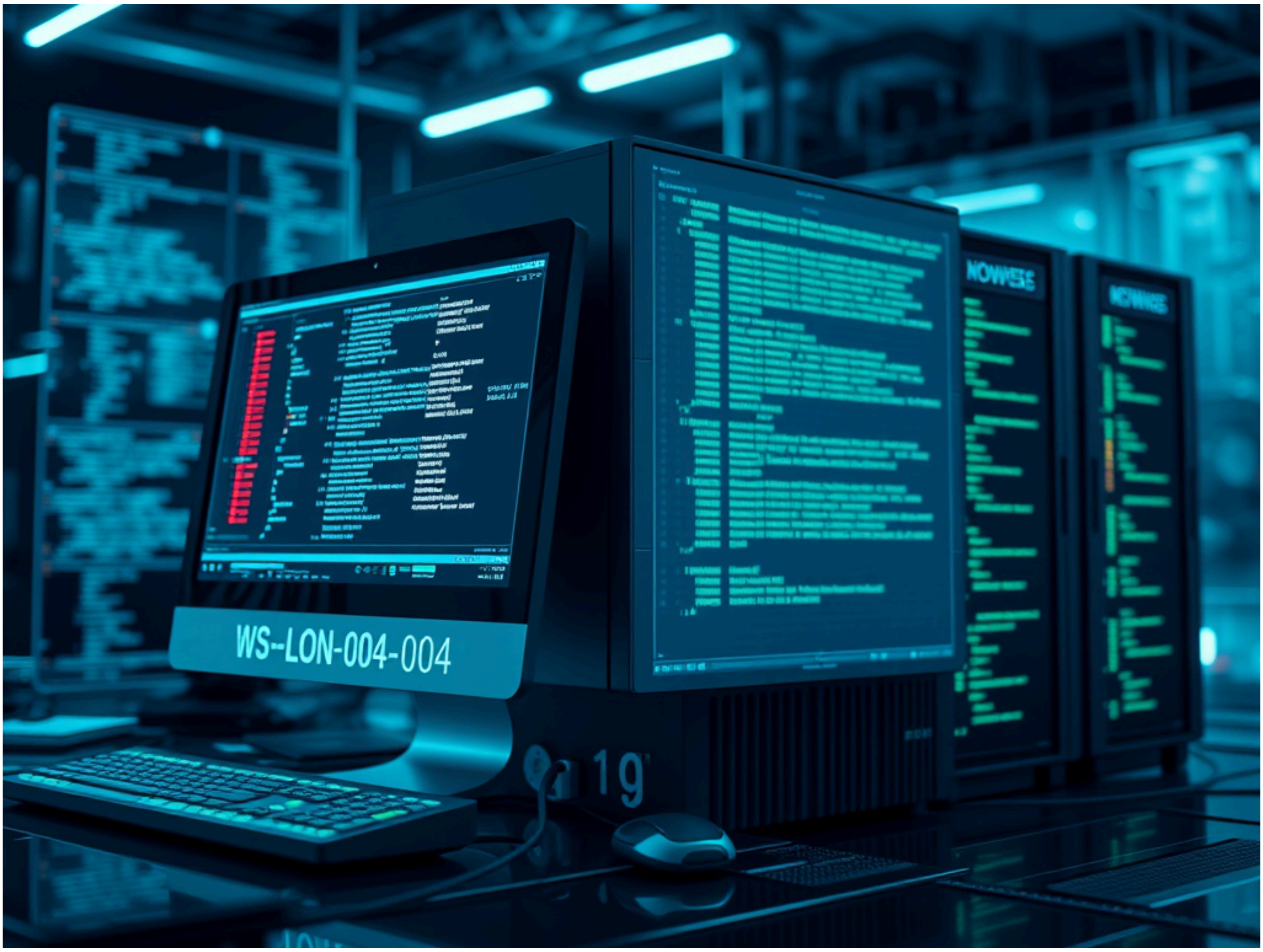
Just another island on the internet

Despair leads to boredom, electronic games, computer hacking, poetry and other bad habits.

