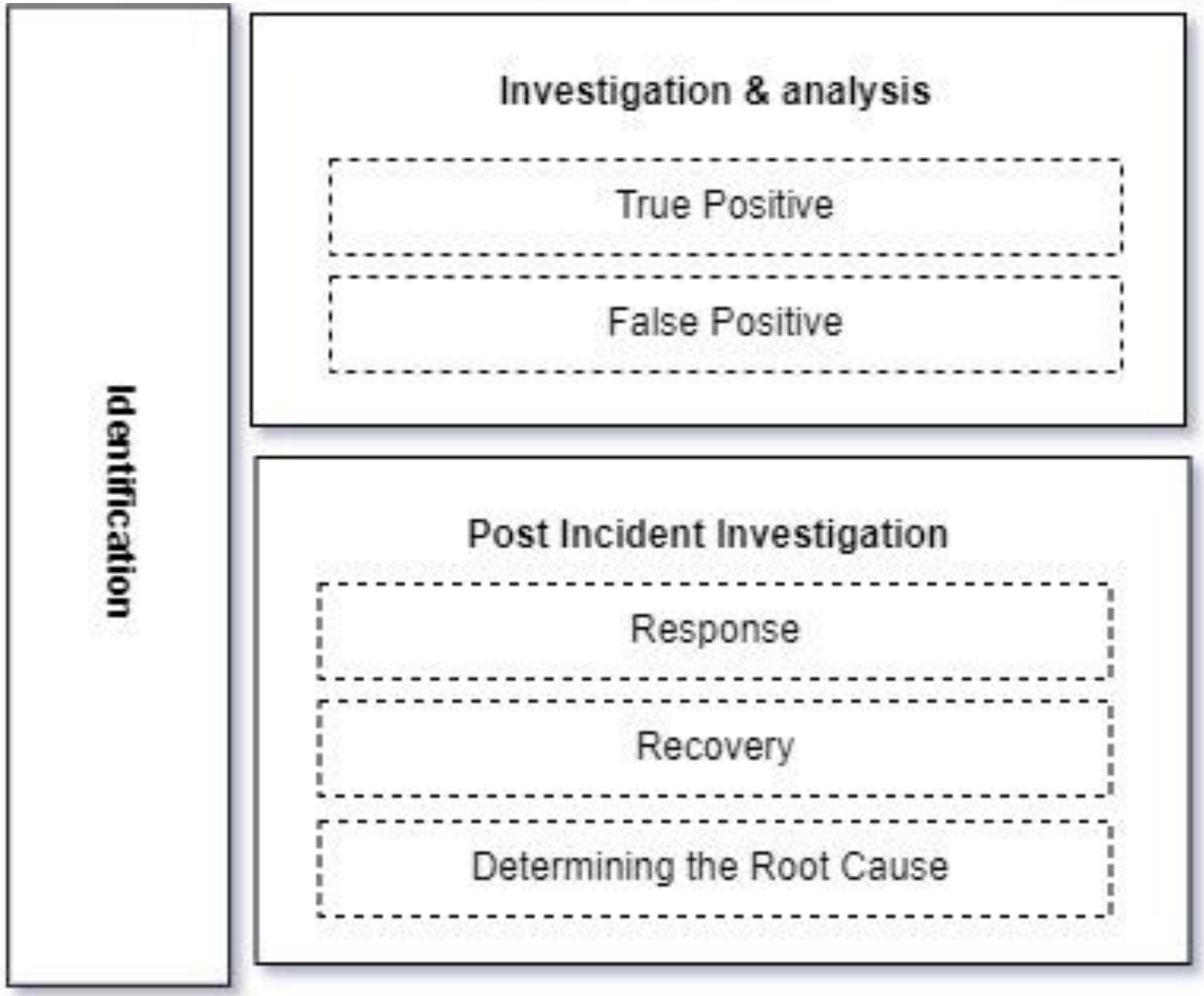
- Investigate the targeted URL/URI
- Identify IP associated with the activity
- Examine the Status Codes
- Identify the User Agents
- Determine the timestamp of the login event
- Co-relate with network monitoring tool

