Timeline Summary and Findings:

Instinct-mde-te has been internet facing for several days:

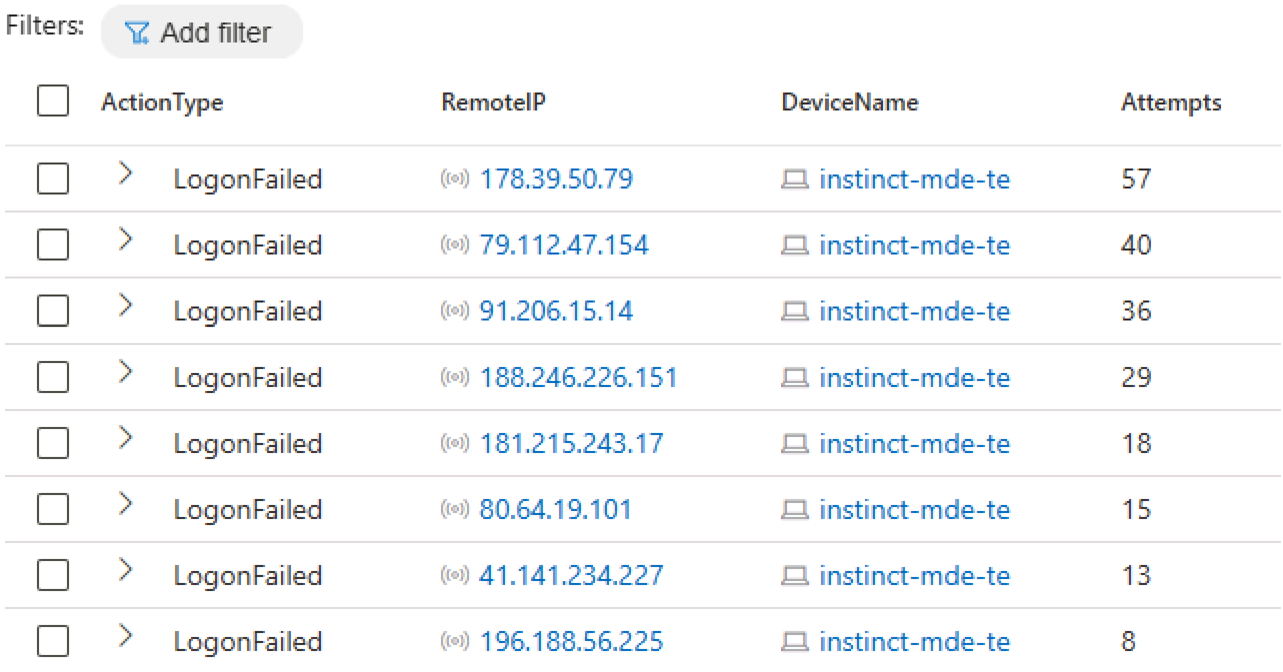
```
DeviceInfo
| where DeviceName startswith "instinct"
| where IsInternetFacing == true
| order by Timestamp desc
```

Last Internet facing time: 2025-08-11T05:58:54.16093Z

—-----

Several bad actors have been discovered attempting to log into the target machine

```
DeviceLogonEvents
| where DeviceName startswith "instinct"
| where LogonType has_any("Network", "Interactive", "RemoteInteractive", "Unlock")
| where ActionType == "LogonFailed"
| where isnotempty(RemoteIP)
| summarize Attempts = count() by ActionType, RemoteIP, DeviceName
| order by Attempts
```



□	ActionType	RemoteIP	DeviceName	Attempts
□	› LogonFailed	178.39.50.79	instinct-mde-te	57
□	› LogonFailed	79.112.47.154	instinct-mde-te	40
□	› LogonFailed	91.206.15.14	instinct-mde-te	36
□	› LogonFailed	188.246.226.151	instinct-mde-te	29
□	› LogonFailed	181.215.243.17	instinct-mde-te	18
□	› LogonFailed	80.64.19.101	instinct-mde-te	15
□	› LogonFailed	41.141.234.227	instinct-mde-te	13
□	› LogonFailed	196.188.56.225	instinct-mde-te	8