WRITTEN BY SIMON2025-01-09

Answers for the TryHackMe Baselines and Anomalies Room

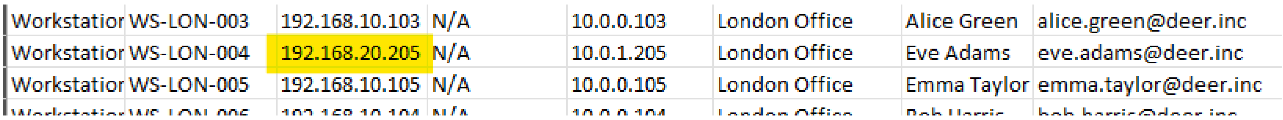


The TryHackMe Baselines and Anomalies room is a subscriber only room. In it, we learn the theory of baselines and what can be an anomaly and then move on to do investigating Anomalies in logs with ELK. This room can be accessed at: https://tryhackme.com/r/room/baselineanomalies

(https://tryhackme.com/r/room/baselineanomalies)

1.1 What is the name of the workstation that has the anomalous IP address?

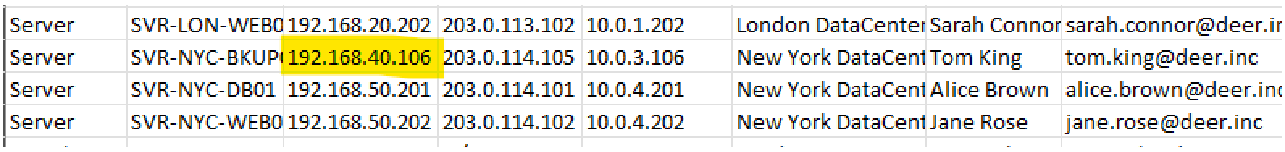
Answer: WS-LON-004



Workstatior	WS-LON-003	192.168.10.103	N/A	10.0.0.103	London Office	Alice Green	alice.green@deer.inc
Workstatior	WS-LON-004	192.168.20.205	N/A	10.0.1.205	London Office	Eve Adams	eve.adams@deer.inc
Workstatior	WS-LON-005	192.168.10.105	N/A	10.0.0.105	London Office	Emma Taylor	emma.taylor@deer.inc
Workstatior	WS-LON-006	192.168.10.104	N/A	10.0.0.104	London Office	Bob Harris	bob.harris@deer.inc

1.2 What is the name of the server with the anomalous IP address?

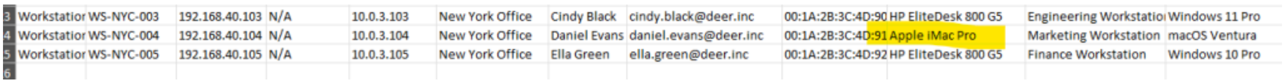
Answer: SVR-NYC-BKUP01



Server	SVR-LON-WEB0	192.168.20.202	203.0.113.102	10.0.1.202	London DataCentei	Sarah Connor	sarah.connor@deer.ir
Server	SVR-NYC-BKUPI	192.168.40.106	203.0.114.105	10.0.3.106	New York DataCent	Tom King	tom.king@deer.inc
Server	SVR-NYC-DB01	192.168.50.201	203.0.114.101	10.0.4.201	New York DataCent	Alice Brown	alice.brown@deer.in(
Server	SVR-NYC-WEB0	192.168.50.202	203.0.114.102	10.0.4.202	New York DataCent	Jane Rose	jane.rose@deer.inc