Technology

Three Phases of Cyber Defence

The overall overview of Cyber Defence has been grouped into three categories

- Identification
- Investigation & Analysis
- Post Incident Investigation



Identification

Investigation & analysis

True Positive

False Positive

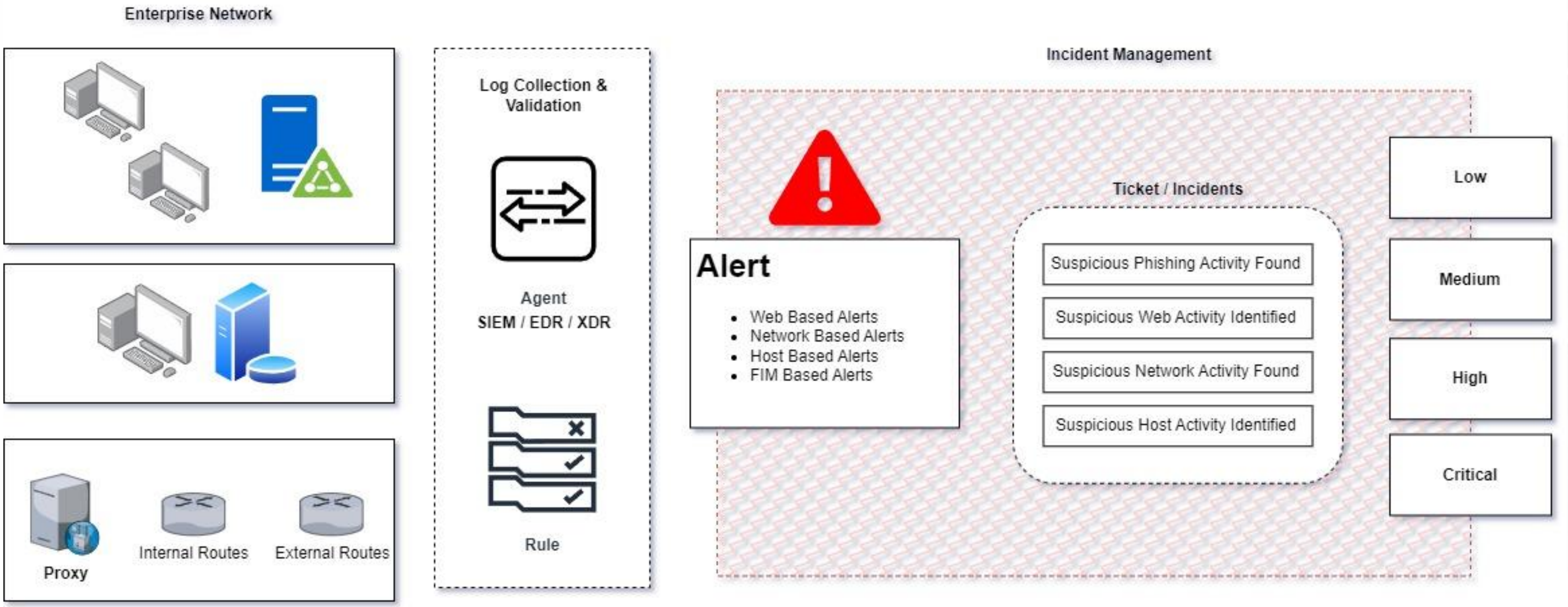
Post Incident Investigation

Response

Recovery

Determining the Root Cause

Identification Phase



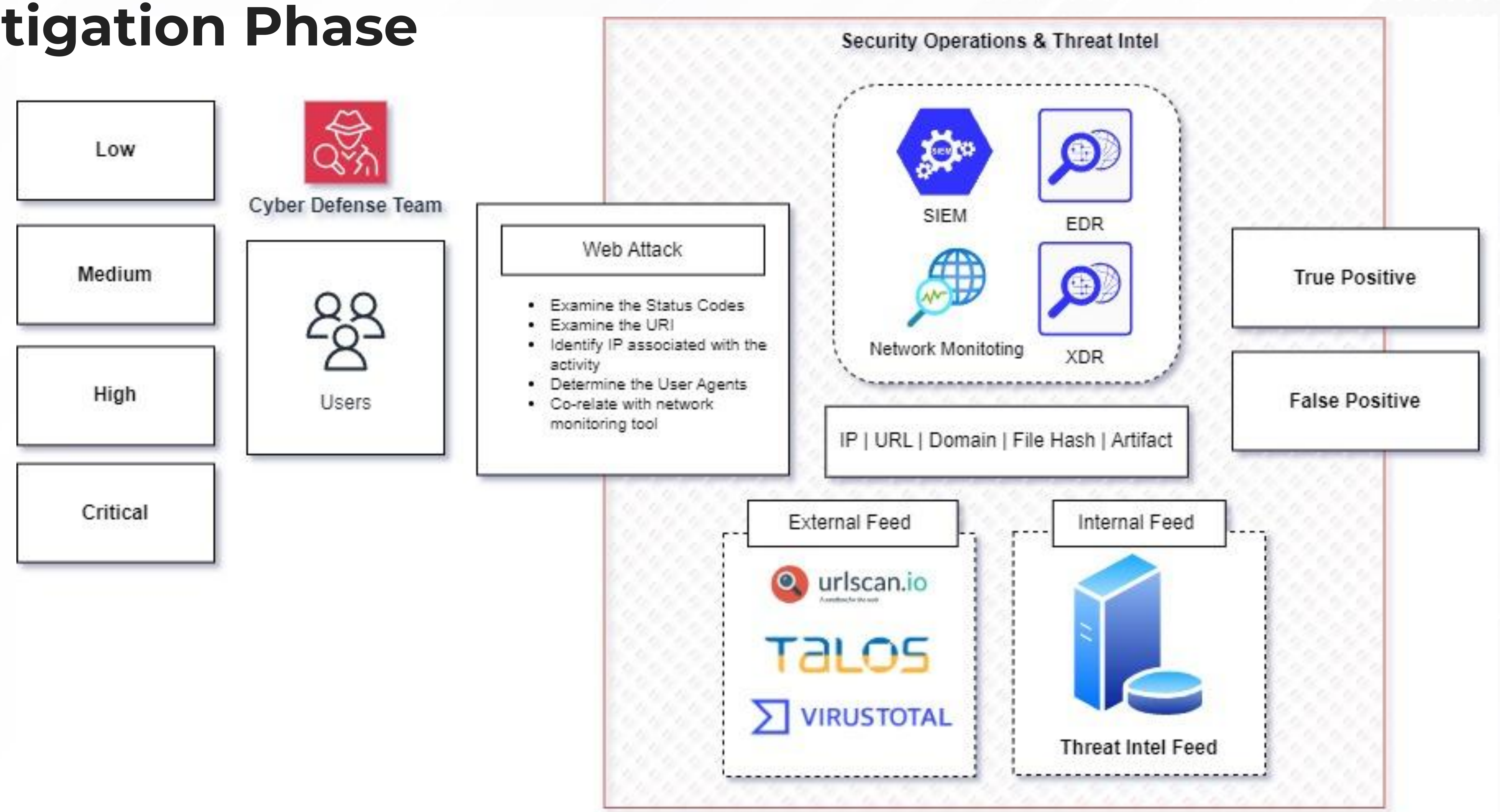
Alert

- Web Based Alerts
- Network Based Alerts
- Host Based Alerts
- FIM Based Alerts

Ticket / Incidents

- Suspicious Phishing Activity Found
- Suspicious Web Activity Identified
- Suspicious Network Activity Found
- Suspicious Host Activity Identified

Investigation Phase



Low

Medium

High

Critical

Cyber Defense Team

Users

Web Attack

- Examine the Status Codes
- Examine the URI
- Identify IP associated with the activity
- Determine the User Agents
- Co-relate with network monitoring tool

Security Operations & Threat Intel

SIEM

EDR

Network Monitoting

XDR

IP | URL | Domain | File Hash | Artifact

External Feed

urlscan.io

TALOS

VIRUSTOTAL

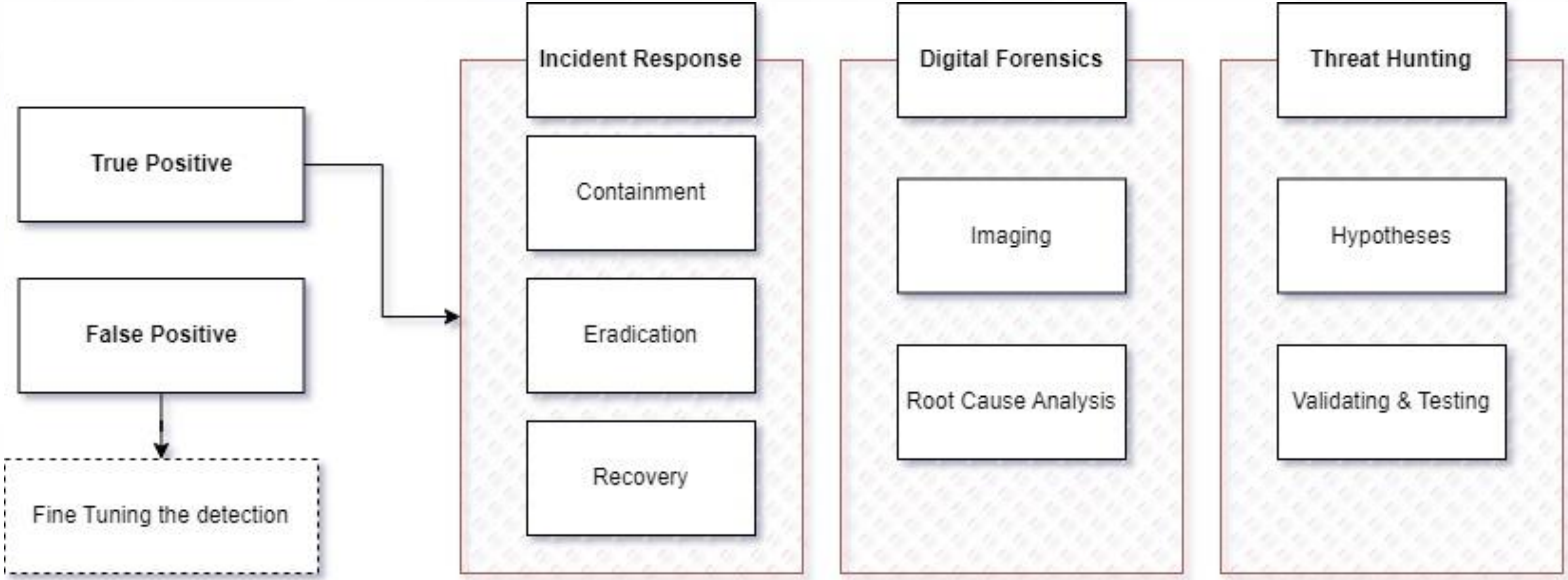
Internal Feed

Threat Intel Feed

True Positive

False Positive

Post Investigation Phase



Essential Abilities for Successful Cybersecurity Defenders

LOG Monitoring	Log Correlation	Incident Management	Prioritising the incident
Incident Investigations	Observing the findings	Correlation with various intel feeds	Determining the true nature of the events
Incident Response plan	Identifying and determining the root cause	Enhancing the detection rules	Tools & Technologies

Chained Incident Investigation : Demo

In our demonstration we will be detailly discussing about how the chained attacks are been investigated and responded.

- Suspicious network scan activity detected
- Remote service Brute Forcing activity detected
- Remote login activity detected

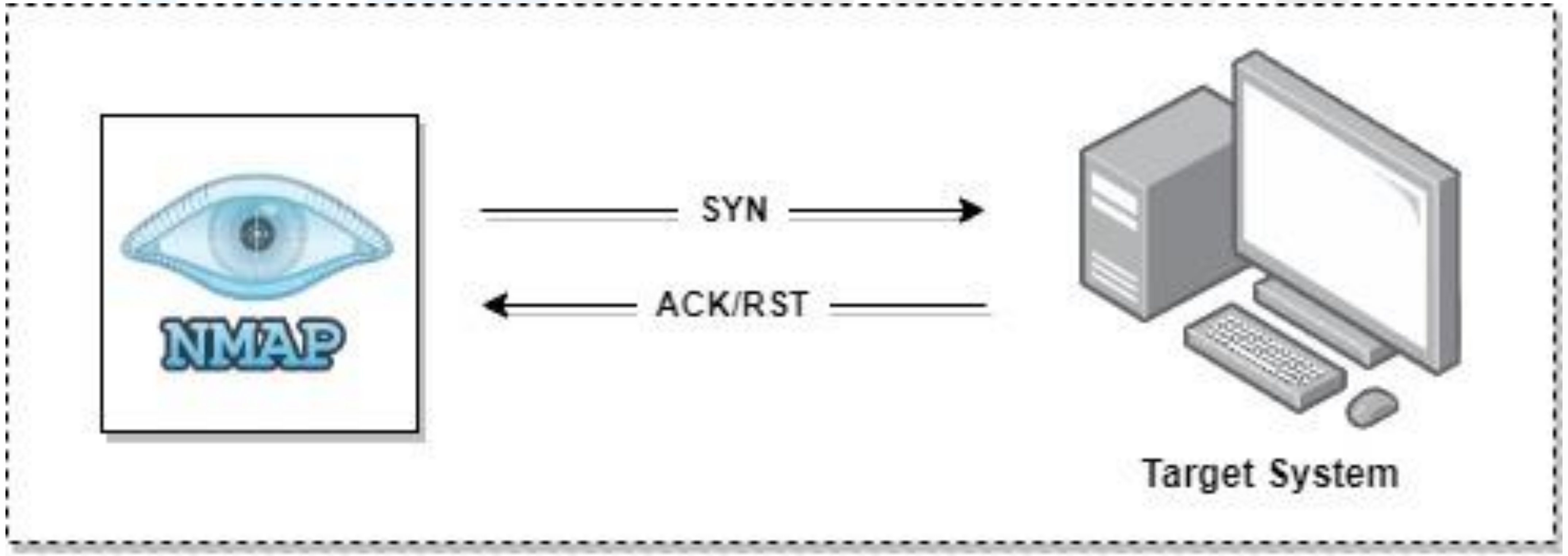
Suspicious network scan activity investigation

