Microsoft Sentinel To The Rescue

IT services group for international manufacturers looks to Sentinel to strengthen security

OVERVIEW

Oakwood's Security Team recently received some tangible results and praise for their Microsoft Sentinel deployment within the client's Azure environment.

For several years, Oakwood has been working closely with the IT services arm of a large international manufacturer representing some very well-respected brands. Oakwood has earned the client's trust over the years through several successful consulting and implementation engagements. The list of projects include such things as; acting as Cloud Solution Provider (CSP) for 365 licensing and optimization, migrating on-premises servers to Azure, implementing Azure Site Recovery (ASR), data reporting with Power BI, Intune, MFA, and more.

SOLUTION

Earlier this year, Oakwood was brought in to review and provide recommendations for perimeter security throughout the client's Azure footprint. This included documenting all of the requirements and use case for a Microsoft Sentinel deployment across on-premises and Azure datacenters and how to automate remediation efforts and reporting of threats.

The Oakwood Team deployed, tested and configured Sentinel across a variety of resource groups and Vnets in Azure in addition to on-premises datacenter architecture in VMware. Oakwood also worked with the client to fine tune Sentinel policies including remediation and escalation plans.

SENTINEL IN ACTION

Just a few months after implementation the AI tools within Sentinel had alerted the client to a suspicious key logger that had been deployed on one of their newly built workstations. This activity was actually missed by other installed endpoint protection utilities.

Oakwood's client notified the Oakwood Security Team and, upon further investigation, Oakwood Engineers found an .exe file that was compromised. Had Sentinel not caught this activity - keystrokes and

SUMMARY

Business Challenge:
Oakwood's long-standing client was concerned that their disparate security tools were not adequate in providing trustworthy threat notifications and remediation guidance. They need a SIEM solution that could bridge together both on-premises and cloud resources in a single dashboard with customizable alerts and remediation action plans.

Solution:
Microsoft Sentinel deployment across on-premises datacenters and Azure resources to strengthen perimeter security posture.

Benefits:
Shortly after implementation, Sentinel alerted the client to malicious activity that was overlooked by other security tools.

credentials would have streamed from the workstation to the hackers who compromised the file without anyone knowing.

Each and every day cyber-attacks are becoming more sophisticated. You need the proper tools and the Oakwood Team on your side to ensure cyber intrusions are kept at bay.

Contact us today to learn more about how to get started with Microsoft Sentinel!