Unauthorized VPN and VDI Access

Preparation:

In order to prepare for this incident, I patched asset vulnerabilities, performed routine inspections of controls/weapons, ensured Antivirus/Endpoint protection software is installed on workstations and laptops, prohibited non-employees from accessing company devices, ensured that all remotely accessible services are logging to a central location, provided security awareness training to employees, used multifactor authentication where possible, ensured proper network segmentation/firewall rules are in place for remote users, and routinely audit remote system access.

Investigation:

To Investigate this incident, I monitored for: remote access during unusual hours/days, remote access from unusual sources (i.e. geographic locations, IPs, etc.), excessive failed login attempts, IPS/IDS alerts, antivirus/Endpoint alerts, investigate and clear all alerts associated with the impacted assets and contacted the user out of band to determine the legitimacy of the detected activity.

Containment, Eradication and Recovery:

To contain, eradicate and recover effected inventory (enumerate & assets), I Issued perimeter enforcement for known threat actor locations, blocked access from the compromised user, locked accounts associated with the compromised user and inspected all potentially compromised systems for IOCs. To eradicate, I closed the attack vector, patched asset vulnerabilities, performed Endpoint/AV scans on affected systems, reviewed logs to determine the extent of the unauthorized activity. To recover, I restored to the RPO within the RTO, addressed collateral damage, resolved any related security incidents, performed routine cyber hygiene due diligence and engage external cybersecurity-as-a-service providers and response professionals