Attackers generally uses various techniques such as network scan to determine and identify the open and vulnerable port for further exploitation

1. Host Discovery
2. Port Scanning
3. Service Version Detection
4. OS Fingerprinting
5. Firewall and Security Policy Auditing

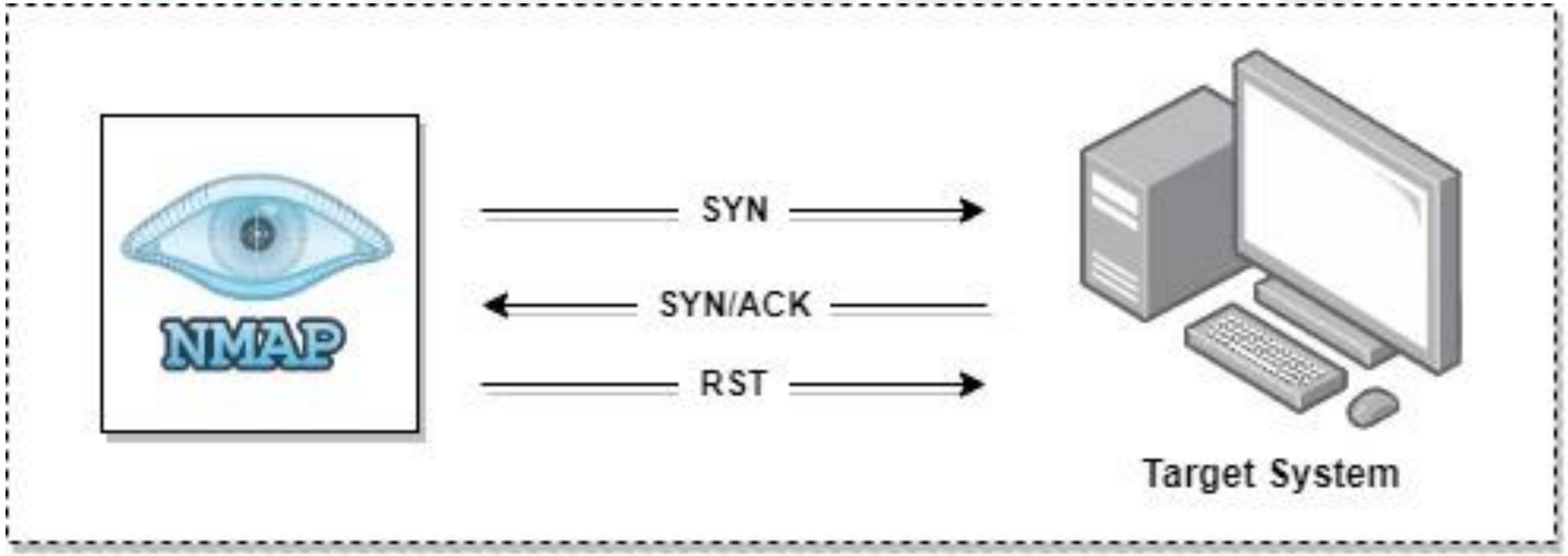
Working of Port Scanning in NMAP

Nmap requests are generally custom crafted network packets for enumeration, The pattern of the **SYN** flag with a response of **ACK/RST** is observed when an attacker is trying to execute NMAP Port Scan activity.



Working of Port Scanning in NMAP

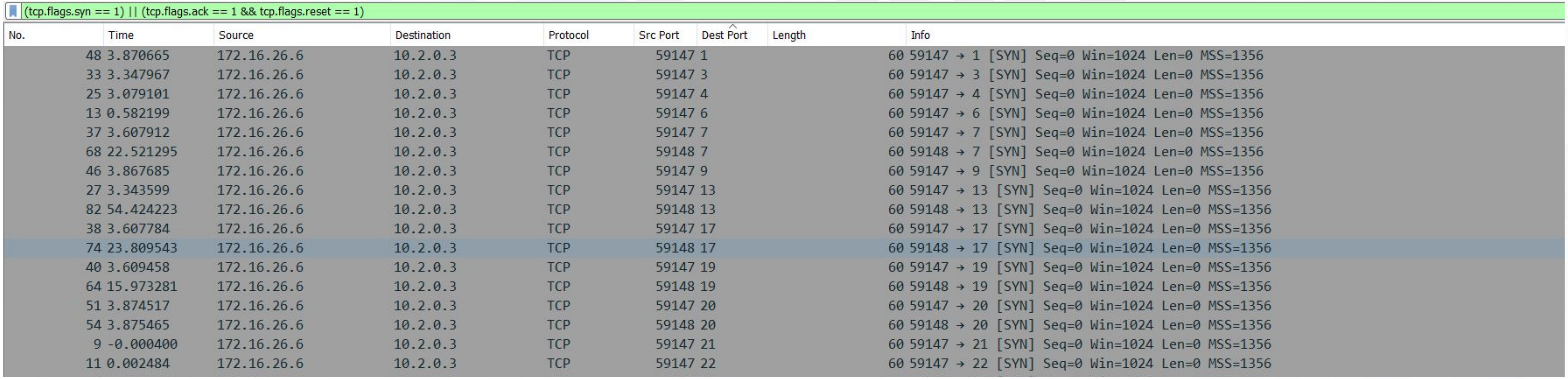
The pattern of the **SYN** | **SYN/ACK** | **RST** is observed when an attacker successfully enumerates the open port in the target system.



Detecting NMAP : Port Scan Activity

To determine the NMAP Port scan activity

```
(tcp.flags.syn == 1) || (tcp.flags.ack == 1 && tcp.flags.reset == 1)
```

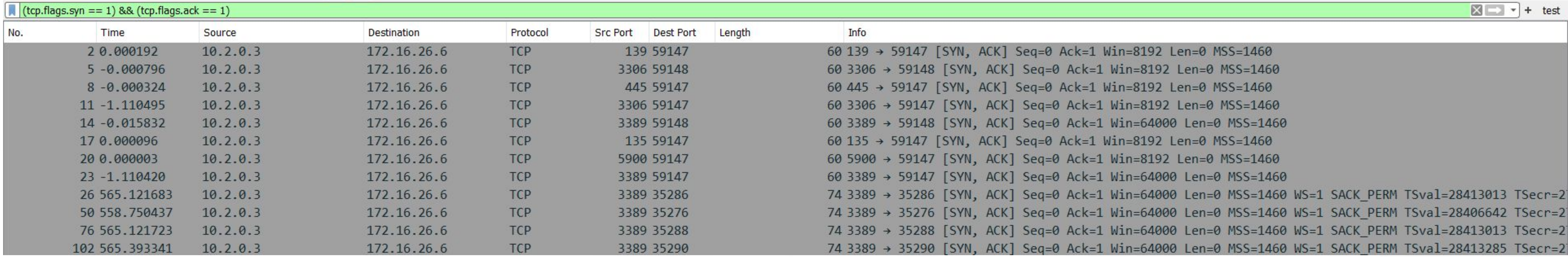


```
(tcp.flags.syn == 1) || (tcp.flags.ack == 1 && tcp.flags.reset == 1)
No.    Time       Source       Destination  Protocol  Src Port Dest Port  Length  Info
    48 3.870665   172.16.26.6  10.2.0.3     TCP       59147 1                 60 59147 → 1 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    33 3.347967   172.16.26.6  10.2.0.3     TCP       59147 3                 60 59147 → 3 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    25 3.079101   172.16.26.6  10.2.0.3     TCP       59147 4                 60 59147 → 4 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    13 0.582199   172.16.26.6  10.2.0.3     TCP       59147 6                 60 59147 → 6 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    37 3.607912   172.16.26.6  10.2.0.3     TCP       59147 7                 60 59147 → 7 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    68 22.521295  172.16.26.6  10.2.0.3     TCP       59148 7                 60 59148 → 7 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    46 3.867685   172.16.26.6  10.2.0.3     TCP       59147 9                 60 59147 → 9 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    27 3.343599   172.16.26.6  10.2.0.3     TCP       59147 13                60 59147 → 13 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    82 54.424223  172.16.26.6  10.2.0.3     TCP       59148 13                60 59148 → 13 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    38 3.607784   172.16.26.6  10.2.0.3     TCP       59147 17                60 59147 → 17 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    74 23.809543  172.16.26.6  10.2.0.3     TCP       59148 17                60 59148 → 17 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    40 3.609458   172.16.26.6  10.2.0.3     TCP       59147 19                60 59147 → 19 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    64 15.973281  172.16.26.6  10.2.0.3     TCP       59148 19                60 59148 → 19 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    51 3.874517   172.16.26.6  10.2.0.3     TCP       59147 20                60 59147 → 20 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    54 3.875465   172.16.26.6  10.2.0.3     TCP       59148 20                60 59148 → 20 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
     9 -0.000400  172.16.26.6  10.2.0.3     TCP       59147 21                60 59147 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
    11 0.002484   172.16.26.6  10.2.0.3     TCP       59147 22                60 59147 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1356
```