1.3 Which workstation has a device model different from the rest?

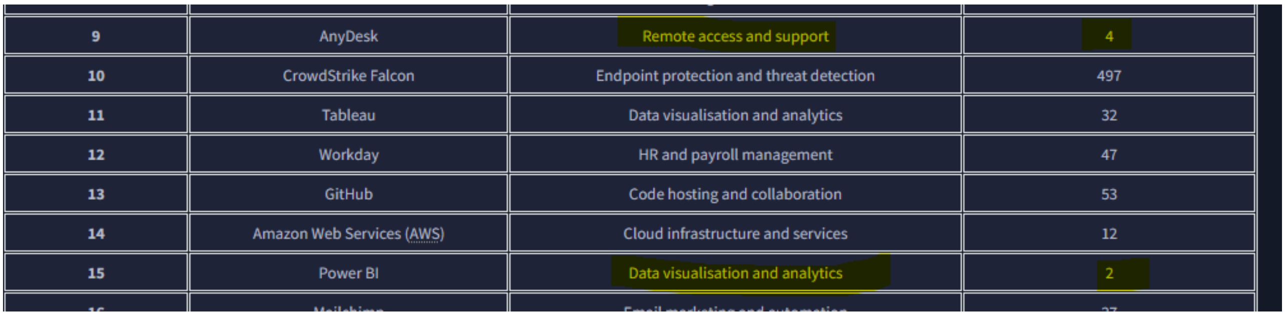
Answer: WS-NYC-004



3	Workstatior	WS-NYC-003	192.168.40.103	N/A	10.0.3.103	New York Office	Cindy Black	cindy.black@deer.inc	00:1A:2B:3C:4D:90	HP EliteDesk 800 G5	Engineering Workstatio	Windows 11 Pro
4	Workstatior	WS-NYC-004	192.168.40.104	N/A	10.0.3.104	New York Office	Daniel Evans	daniel.evans@deer.inc	00:1A:2B:3C:4D:91	Apple iMac Pro	Marketing Workstation	macOS Ventura
5	Workstatior	WS-NYC-005	192.168.40.105	N/A	10.0.3.105	New York Office	Ella Green	ella.green@deer.inc	00:1A:2B:3C:4D:92	HP EliteDesk 800 G5	Finance Workstation	Windows 10 Pro
6												

2.1 There are two installed software programs that should not be included in Anna's list. Which ones are they? Share their serial numbers. Answer format: X, Y

Answer: 9, 15



9	AnyDesk	Remote access and support	4
10	CrowdStrike Falcon	Endpoint protection and threat detection	497
11	Tableau	Data visualisation and analytics	32
12	Workday	HR and payroll management	47
13	GitHub	Code hosting and collaboration	53
14	Amazon Web Services (AWS)	Cloud infrastructure and services	12
15	Power BI	Data visualisation and analytics	2
16	Mailchimp	Email marketing and automation	27

3.1 When trying to identify if an activity was performed by the administrator or not, what is the biggest tool that a defender can use?

Answer: communication

3.2 Which process can be used to track and approve changes to the firewall Access Control List?

Answer: Change Management and Approvals

4.1 If we are looking for DNS traffic bypassing the local DNS server, what should we exclude from the search of all queries to the DNS port?

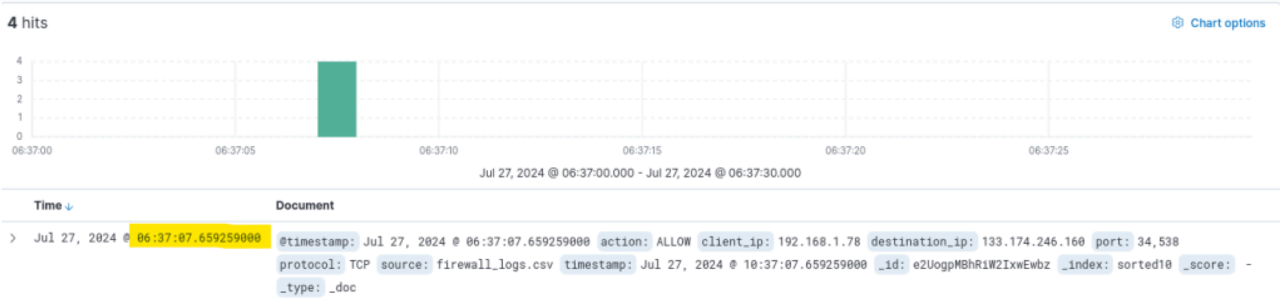
Answer: Internal DNS server

5.1 What kind of alert should be generated if a user logs in from two vastly geographically different places in a short amount of time?

Answer: Impossible travel

6.1 You have been alerted of a login outside of normal office hours on the 27th of July, 2024. Can you identify the time this login happened?

