COMPASS MSP

CASE STUDY:

SECURE PATH

SOC AS A SERVICE

Incident

An attacker gained unauthorized access to a client's Office 365 tenant, logging into a finance employee's user account from a foreign country. This suspicious login activity triggered a high-priority alert for the CompassMSP SOC.

Response

After analyzing the alert details, verifying the threat, and consulting the client's incident response profile, the CompassMSP SOC followed standard procedure, utilizing direct access to the client's Office 365 tenant to disable the impacted account and revoke active malicious sessions to mitigate further impact. From there, the SOC initiated a formal incident response / investigation, notifying the client and other relevant service teams and examining the tenant for other indicators of compromises. Upon discussing the attack with the client's CompassMSP AutoPilot service team, the SOC identified another area needing containment: the client's O365 tenant was syncing with their local AD domain. As such, user account containment also needed to occur within the local domain itself to be most effective. Since the SOC and IT have a direct line to each other, Compass was able to better protect and secure the client despite the breach.

COMPASSMSP

CASE STUDY:

SECURE PATH

SOC AS A SERVICE

Results

The CompassMSP SOC leveraged their proximity to the client's environment to take meaningful containment steps ASAP, preventing negative impact and client losses altogether. If the client had been using multiple parties, the time between the various phases of detection, escalation, threat analysis, verification, and containment/response may be drawn out in such a way as to allow attackers ample time to carry out their malicious intent. When critical alerts trigger, time is of the essence. The CompassMSP SOC had the both the expertise to handle and the access needed to ensure an efficient incident response.

SECURE PATH

CYBERSECURITY AND COMPLIANCE SERVICES:

Benefit from strategic cybersecurity guidance and advisory services that help to develop and implement effective cybersecurity strategies aligned with your goals. Navigate complex regulatory requirements effortlessly with compliance reporting and regulatory support.

contactus@compassmsp.com compassmsp.com (833) 444-2677