Detecting NMAP : Port Scan Activity

To determine the result of the NMAP Port scan activity

(tcp.flags.syn == 1) && (tcp.flags.ack == 1)



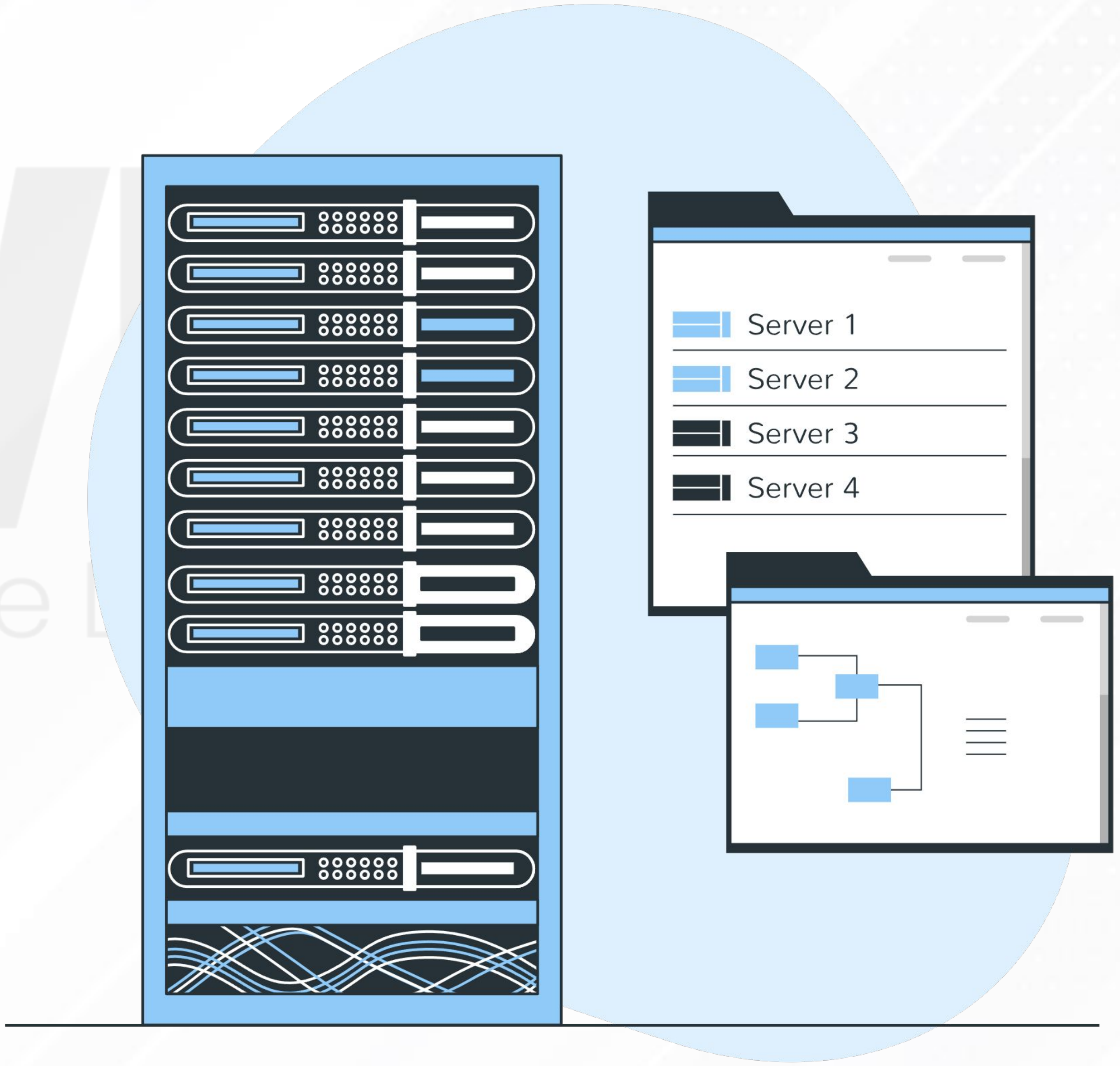
(tcp.flags.syn == 1) && (tcp.flags.ack == 1)

No.	Time	Source	Destination	Protocol	Src Port	Dest Port	Length	Info
2	0.000192	10.2.0.3	172.16.26.6	TCP	139	59147	60	139 → 59147 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
5	-0.000796	10.2.0.3	172.16.26.6	TCP	3306	59148	60	3306 → 59148 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
8	-0.000324	10.2.0.3	172.16.26.6	TCP	445	59147	60	445 → 59147 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
11	-1.110495	10.2.0.3	172.16.26.6	TCP	3306	59147	60	3306 → 59147 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
14	-0.015832	10.2.0.3	172.16.26.6	TCP	3389	59148	60	3389 → 59148 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
17	0.000096	10.2.0.3	172.16.26.6	TCP	135	59147	60	135 → 59147 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
20	0.000003	10.2.0.3	172.16.26.6	TCP	5900	59147	60	5900 → 59147 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
23	-1.110420	10.2.0.3	172.16.26.6	TCP	3389	59147	60	3389 → 59147 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
26	565.121683	10.2.0.3	172.16.26.6	TCP	3389	35286	74	3389 → 35286 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM TSval=28413013 TSecr=2
50	558.750437	10.2.0.3	172.16.26.6	TCP	3389	35276	74	3389 → 35276 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM TSval=28406642 TSecr=2
76	565.121723	10.2.0.3	172.16.26.6	TCP	3389	35288	74	3389 → 35288 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM TSval=28413013 TSecr=2
102	565.393341	10.2.0.3	172.16.26.6	TCP	3389	35290	74	3389 → 35290 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM TSval=28413285 TSecr=2

Remote Brute Forcing activity detected

The attacker systematically tries various combinations of usernames and passwords until they find the correct credentials to gain access. Brute force attacks can be automated using software tools that rapidly generate and test password combinations.

1. Identification of RDP Service
2. Brute Forcing the identified RDP service
3. Performing Password Guessing



Working of Remote Brute Forcing

RDP Brute Forcing generate a high volume of network traffic and request towards the targeted victim, below listed as some commonly targeted remote service based attacks

3389 : RDP | Used for remote access and control of Windows systems.

5900 : VNC | Provides remote desktop sharing and control.

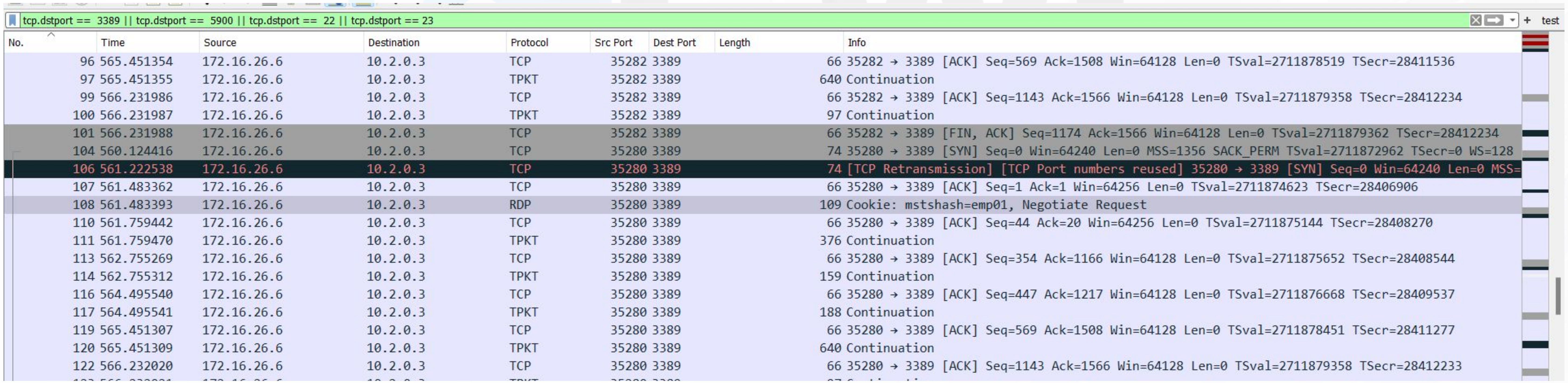
22 : SSH | Used to securely sending commands to a computer over an unsecured network.