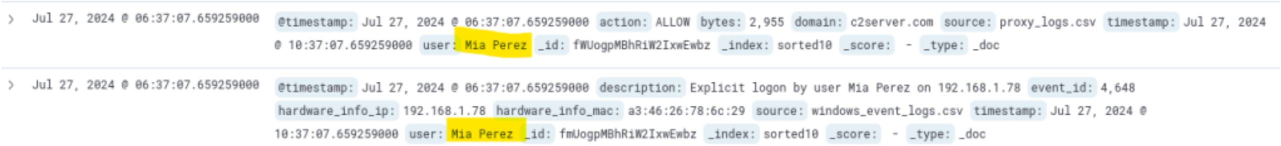
Answer: 06:37:07.659259000



```
> Jul 27, 2024 @ 06:37:07.659259000 @timestamp: Jul 27, 2024 @ 06:37:07.659259000 action: ALLOW client_ip: 192.168.1.78 destination_ip: 133.174.246.160 port: 34,538
protocol: TCP source: firewall_logs.csv timestamp: Jul 27, 2024 @ 10:37:07.659259000 _id: e2UogpMBhRiW2IxwEwbz _index: sorted10 _score: -
_type: _doc
```

6.2 Which user logged in at this time?

Answer: Mia Perez

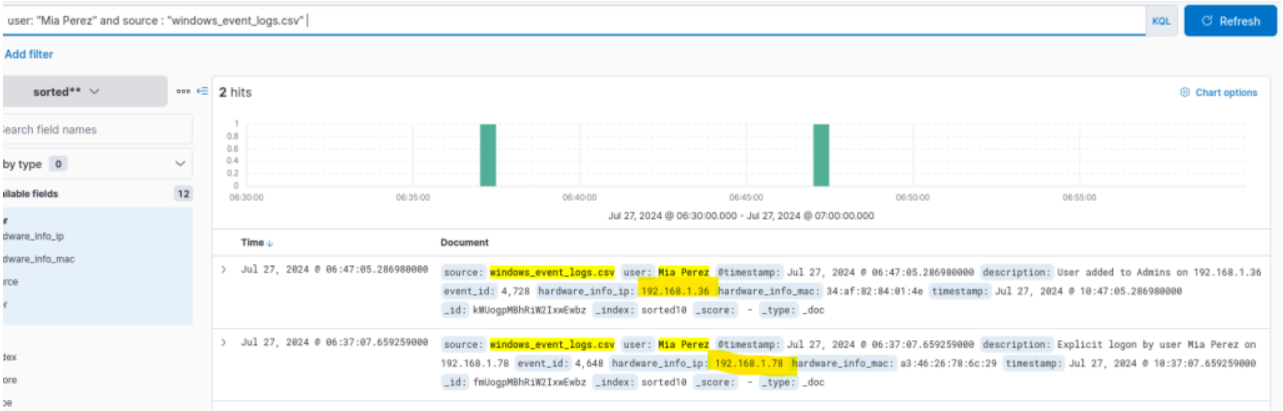


```
> Jul 27, 2024 @ 06:37:07.659259000 @timestamp: Jul 27, 2024 @ 06:37:07.659259000 action: ALLOW bytes: 2,955 domain: c2server.com source: proxy_logs.csv timestamp: Jul 27, 2024
@ 10:37:07.659259000 user: Mia Perez _id: fWUogpMBhRiW2IxwEwbz _index: sorted10 _score: - _type: _doc

> Jul 27, 2024 @ 06:37:07.659259000 @timestamp: Jul 27, 2024 @ 06:37:07.659259000 description: Explicit logon by user Mia Perez on 192.168.1.78 event_id: 4,648
hardware_info_ip: 192.168.1.78 hardware_info_mac: a3:46:26:78:6c:29 source: windows_event_logs.csv timestamp: Jul 27, 2024 @
10:37:07.659259000 user: Mia Perez _id: fmUogpMBhRiW2IxwEwbz _index: sorted10 _score: - _type: _doc
```

