

Eagle SOC

Login activity analysis report

Thanuka Thathsara
SOC Tier 1

23/12/2024

Case

You have been hired by Eagle as a SOC Tier 1 analyst. Yesterday was your on-boarding day with the company, and today you will be familiarized with the SOC. Your day will begin by meeting up with a senior analyst, who will provide insights into the environment, and afterwards, you are expected to begin monitoring alerts and security events in our home-cooked SOC dashboards.

The following are your notes after meeting the senior analyst, who provided insights into the environment:

Eagle IT security Policy

- All hosting has moved to the cloud; old DMZ network is shut down.
- Core IT team includes 4 admins with high privileges.
- Admins frequently use default administrator accounts (against best practices).
- Endpoints are hardened using CIS baselines; limited application whitelisting in place.
- A Privileged Admin Workstation (PAW) is required for all admin tasks.
- Legacy Linux servers are still present but rarely used.
 - Root access is disabled remotely due to audit issues.
 - Admin access must be gained via sudo.
- Strict naming conventions are enforced:
 - Service accounts include “-svc” in their names.
 - Service accounts have strong, complex passwords and limited roles.

Task - Analyze user login behavior for suspicious activity, policy violations, or areas needing escalation

IT Security Posture Review

- **Overall Setup**
 - Everything is in the cloud now — no physical servers or DMZ (demilitarized zone) anymore, so less risk from on-premise attacks.
 - **IT Admins**
 - There are only 4 core IT admins, and they are the only ones with high privileges. *Problem: They often use default admin accounts, even when told not to. This is risky because default accounts are predictable and easier to exploit.*
 - **Device & Access Security**
 - All end-user devices follow CIS hardening guidelines (which makes them more secure).
Whitelisting (only allowing approved apps to run) is only partially used, which leaves room for some risk.
 - **Admin Workstation (PAW)**
 - A Privileged Admin Workstation (PAW) was created by IT Security. All admin tasks must be done on this secure machine, reducing the risk of sensitive tasks being done from less secure devices.
 - **Linux Servers**
 - Some old Linux servers are still around, but they are barely used. Root access is blocked remotely due to past audit issues. To get admin rights, users must use `sudo` instead of logging in as root. This adds a layer of control and logging.
 - **Naming & Account Rules**
 - Strict naming rules exist for accounts, especially service accounts. Example: All service accounts have “-svc” in their names. These accounts use strong passwords and only do specific tasks (like running a service).
-

Failed logon attempts [All users]

Username	Event logged by	Logon type	# of logins
PAW	DC2	Network	4
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
bob	WS001	Interactive	2
sql-svc1	PK1	Network	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1
anni	WS001	Interactive	1
eAdministrator	DC1	Network	1

Failed logon attempts [Admin users only]

Username	Event logged by	Logon type	# of logins
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1

Admin logon not from PAW Feb 28, 2023 @ 18:00:00.000 to now

User	Connect from	Count of records
Administrator	192.168.28.132	51
Administrator	192.168.28.200	8

Failed logon attempts [Disabled user]

Username	Event logged by	# of logins
anni	WS001	1

Elastic SIEM Dashboard

Log Analysis

Analysis :

Multiple logins using default **"administrator"** accounts from various machines (e.g., DC1, DC2, WSO1, PK1).

Concern :

- This violates the policy of not using default admin accounts
- IT operations team is known to ignore the guideline, but repeated usage still increases
- Could be hard to track individual accountability.

Action :

Contact IT Operations - Educate or remind them of policy violations and enforce proper account usage.

Failed Logon attempt - Consult IT OP
 Fail log at Disabled account - Escalate
 Admin user only - Nothing
 RDP - Escalate
 local group - Consult
 PAW - consult it
 SSH- Escalate

Failed logon attempts [All users]					
Username	Event logged by	Logon type		# of logins	
PAW	DC2	Network		4	
Administrator	DC1	Interactive		3	
administrator	PAW	Interactive		2	
bob	WS001	Interactive		2	
sql-svc1	PKI	Network		2	
Administrator	DC1	Unlock		1	
administrator	PAW	Unlock		1	
administrator	DC2	Interactive		1	
anni	WS001	Interactive		1	
eAdministrator	DC1	Network		1	
eagleAdministrator	DC1	Network		1	

Failed logon attempts [Disabled user]					
Username	Event logged by			# of logins	
anni	WS001			1	

Failed logon attempts [Admin users only]



Username	Event logged by	Logon type	# of logins
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1

RDP logon for service account



Username	Connect to	Connect from	# of logins
svc-sql1	PKI	192.168.28.130	2

User added or removed from a local group Mar 5, 2023 @ 18:00:00.000 to now



User performing the action	User added	Group modified	Action permed	Action performed on	Count of records
Administrator	S-1-5-21-151813...	Administrators	added-member-to-group	PKI.eagle.local	1

Admin logon not from PAW



User	Connect from	Count of records
Administrator	192.168.28.132	336
Administrator	192.168.28.130	140
Administrator	192.168.28.201	121
Administrator	192.168.28.200	46
Administrator	192.168.28.128	23
Administrator	192.168.28.131	12
Administrator	::1	6
Administrator	fe80::b1e5:895:1208:2617	3
Administrator	fe80::7832:439f:cac2:5a01	2
Administrator	fe80::da26:ad7f:80ca:8a7b	1
Admin	192.168.28.128	9
admin	192.168.28.132	3
administrator	192.168.28.128	1

SSH Logins



Action	User	Outcome	Authenticatio	From	Count of reco
ssh_login	root	Failed	password	192.168.28.1...	6