23 : Telnet | Provides remote access to command-line interface (CLI)

Detecting Remote Brute Forcing

To identify which Remote service is been targeted

```
tcp.dstport ==  3389 || tcp.dstport ==  5900 || tcp.dstport ==  22 || tcp.dstport == 23
```

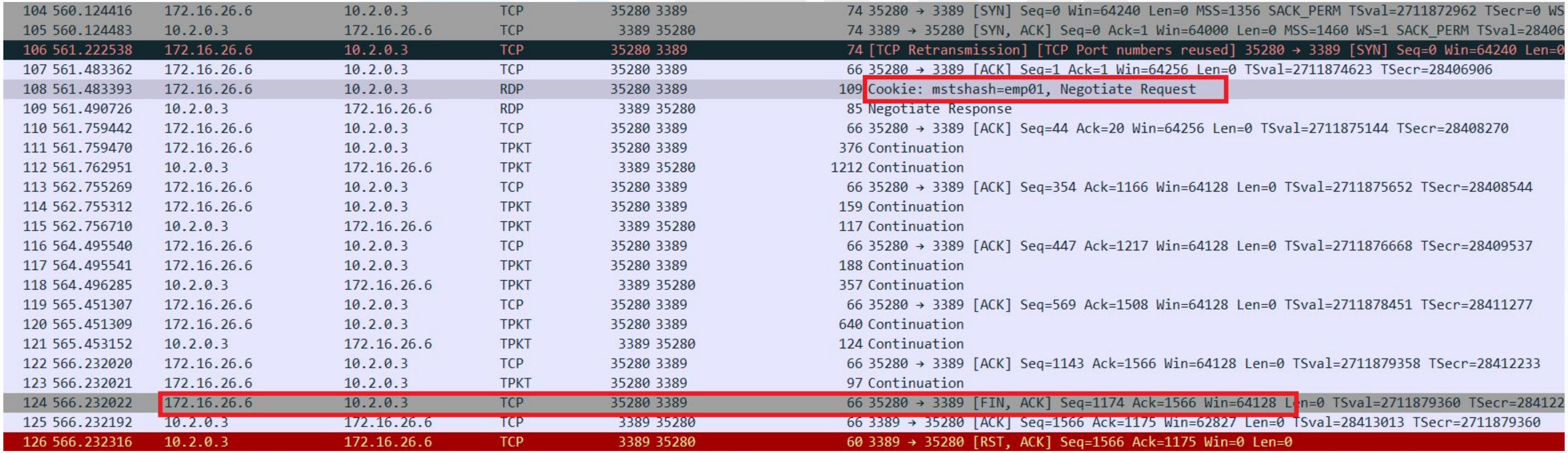


```
tcp.dstport ==  3389 || tcp.dstport ==  5900 || tcp.dstport ==  22 || tcp.dstport == 23
```

```
No.   Time        Source       Destination  Protocol  Src Port Dest Port  Length  Info
   96 565.451354  172.16.26.6  10.2.0.3     TCP       35282 3389              66 35282 → 3389 [ACK] Seq=569 Ack=1508 Win=64128 Len=0 TSval=2711878519 TSecr=28411536
   97 565.451355  172.16.26.6  10.2.0.3     TPKT      35282 3389             640 Continuation
   99 566.231986  172.16.26.6  10.2.0.3     TCP       35282 3389              66 35282 → 3389 [ACK] Seq=1143 Ack=1566 Win=64128 Len=0 TSval=2711879358 TSecr=28412234
  100 566.231987  172.16.26.6  10.2.0.3     TPKT      35282 3389              97 Continuation
  101 566.231988  172.16.26.6  10.2.0.3     TCP       35282 3389              66 35282 → 3389 [FIN, ACK] Seq=1174 Ack=1566 Win=64128 Len=0 TSval=2711879362 TSecr=28412234
  104 560.124416  172.16.26.6  10.2.0.3     TCP       35280 3389              74 35280 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1356 SACK_PERM TSval=2711872962 TSecr=0 WS=128
  106 561.222538  172.16.26.6  10.2.0.3     TCP       35280 3389              74 [TCP Retransmission] [TCP Port numbers reused] 35280 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=
  107 561.483362  172.16.26.6  10.2.0.3     TCP       35280 3389              66 35280 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2711874623 TSecr=28406906
  108 561.483393  172.16.26.6  10.2.0.3     RDP       35280 3389             109 Cookie: mstshash=emp01, Negotiate Request
  110 561.759442  172.16.26.6  10.2.0.3     TCP       35280 3389              66 35280 → 3389 [ACK] Seq=44 Ack=20 Win=64256 Len=0 TSval=2711875144 TSecr=28408270
  111 561.759470  172.16.26.6  10.2.0.3     TPKT      35280 3389             376 Continuation
  113 562.755269  172.16.26.6  10.2.0.3     TCP       35280 3389              66 35280 → 3389 [ACK] Seq=354 Ack=1166 Win=64128 Len=0 TSval=2711875652 TSecr=28408544
  114 562.755312  172.16.26.6  10.2.0.3     TPKT      35280 3389             159 Continuation
  116 564.495540  172.16.26.6  10.2.0.3     TCP       35280 3389              66 35280 → 3389 [ACK] Seq=447 Ack=1217 Win=64128 Len=0 TSval=2711876668 TSecr=28409537
  117 564.495541  172.16.26.6  10.2.0.3     TPKT      35280 3389             188 Continuation
  119 565.451307  172.16.26.6  10.2.0.3     TCP       35280 3389              66 35280 → 3389 [ACK] Seq=569 Ack=1508 Win=64128 Len=0 TSval=2711878451 TSecr=28411277
  120 565.451309  172.16.26.6  10.2.0.3     TPKT      35280 3389             640 Continuation
  122 566.232020  172.16.26.6  10.2.0.3     TCP       35280 3389              66 35280 → 3389 [ACK] Seq=1143 Ack=1566 Win=64128 Len=0 TSval=2711879358 TSecr=28412233
```

