

Notes / Findings:

Timeline Summary and Findings:

“edr-andres” has been exposed/internet facing for a couple hours now. VM went live August 14 early afternoon.

```
DeviceInfo
```

















```
| where DeviceName == "edr-andres"
| where IsInternetFacing == true
| order by Timestamp desc
```

Latest TimeStamp: 2025-08-14T22:11:56.0984323Z

(August 14, 2025, 10:11:56 PM UTC)

Many remote IP's have been trying to connect to “edr-andres” impersonating as administrators all around the world. Query used:

```
let target_machine = "edr-andres";
DeviceLogonEvents
| where DeviceName == target_machine
| where ActionType == "LogonFailed"
| summarize FailedLogonCount = count() by AccountName, DeviceName, RemoteIP
| order by FailedLogonCount desc
```

Filters: Add filter					
<input type="checkbox"/>	AccountName	DeviceName	RemoteIP	LogonType	FailedLogonCount
<input type="checkbox"/>	> admin	 edr-andres	 57.129.140.32	Network	26
<input type="checkbox"/>	> administrator	 edr-andres	 27.123.9.202	Network	12
<input type="checkbox"/>	> admin	 edr-andres	 27.123.9.202	Network	12
<input type="checkbox"/>	> user	 edr-andres	 27.123.9.202	Network	12
<input type="checkbox"/>	> test	 edr-andres	 27.123.9.202	Network	12
<input type="checkbox"/>	> administrator	 edr-andres	 36.111.189.177	Network	2
<input type="checkbox"/>	> administrator	 edr-andres	 86.26.116.193	Network	2
<input type="checkbox"/>	> administrator	 edr-andres	 165.140.167.252	Network	2

Not a single previous RemoteIP's has been able to log in. Query used:

```
let RemoteIPsInQuestion = dynamic(["57.129.140.32", "27.123.9.202", "36.111.189.177",
"86.26.116.193", "165.140.167.252"]);
DeviceLogonEvents
| where LogonType has_any("Network", "Interactive", "RemoteInteractive", "Unlock")
| where ActionType == "LogonSuccess"
| where RemoteIP has_any(RemoteIPsInQuestion)
```

Results with “LogonSuccess”: None.






The only successful remote/network logons in the last 30 days was from the “irlab14#” account name which is 5 total

```
DeviceLogonEvents
| where DeviceName == "edr-andres"
| where LogonType == "Network"
| where ActionType == "LogonSuccess"
| summarize count()
```

When checking all the RemoteIP logins for Account Name “irlab14#” there's none with a suspicious or unusual location.

```
DeviceLogonEvents
| where DeviceName == "edr-andres"
| where LogonType == "Network"
| where ActionType == "LogonSuccess"
| where AccountName == "irlab14#"
| summarize LoginCount = count() by DeviceName, ActionType, AccountName, RemoteIP
```

Filters: Add filter

<input type="checkbox"/>	DeviceName	ActionType	AccountName	RemoteIP	LoginCount
<input type="checkbox"/>	>  edr-andres	LogonSuccess	irlab14#		2
<input type="checkbox"/>	>  edr-andres	LogonSuccess	irlab14#	 10.0.8.4	1
<input type="checkbox"/>	>  edr-andres	LogonSuccess	irlab14#	 10.0.8.6	2

Even with the device exposed to the internet and many brute force attempts have taken place, there is no evidence of any brute force success or unauthorized access by it. So no indicators of compromise.

Relevant MITRE ATT&CK TTPs

- T1190: Exploit Public-Facing Application
- T1078: Valid Accounts (Successful logons by legitimate account “irlab14#”)
- T1587.001: Develop Capabilities: Exploit Code (indirect inference from multiple bad actors attempting to log into my device which can be seen as reconnaissance or exploitation attempts by attackers using and/or testing their exploit tools)

Response Actions:

- Harden the NSG to allow only RDP traffic inbound which also makes it where there's no wide public internet access
- Implement Account lockout Policy
- Implement MFA

Improvements:

- Recording findings and learning from them to improve future hunts and defenses.
- Improve efficiency with KQL queries to detect anomalies faster.