—-------

The top 7 most failed login attempt IP addresses have not been able to successfully break into the VM

```
// Take the top 10 IPs with the most logon failures and see if any succeeded to logon

let RemoteIPsInQuestion = dynamic(["178.39.50.79","79.112.47.154", "91.206.15.14",
"188.246.226.151", "181.215.243.17", "80.64.19.101", "41.141.234.227"]);
```

```
DeviceLogonEvents

| where LogonType has_any("Network", "Interactive", "RemoteInteractive", "Unlock")

| where ActionType == "LogonSuccess"

| where RemoteIP has_any(RemoteIPsInQuestion)
```

<Query no result>

—--

The only successful remote/network logons in the last 7 days was for the “Instinct” account (15 total)

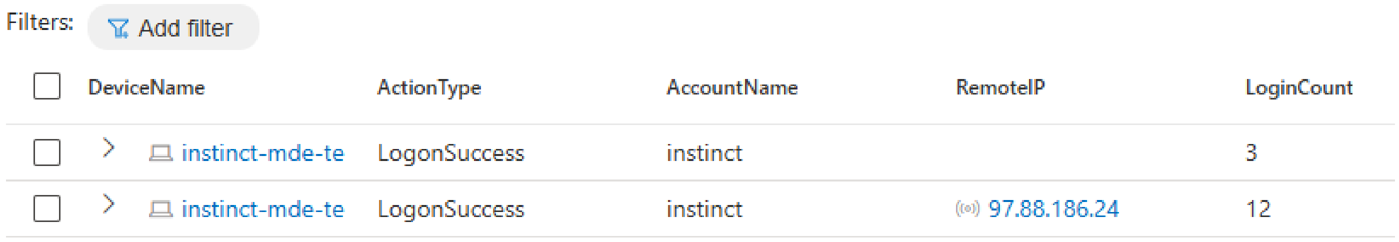
```
DeviceLogonEvents
| where DeviceName startswith "instinct"
| where LogonType == "Network"
| where ActionType == "LogonSuccess"
| where AccountName == "instinct"
| summarize count()
```

There were zero failed logons for the “instinct” account, indicating that a bruteforce attempt for this account didn’t take place, and a 1-time password guess is unlikely.

```
DeviceLogonEvents
| where DeviceName startswith "instinct"
| where LogonType == "Network"
| where ActionType == "Logonfailed"
| where AccountName == "instinct"
| summarize count()
```

We checked all of the successful IP addresses for the lab user to see if any of them were unusual or from an unexpected location. All were normal.

```
DeviceLogonEvents
| where DeviceName startswith "instinct"
| where LogonType == "Network"
| where ActionType == "LogonSuccess"
| where AccountName == "instinct"
| summarize LoginCount = count() by DeviceName, ActionType, AccountName, RemoteIP
```



□	DeviceName	ActionType	AccountName	RemoteIP	LoginCount
□	instinct-mde-te	LogonSuccess	instinct		3
□	instinct-mde-te	LogonSuccess	instinct	97.88.186.24	12

—-

Though the device was exposed to the internet and clear brute force attempts have take place, there is no evidence of any brute force success or unauthorized access from the legitimate account ‘instinct’

Relevant MITRE ATT&CK TTPs:

- T1078: Valid Accounts – Use of legitimate "Instinct" account for successful logons.

- T1110: Brute Force – Multiple failed login attempts from various external IPs.

- T1021.001: Remote Services: Remote Desktop Protocol – RemoteInteractive and Network logon attempts.

- T1030: Data Transfer Size Limits – Internet-facing system potentially enabling large or malicious data transfers (exposure risk).

- T1595: Active Scanning – Internet-facing host attracting attacker login attempts.

—----

Response Action:

- Hardened the NSG attached to instinct-mde-te to allow only RDP traffic from specific endpoints (no public internet access)
- Implemented account lockout policy
- Implemented MFA