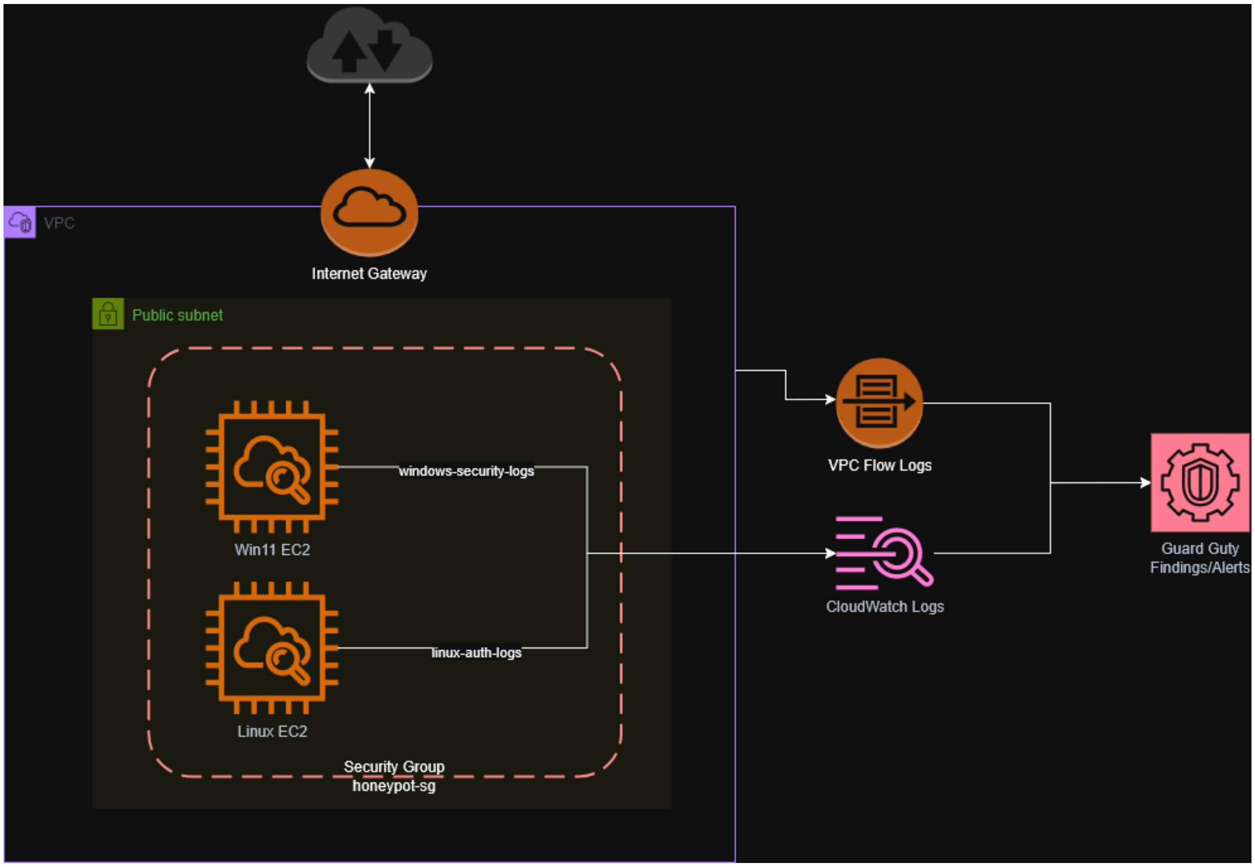
1. Architecture Diagram



2. Log Sources Section

Network Logs

- VPC Flow Logs

Host Logs

- Linux auth logs
- Windows Security logs

Detection Sources

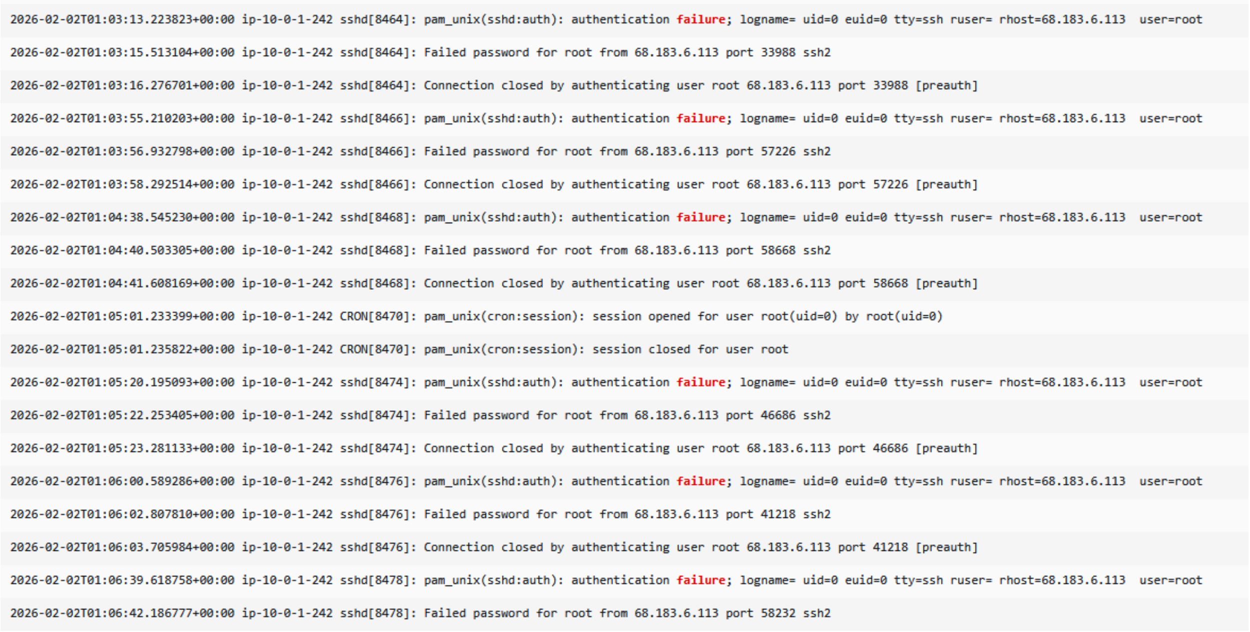