Investigating Remote Brute Forcing

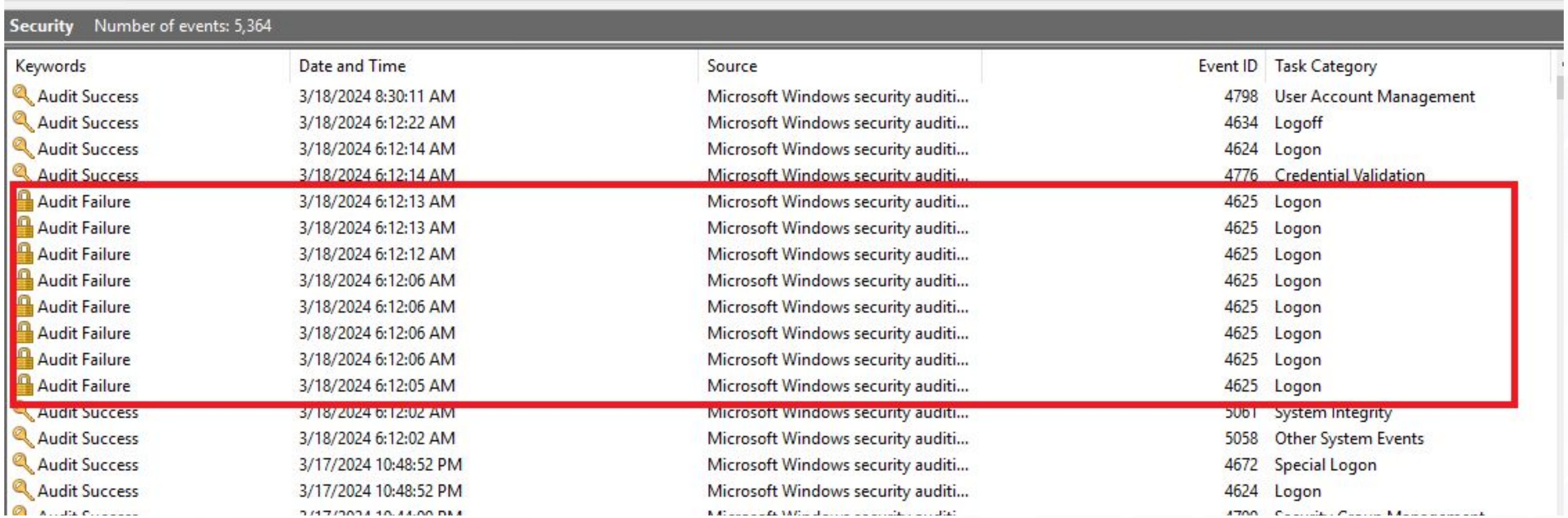
While investigating we observed multiple network packets with the username **emp01** after a short span of time the external IP is been sending **FIN - ACK**



```
104 560.124416  172.16.26.6  10.2.0.3     TCP   35280 3389    74 35280 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1356 SACK_PERM TSval=2711872962 TSecr=0 WS
105 560.124483  10.2.0.3     172.16.26.6  TCP    3389 35280   74 3389 → 35280 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM TSval=28406
106 561.222538  172.16.26.6  10.2.0.3     TCP   35280 3389    74 [TCP Retransmission] [TCP Port numbers reused] 35280 → 3389 [SYN] Seq=0 Win=64240 Len=0
107 561.483362  172.16.26.6  10.2.0.3     TCP   35280 3389    66 35280 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2711874623 TSecr=28406906
108 561.483393  172.16.26.6  10.2.0.3     RDP   35280 3389   109 Cookie: mstshash=emp01, Negotiate Request
109 561.490726  10.2.0.3     172.16.26.6  RDP    3389 35280   85 Negotiate Response
110 561.759442  172.16.26.6  10.2.0.3     TCP   35280 3389    66 35280 → 3389 [ACK] Seq=44 Ack=20 Win=64256 Len=0 TSval=2711875144 TSecr=28408270
111 561.759470  172.16.26.6  10.2.0.3     TPKT  35280 3389   376 Continuation
112 561.762951  10.2.0.3     172.16.26.6  TPKT   3389 35280 1212 Continuation
113 562.755269  172.16.26.6  10.2.0.3     TCP   35280 3389    66 35280 → 3389 [ACK] Seq=354 Ack=1166 Win=64128 Len=0 TSval=2711875652 TSecr=28408544
114 562.755312  172.16.26.6  10.2.0.3     TPKT  35280 3389   159 Continuation
115 562.756710  10.2.0.3     172.16.26.6  TPKT   3389 35280  117 Continuation
116 564.495540  172.16.26.6  10.2.0.3     TCP   35280 3389    66 35280 → 3389 [ACK] Seq=447 Ack=1217 Win=64128 Len=0 TSval=2711876668 TSecr=28409537
117 564.495541  172.16.26.6  10.2.0.3     TPKT  35280 3389   188 Continuation
118 564.496285  10.2.0.3     172.16.26.6  TPKT   3389 35280  357 Continuation
119 565.451307  172.16.26.6  10.2.0.3     TCP   35280 3389    66 35280 → 3389 [ACK] Seq=569 Ack=1508 Win=64128 Len=0 TSval=2711878451 TSecr=28411277
120 565.451309  172.16.26.6  10.2.0.3     TPKT  35280 3389   640 Continuation
121 565.453152  10.2.0.3     172.16.26.6  TPKT   3389 35280  124 Continuation
122 566.232020  172.16.26.6  10.2.0.3     TCP   35280 3389    66 35280 → 3389 [ACK] Seq=1143 Ack=1566 Win=64128 Len=0 TSval=2711879358 TSecr=28412233
123 566.232021  172.16.26.6  10.2.0.3     TPKT  35280 3389    97 Continuation
124 566.232022  172.16.26.6  10.2.0.3     TCP   35280 3389    66 35280 → 3389 [FIN, ACK] Seq=1174 Ack=1566 Win=64128 Len=0 TSval=2711879360 TSecr=284122
125 566.232192  10.2.0.3     172.16.26.6  TCP    3389 35280   66 3389 → 35280 [ACK] Seq=1566 Ack=1175 Win=62827 Len=0 TSval=28413013 TSecr=2711879360
126 566.232316  10.2.0.3     172.16.26.6  TCP    3389 35280   60 3389 → 35280 [RST, ACK] Seq=1566 Ack=1175 Win=0 Len=0
```

Investigating Remote Brute Forcing

Alternatively this activity can be cross verified with the event log associated with the targeted host machine, as we observed multiple failed login failed simultaneously in a short period of time.



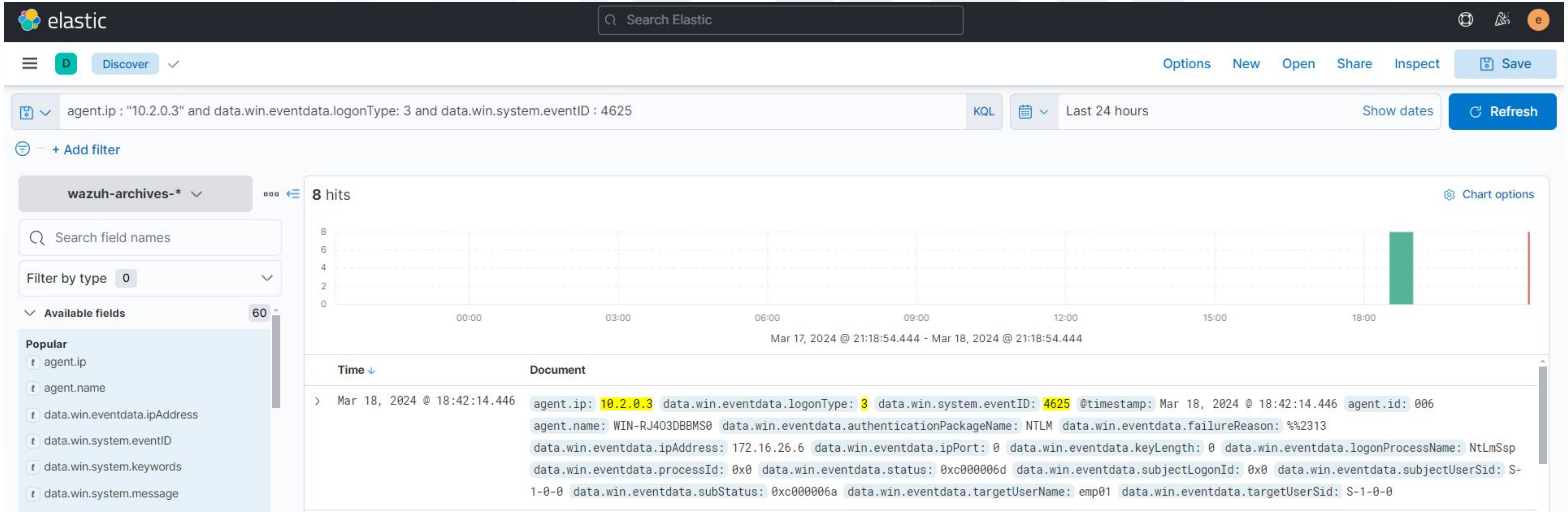
Security Number of events: 5,364

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	3/18/2024 8:30:11 AM	Microsoft Windows security auditi...	4798	User Account Management
Audit Success	3/18/2024 6:12:22 AM	Microsoft Windows security auditi...	4634	Logoff
Audit Success	3/18/2024 6:12:14 AM	Microsoft Windows security auditi...	4624	Logon
Audit Success	3/18/2024 6:12:14 AM	Microsoft Windows security auditi...	4776	Credential Validation
Audit Failure	3/18/2024 6:12:13 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:13 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:12 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:06 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:06 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:06 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:06 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:05 AM	Microsoft Windows security auditi...	4625	Logon
Audit Success	3/18/2024 6:12:02 AM	Microsoft Windows security auditi...	5061	System Integrity
Audit Success	3/18/2024 6:12:02 AM	Microsoft Windows security auditi...	5058	Other System Events
Audit Success	3/17/2024 10:48:52 PM	Microsoft Windows security auditi...	4672	Special Logon
Audit Success	3/17/2024 10:48:52 PM	Microsoft Windows security auditi...	4624	Logon
Audit Success	3/17/2024 10:44:09 PM	Microsoft Windows security auditi...	4799	Security Group Management

Investigating Remote Brute Forcing

To determine the login failed in SIEM

```
agent.ip : "10.2.0.3" and data.win.eventdata.logonType: 3 and data.win.system.eventID : 4625
```



```
agent.ip : "10.2.0.3" and data.win.eventdata.logonType: 3 and data.win.system.eventID : 4625
```

8 hits

Mar 17, 2024 @ 21:18:54.444 - Mar 18, 2024 @ 21:18:54.444

```
Mar 18, 2024 @ 18:42:14.446  agent.ip: 10.2.0.3 data.win.eventdata.logonType: 3 data.win.system.eventID: 4625 @timestamp: Mar 18, 2024 @ 18:42:14.446 agent.id: 006
agent.name: WIN-RJ403DBBMS0 data.win.eventdata.authenticationPackageName: NTLM data.win.eventdata.failureReason: %%2313
data.win.eventdata.ipAddress: 172.16.26.6 data.win.eventdata.ipPort: 0 data.win.eventdata.keyLength: 0 data.win.eventdata.logonProcessName: NtLmSsp
data.win.eventdata.processId: 0x0 data.win.eventdata.status: 0xc000006d data.win.eventdata.subjectLogonId: 0x0 data.win.eventdata.subjectUserSid: S-
1-0-0 data.win.eventdata.subStatus: 0xc000006a data.win.eventdata.targetUserName: emp01 data.win.eventdata.targetUserSid: S-1-0-0
```

Remote login activity detected

In order to carry out different offensive operations, an attacker often has to establish a initial foothold with the targeted infrastructure. RDP is one of the most frequently targeted services to obtain an initial access.