6.3 This user performed anomalous activities from two different machines; what is the IP address of the other machine?

Answer: 192.168.1.36



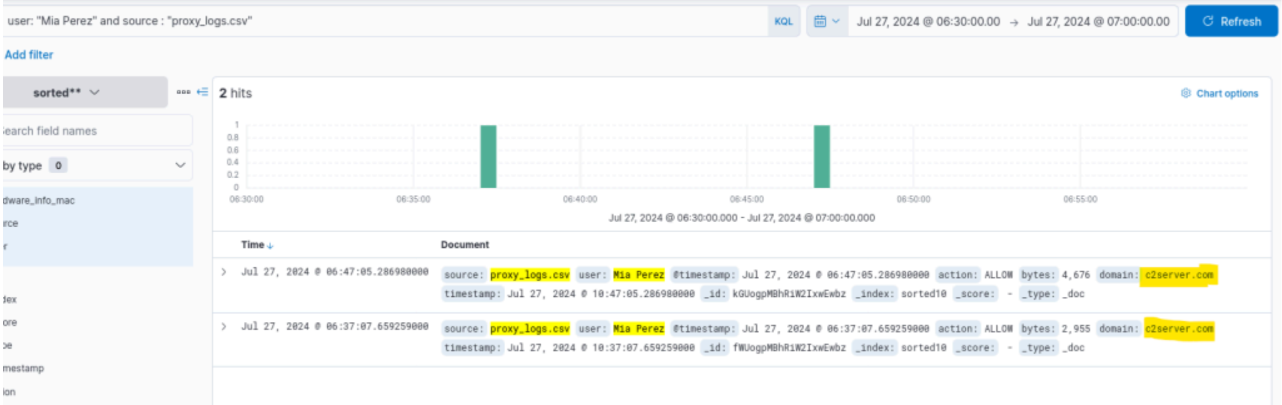
```
user: "Mia Perez" and source : "windows_event_logs.csv"
```

```
> Jul 27, 2024 @ 06:47:05.286980000 source: windows_event_logs.csv user: Mia Perez @timestamp: Jul 27, 2024 @ 06:47:05.286980000 description: User added to Admins on 192.168.1.36
event_id: 4,728 hardware_info_ip: 192.168.1.36 hardware_info_mac: 34:af:82:84:01:4e timestamp: Jul 27, 2024 @ 10:47:05.286980000
_id: kWUogpMBhRiW2IxwEwbz _index: sorted10 _score: - _type: _doc

> Jul 27, 2024 @ 06:37:07.659259000 source: windows_event_logs.csv user: Mia Perez @timestamp: Jul 27, 2024 @ 06:37:07.659259000 description: Explicit logon by user Mia Perez on
192.168.1.78 event_id: 4,648 hardware_info_ip: 192.168.1.78 hardware_info_mac: a3:46:26:78:6c:29 timestamp: Jul 27, 2024 @ 10:37:07.659259000
_id: fmUogpMBhRiW2IxwEwbz _index: sorted10 _score: - _type: _doc
```

6.4 What suspicious domain does this user connect to?

Answer: c2server.com



```
user: "Mia Perez" and source : "proxy_logs.csv"
```

Jul 27, 2024 @ 06:30:00.00 → Jul 27, 2024 @ 07:00:00.00

2 hits

Jul 27, 2024 @ 06:30:00.000 - Jul 27, 2024 @ 07:00:00.000

```
Time ↓                            Document
> Jul 27, 2024 @ 06:47:05.286980000   source: proxy_logs.csv user: Mia Perez @timestamp: Jul 27, 2024 @ 06:47:05.286980000 action: ALLOW bytes: 4,676 domain: c2server.com
                                      timestamp: Jul 27, 2024 @ 10:47:05.286980000 _id: kGUogpMBhRiW2IxwEwbz _index: sorted10 _score: - _type: _doc
> Jul 27, 2024 @ 06:37:07.659259000   source: proxy_logs.csv user: Mia Perez @timestamp: Jul 27, 2024 @ 06:37:07.659259000 action: ALLOW bytes: 2,955 domain: c2server.com
                                      timestamp: Jul 27, 2024 @ 10:37:07.659259000 _id: fWUogpMBhRiW2IxwEwbz _index: sorted10 _score: - _type: _doc
```

POSTED IN ANSWERS, TRYHACKME.TAGGED ANSWERS, CYBERSECURITY, ELK, LOGS, SECURITY, SIEM, SOC, TRYHACKME.

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Website Powered by WordPress.com.