- GuardDuty findings

Purpose of each

Explain what each log detects:

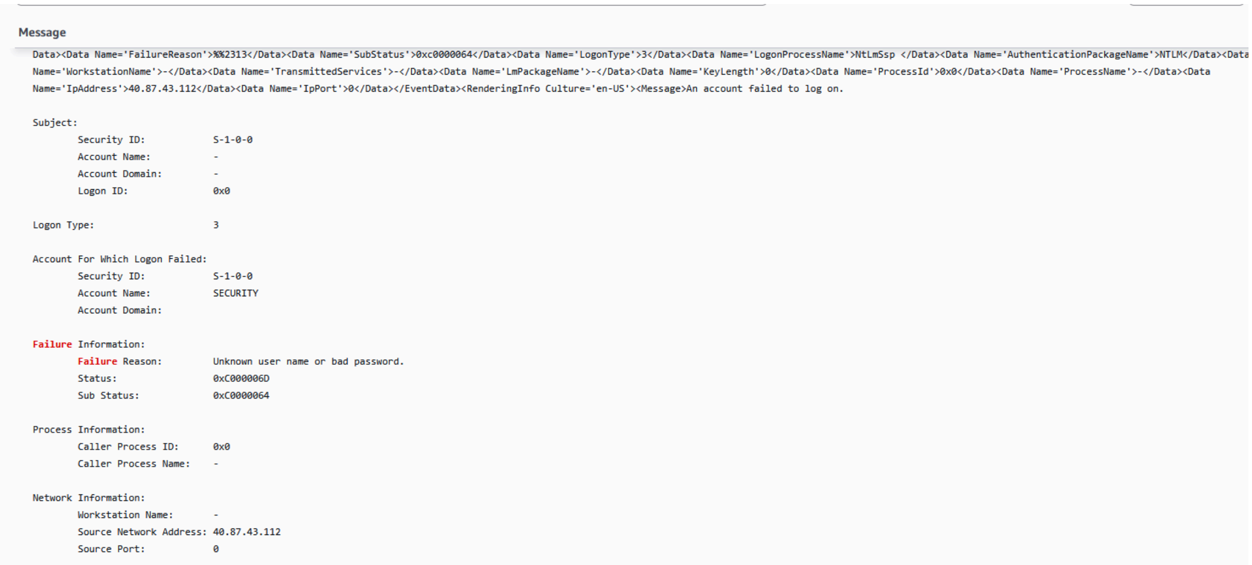
Log	Detects
Flow Logs	scanning and connections
Linux auth	SSH brute force
Windows log	RDP brute force
GuardDuty	Behavioral threats