Working of Remote login

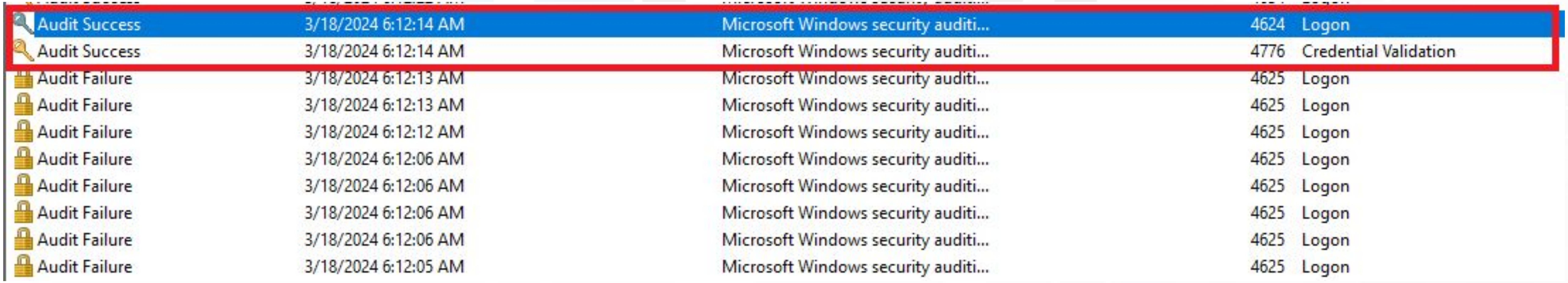
An successful RDP login will result with an **event ID 4624** with an **logon type 3**

Event ID 4624 : Generated when a account is been successfully logged in

Logon Type 03 : Logon Type 3 refers to a specific type of logon event in the Windows Event Log that indicates a network logon.

Investigating Remote login activity

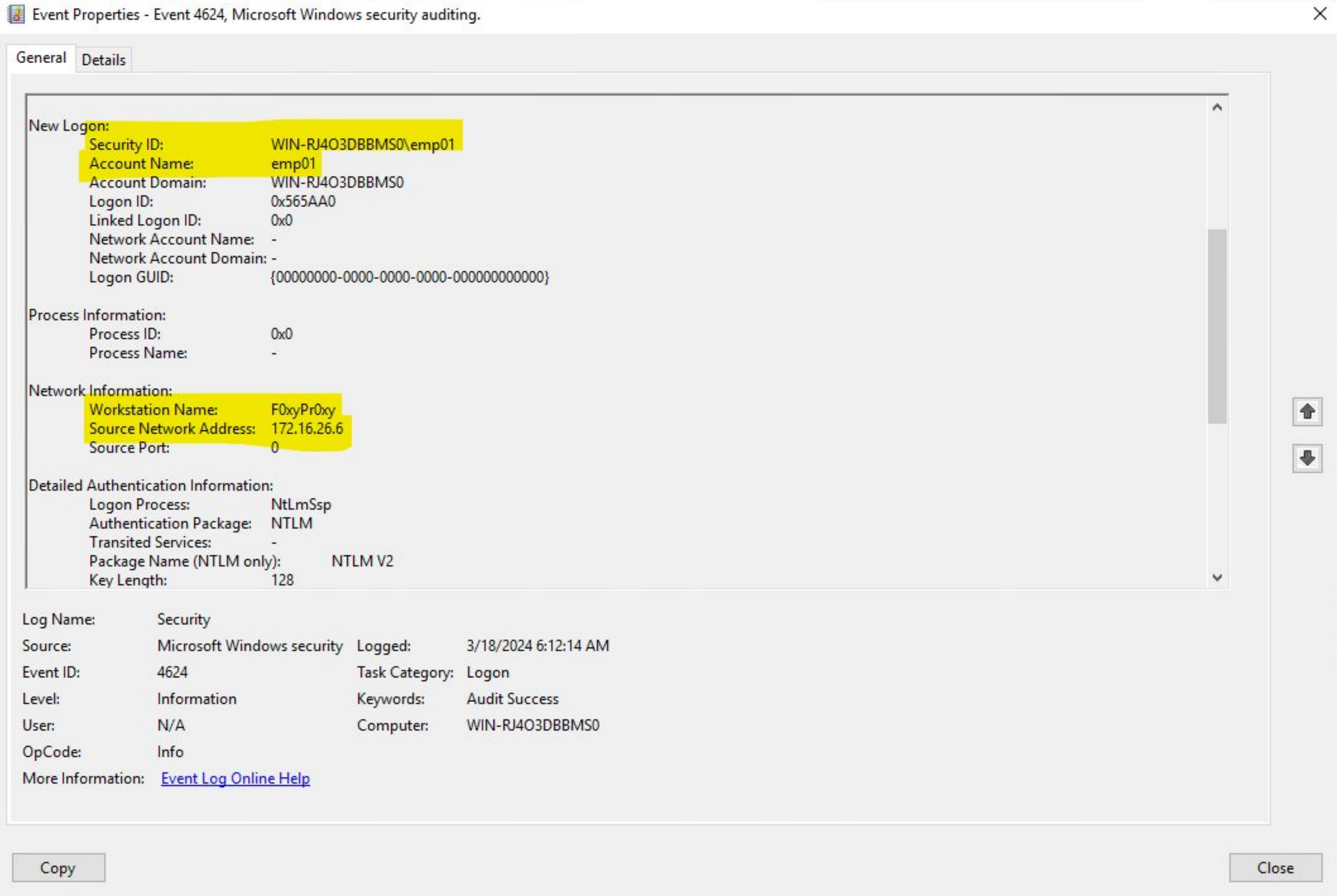
The most effective way to look into the remote login is to use event viewer to correlate the events when credential validation and logon success are seen following after logon failure event. This indicates that the attacker used brute force to input the valid credentials.



Audit Success	3/18/2024 6:12:14 AM	Microsoft Windows security auditi...	4624	Logon
Audit Success	3/18/2024 6:12:14 AM	Microsoft Windows security auditi...	4776	Credential Validation
Audit Failure	3/18/2024 6:12:13 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:13 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:12 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:06 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:06 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:06 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:06 AM	Microsoft Windows security auditi...	4625	Logon
Audit Failure	3/18/2024 6:12:05 AM	Microsoft Windows security auditi...	4625	Logon

Investigating Remote login activity

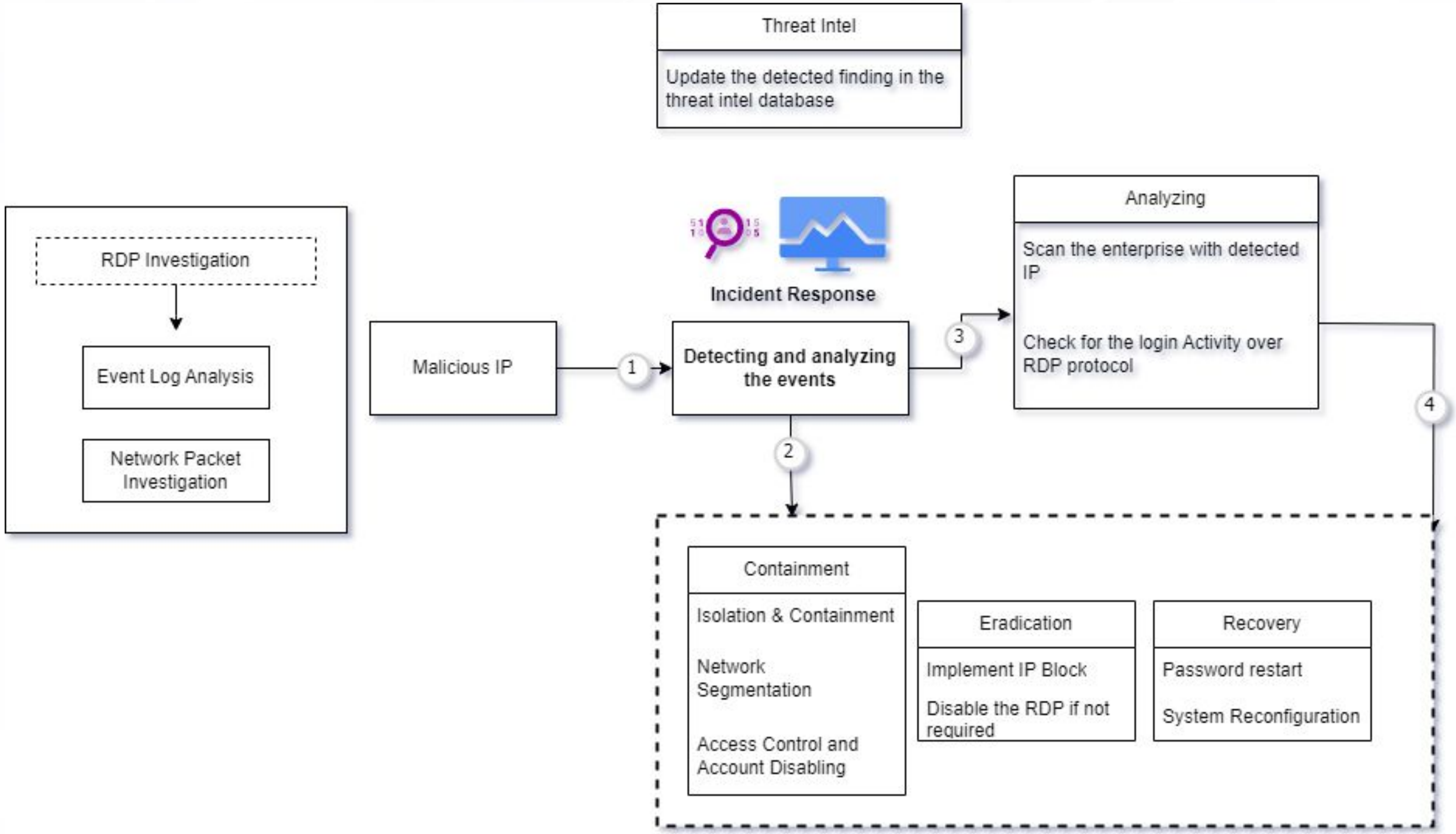
While deep investigating we observed that the external IP is been successfully logged in to the targeted victim.


