Microsoft Defender for Identity

Case Study - Large Manufacturer in Chicago

the challenge

A large supplier of tooling and industrial materials with over 9,000 users needed a way to monitor login activity among the organization's many cloud-based applications without spending countless hours combing log files and searching for suspicious activity. The company engaged Peters & Associates to secure its identity management infrastructure against cybersecurity attacks with Microsoft Defender for Identity (formerly known as Azure ATP).

Today's Threat Landscape

As organizations move more business processes outside of the office and into the cloud, the traditional idea of the "perimeter" expands and becomes more complex. Today's perimeter can no longer be guarded with simple firewalls; threat actors are leveraging security gaps in cloud-based applications and even revamping malware code that can remain hidden for months, as we saw in the recent SolarWinds and Malwarebytes breaches.

Monitoring your identity database (Active Directory, for many companies) is critical in this evolving threat environment. However, log files are complicated and can be difficult to parse at surface level. **Microsoft Defender for Identity,** formerly Azure ATP**,** is cloud-based security software that solves this problem by analyzing and parsing Active Directory activity, intelligently learning to identify and report threats. Defender for Identity also enables the configuration of honeytoken accounts, which are used as traps for malicious actors - any authentication associated with these honeytoken accounts (normally dormant), triggers an alert.

the solution

Peters accomplished the customer's goal by deploying Microsoft Defender for Identity in their environment. Much like a firewall protects the devices that sit behind it, Microsoft Defender for Identity adds a layer of protection to the identity perimeter. Peters configured Microsoft Defender for Identity to use the signals given off by the on-premise Active Directory infrastructure to identify and investigate potential identity-based security threats.

How Defender for Identity Works

Microsoft Defender for Identity has a four-pronged approach to identity management: analysis, learning, detection, & alerting. Most SMB deployments will be 5 days but could scale up to more if there are more than 4 DC's, or integration with a SIEM. After a couple weeks, customer may need help with triggered events being generated.

Analysis

The solution collects and analyzes data from different sources, like logs and domain controller activity.

Machine Learning & API

Microsoft Defender for Identity parses collected information to begin identifying patterns of activity to help identify anomalies more quickly.

Detection

Defender for Identity can more accurately detect malicious attacks, abnormal behavior, and other cybersecurity-related issues.

Devices & IoT

Smart alerts provide a clear snapshot of what is being targeted and how it is being attacked.

Microsoft Defender for Identity is a common security choice for businesses because it provides accurate deep-level visibility into identity security and threats, and it's relatively straightforward to deploy.

Common events might be:

DNS Enumeration
("hey...what are your server names on this network?")

Unusual Login Attempts
(15 attempts in a short period vs an account)

Lateral Movement and/or Escalation of Privilege
Workstation that falls off then rejoins domain (imaging workstations can trigger)

Solution Implementation

A "Plan the Work and Work the Plan" Mentality

The customer is a large-scale international company with over 9,000 users and numerous domain controllers throughout the organization. Having a solid deployment plan allowed Peters & Associated to get the solution implemented quickly and effectively.

Honeypot accounts are fake accounts designed to look like common cyberattack targets, thereby luring bad actors towards the fake accounts and away from targeting the real ones that hold sensitive data. Peters & Associates set up honeypot accounts that trigger alerts when targeted, so the customer will know about security threats when they hit the decoy honeypot accounts and before they target any real accounts. Peters also developed custom auditing policies to help Defender for Identity accurately recognize and report suspicious activity. From there, Peters installed the necessary ATP sensors and implemented the Microsoft Defender for Identity tenant, integrating it within the Active Directory infrastructure. Finally, the Peters & customer's IT teams worked together to validate connectivity and complete all test plans before going live with the solution.

"As a global manufacturer of industrial tooling with 9,000 employees, our IT footprint is complex. Defender for Identity makes the process of detecting critical security events in Active Directory quite simple with little noise. With the help of Peters & Associates, we improved our security posture in just a few weeks."

- Team Lead / IT Security, Manufacturing Firm

results

There were two notable strategies from this implementation that aided in the overall success of the project:

Risk Reduction & Compliance
Peters' implementation of Defender for Identity helped its client boost security and compliance, reducing the risk of breaches, data loss and non-compliance fees.

Investment Maximization
Peters surveyed the tools the client already had in place, like Microsoft 365 and E5 security, to pair with Defender for Identity to maximize the client's investment.

Thanks to careful planning and clear scope definition, the team at Peters & Associates was able to get the Microsoft Defender for Identity solution up and running so that the customer was leveraging it within two weeks of signing the proposal.

The customer was leveraging the security solution within two weeks of signing the proposal from Peters & Associates.

contact us

Are you interested in learning more about how Peters & Associates can help protect your identity perimeter from malicious activity through real-time detection and analysis? Contact us today.

Contact Us