3. Sample Findings



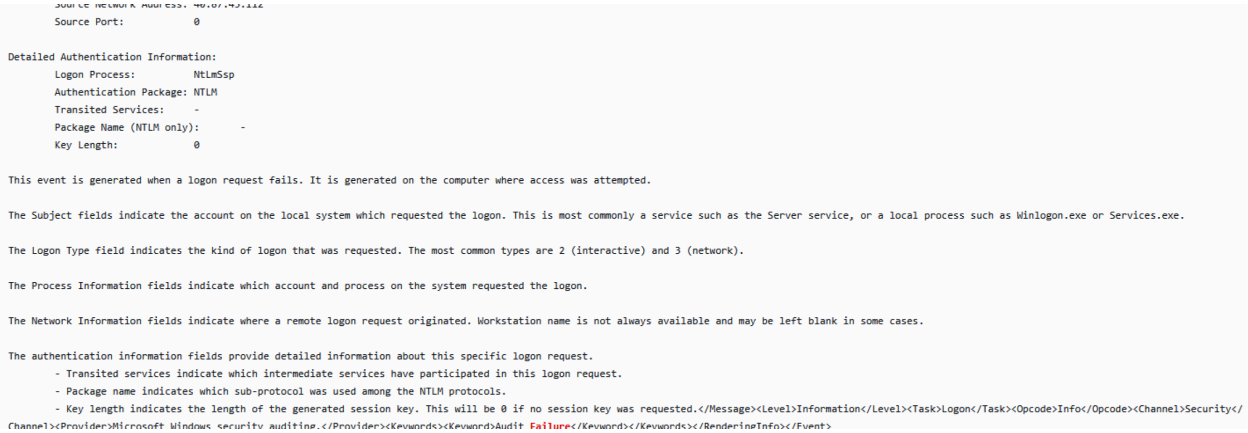
```
2026-02-02T01:03:13.223823+00:00 ip-10-0-1-242 sshd[8464]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=68.183.6.113  user=root
2026-02-02T01:03:15.513104+00:00 ip-10-0-1-242 sshd[8464]: Failed password for root from 68.183.6.113 port 33988 ssh2
2026-02-02T01:03:16.276701+00:00 ip-10-0-1-242 sshd[8464]: Connection closed by authenticating user root 68.183.6.113 port 33988 [preauth]
2026-02-02T01:03:55.210203+00:00 ip-10-0-1-242 sshd[8466]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=68.183.6.113  user=root
2026-02-02T01:03:56.932798+00:00 ip-10-0-1-242 sshd[8466]: Failed password for root from 68.183.6.113 port 57226 ssh2
2026-02-02T01:03:58.292514+00:00 ip-10-0-1-242 sshd[8466]: Connection closed by authenticating user root 68.183.6.113 port 57226 [preauth]
2026-02-02T01:04:38.545230+00:00 ip-10-0-1-242 sshd[8468]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=68.183.6.113  user=root
2026-02-02T01:04:40.503305+00:00 ip-10-0-1-242 sshd[8468]: Failed password for root from 68.183.6.113 port 58668 ssh2
2026-02-02T01:04:41.608169+00:00 ip-10-0-1-242 sshd[8468]: Connection closed by authenticating user root 68.183.6.113 port 58668 [preauth]
2026-02-02T01:05:01.233399+00:00 ip-10-0-1-242 CRON[8470]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-02T01:05:01.235822+00:00 ip-10-0-1-242 CRON[8470]: pam_unix(cron:session): session closed for user root
2026-02-02T01:05:20.195093+00:00 ip-10-0-1-242 sshd[8474]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=68.183.6.113  user=root
2026-02-02T01:05:22.253405+00:00 ip-10-0-1-242 sshd[8474]: Failed password for root from 68.183.6.113 port 46686 ssh2
2026-02-02T01:05:23.281133+00:00 ip-10-0-1-242 sshd[8474]: Connection closed by authenticating user root 68.183.6.113 port 46686 [preauth]
2026-02-02T01:06:00.589286+00:00 ip-10-0-1-242 sshd[8476]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=68.183.6.113  user=root
2026-02-02T01:06:02.807810+00:00 ip-10-0-1-242 sshd[8476]: Failed password for root from 68.183.6.113 port 41218 ssh2
2026-02-02T01:06:03.705984+00:00 ip-10-0-1-242 sshd[8476]: Connection closed by authenticating user root 68.183.6.113 port 41218 [preauth]
2026-02-02T01:06:39.618758+00:00 ip-10-0-1-242 sshd[8478]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=68.183.6.113  user=root
2026-02-02T01:06:42.186777+00:00 ip-10-0-1-242 sshd[8478]: Failed password for root from 68.183.6.113 port 58232 ssh2
```

Multiple failed SSH attempts from 68.183.6.113 indicate automated credential spraying.