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Copy
Close

```
New Logon:
        Security ID:                WIN-RJ4O3DBBMS0\emp01
        Account Name:               emp01
        Account Domain:             WIN-RJ4O3DBBMS0
        Logon ID:                   0x565AA0
        Linked Logon ID:            0x0
        Network Account Name:       -
        Network Account Domain: -
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:                 0x0
        Process Name:               -

Network Information:
        Workstation Name:           F0xyPr0xy
        Source Network Address:     172.16.26.6
        Source Port:                0

Detailed Authentication Information:
        Logon Process:              NtLmSsp
        Authentication Package:     NTLM
        Transited Services:         -
        Package Name (NTLM only):           NTLM V2
        Key Length:                 128
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         3/18/2024 6:12:14 AM
Event ID:          4624                         Task Category:  Logon
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       WIN-RJ4O3DBBMS0
OpCode:            Info
More Information:  Event Log Online Help
```

IR plan for malicious Remote Logon event



Threat Intel

Update the detected finding in the threat intel database

RDP Investigation

Event Log Analysis

Network Packet Investigation

Malicious IP

Incident Response

Detecting and analyzing the events

Analyzing

Scan the enterprise with detected IP

Check for the login Activity over RDP protocol

Containment

Isolation & Containment

Network Segmentation

Access Control and Account Disabling

Eradication

Implement IP Block

Disable the RDP if not required

Recovery

Password restart

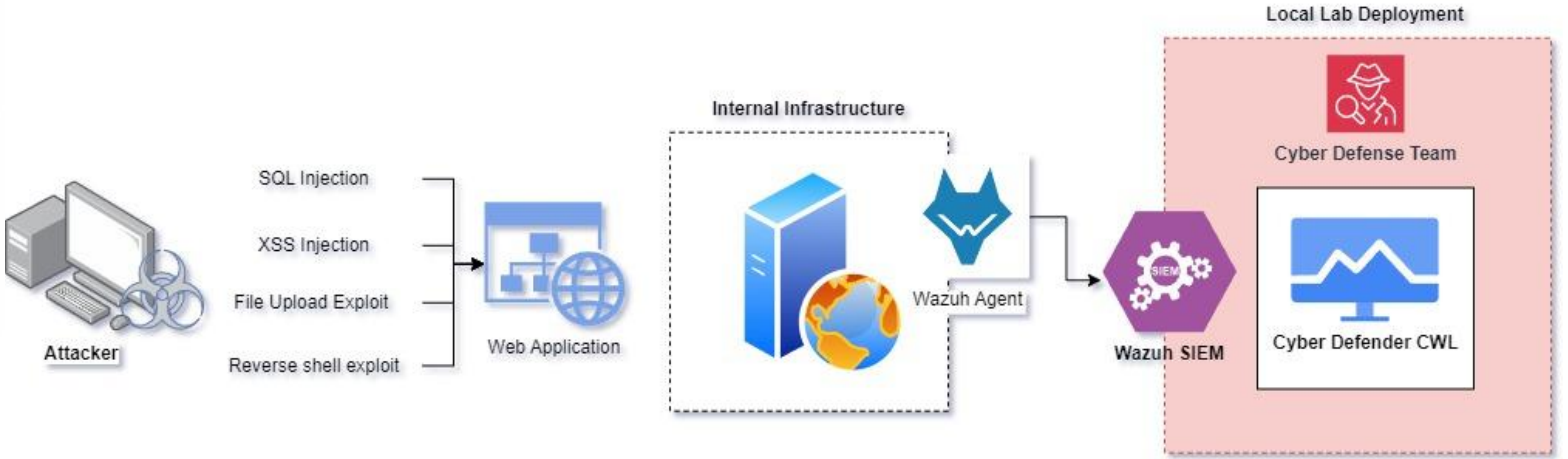
System Reconfiguration

Blue Team Fundamentals : BTF

BTF offers an organised way to start your **blue teaming experience.** This course is specifically made for beginners to provide them with the knowledge and skills needed to began their blue teaming journey.

- Working of Cyber defence
- Enhance the real time investigation skills
- Hands-on investigations
- Local Lab Deployment
- Multiple Investigative mind map
- Custom SIEM search query

BTF Lab Overview



Challenges Included:

We the team CWL has been specifically designed the **Blue Team Fundamentals** to Enhance the real time investigation skills for the cyber defenders to adapt to the evolving threat landscape and effectively safeguard organizations against cyber attacks

BTF consist of 5 unique investigative challenges based on the real case scenarios

SQL Injection Based Investigation

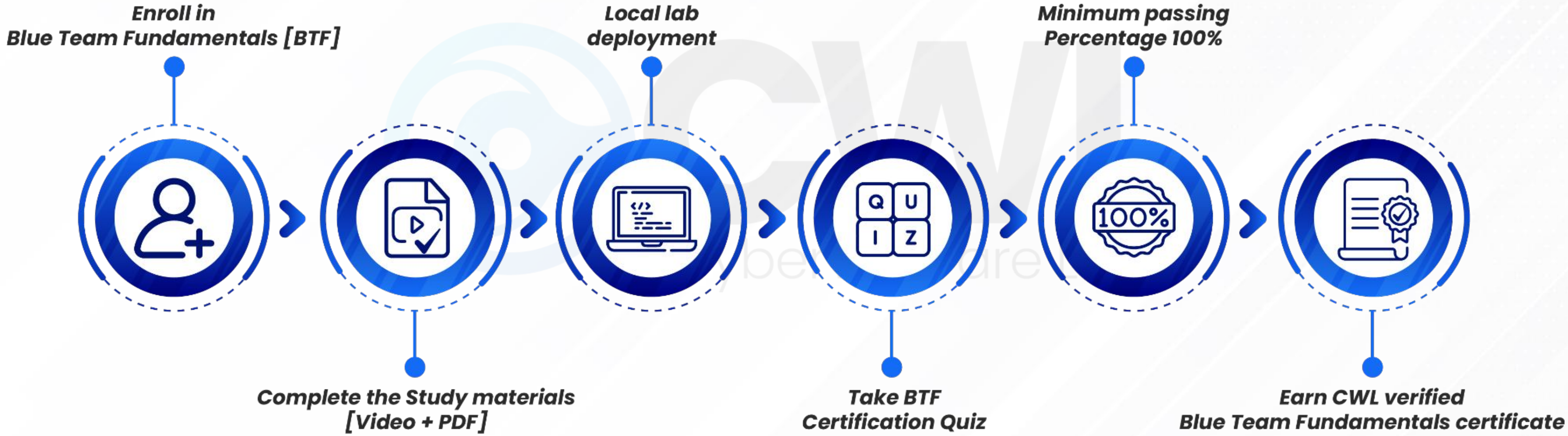
XSS Based Investigation

Remote File Inclusion Activity Investigation

External Network Communication Investigation

Compromised Host Machine : Memory Dump Analysis

Certification Procedure



Enroll in
Blue Team Fundamentals [BTF]

Complete the Study materials
[Video + PDF]

Local lab
deployment

Take BTF
Certification Quiz

Minimum passing
Percentage 100%

Earn CWL verified
Blue Team Fundamentals certificate

Detection Lab

- The objective of this course is to provide participants with a simulated real world enterprise infrastructure, where participants can engage in various investigation and defensive operations.
- The lab deployment instruction will contains a well documented PDF for local installation and configuration,
- Participants will be guided through step-by-step procedure in both identification and detection operation

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings, please contact

support@cyberwarfare.live

To know more about our offerings, please visit: https://cyberwarfare.live