Message

```
Data><Data Name='FailureReason'>%%2313</Data><Data Name='SubStatus'>0xc0000064</Data><Data Name='LogonType'>3</Data><Data Name='LogonProcessName'>NtLmSsp </Data><Data Name='AuthenticationPackageName'>NTLM</Data><Data
Name='WorkstationName'>-</Data><Data Name='TransmittedServices'>-</Data><Data Name='LmPackageName'>-</Data><Data Name='KeyLength'>0</Data><Data Name='ProcessId'>0x0</Data><Data Name='ProcessName'>-</Data><Data
Name='IpAddress'>40.87.43.112</Data><Data Name='IpPort'>0</Data></EventData><RenderingInfo Culture='en-US'><Message>An account failed to log on.

Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

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

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC0000064

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

Network Information:
        Workstation Name:       -
        Source Network Address: 40.87.43.112
        Source Port:            0
```



```
        Source Network Address: 40.87.43.112
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).

The Process Information fields indicate which account and process on the system requested the logon.

The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The authentication information fields provide detailed information about this specific logon request.
        - Transited services indicate which intermediate services have participated in this logon request.
        - Package name indicates which sub-protocol was used among the NTLM protocols.
        - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.</Message><Level>Information</Level><Task>Logon</Task><Opcode>Info</Opcode><Channel>Security</
Channel><Provider>Microsoft Windows security auditing.</Provider><Keywords><Keyword>Audit Failure</Keyword></Keywords></RenderingInfo></Event>
```

Multiple failed RDP attempts from 40.87.43.112 indicate automated credential spraying.

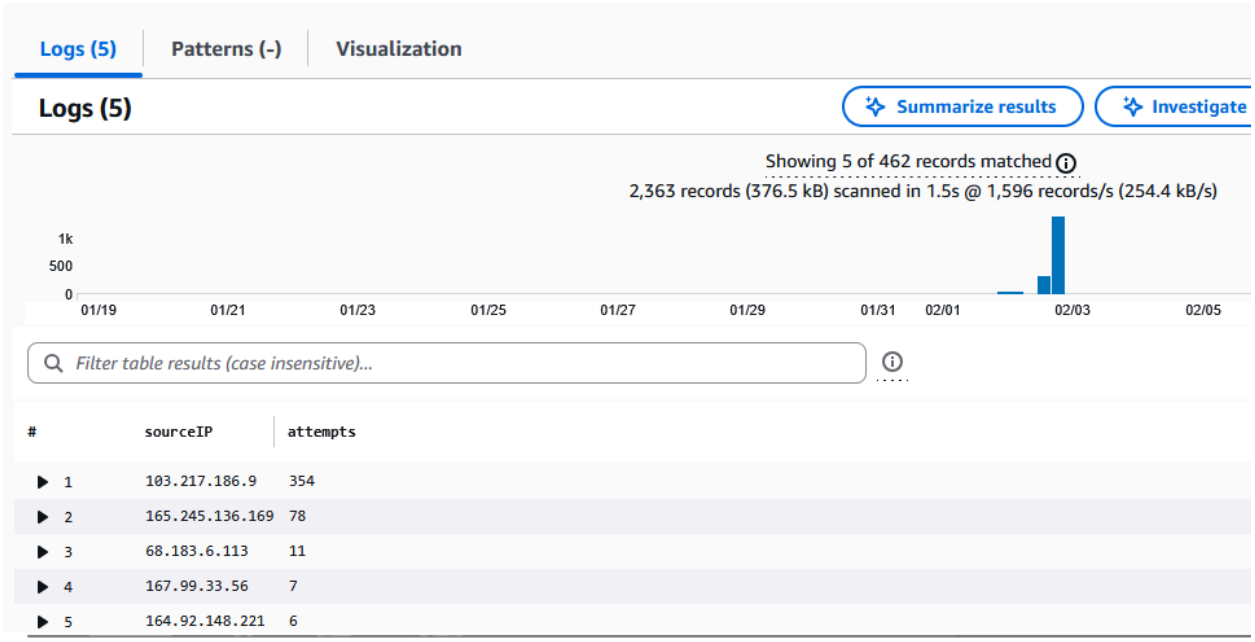
4. Detection Queries

Detection Name: Linux SSH brute-force detection

Purpose: Detect repeated failed SSH attempts

Query:

```
fields @timestamp, @message
| filter @message like "Failed password"
| parse @message "* from * port *" as user, sourceIP, port
| stats count() as attempts by sourceIP
| filter attempts > 5
| sort attempts desc
```



Showing 5 of 462 records matched

2,363 records (376.5 kB) scanned in 1.5s @ 1,596 records/s (254.4 kB/s)

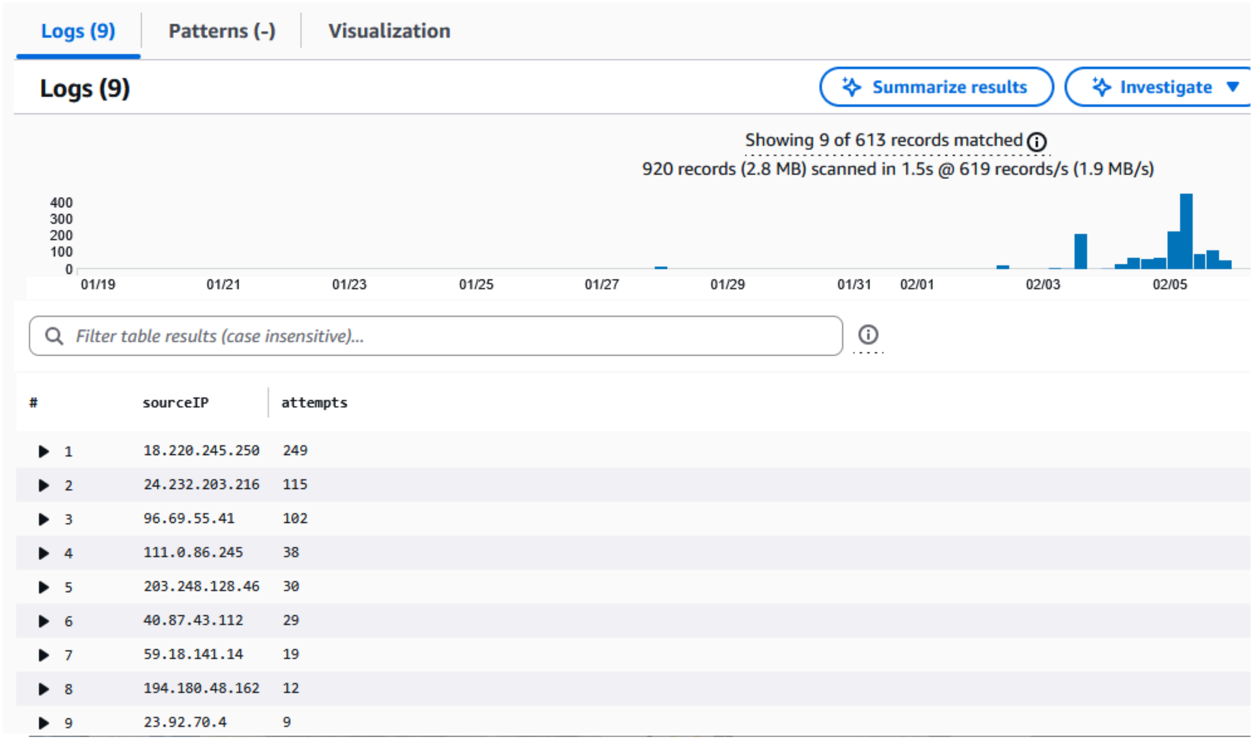
#	sourceIP	attempts
1	103.217.186.9	354
2	165.245.136.169	78
3	68.183.6.113	11
4	167.99.33.56	7
5	164.92.148.221	6

Detection Name: Windows RDP brute-force detection

Purpose: Detect repeated failed RDP attempts

Query:

```
fields @timestamp, @message
| filter @message like "4625"
| parse @message /Source Network Address:\s+(?<sourceIP>[0-9.]+)/
| stats count() as attempts by sourceIP
| filter attempts > 5
| sort attempts desc
```



Logs (9)

Showing 9 of 613 records matched

920 records (2.8 MB) scanned in 1.5s @ 619 records/s (1.9 MB/s)

Filter table results (case insensitive)...

#	sourceIP	attempts
1	18.220.245.250	249
2	24.232.203.216	115
3	96.69.55.41	102
4	111.0.86.245	38
5	203.248.128.46	30
6	40.87.43.112	29
7	59.18.141.14	19
8	194.180.48.162	12
9	23.92.70.4	9

5. Incident Timeline

Time	Event
2026-02-02T01:02:32.040535+00:00	sshd[8462]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=68.183.6.113 user=root
2026-02-02T01:02:33.702825+00:00	sshd[8462]: Failed password for root from 68.183.6.113 port 47104 ssh2
2026-02-02T01:05:20.195093+00:00	sshd[8474]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=68.183.6.113 user=root
2026-02-02T01:05:22.253405+00:00	sshd[8474]: Failed password for root from 68.183.6.113 port 46686 ssh2