THREAT HUNTING IN THE CLOUD NOTES

Bennett Wiley

Part Two Notes:

Chapter 4: Microsoft Azure Cloud Threat Prevention Framework

- Infrastructure & Network
  - VPN Gateway
  - Azure DDos Protection Standard
  - Azure Front Door
  - Azure Firewall
  - Azure Key Vault
  - Key Vault Managed HSM
  - Azure Private Links
  - Azure Application Gateway
  - Azure Service Bus
  - Web Application Firewall
- Using Azure Conditional Access to Protect Against an "Initial Access" TTP: Since there is a constant change in computing and seeing more companies change to a cloud model, it's shown to be difficult to try and access data and document s that companies need to help run a successful business. One of the ways to fix this is to introduce Conditional Access policy.
- Azure Defender: *"Azure Defender, part of Azure Security Center, brings advanced and intelligent protection across the Azure and hybrid resources and workload. Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, and more." p.g 127*
- Detecting Credential Access: This type of an attack is when hackers access or steal credentials of an account to have access and or bypass a company's security to use resources or steal viable data.
- Detecting Lateral Movement: This type of attack is when someone will use non-sensitive accounts and work their way through the system in order to hide under the radar and gain trust to obtain clearance to sensitive accounts. This type of attack can help show and provide sensitive accounts and data though login credentials in accounts, groups, and machines.
- Detecting Command and Control: Also known as C2 or C&C and this method shows how attacks communicate through a system. This method is regarded to be one of the most damaging and the following is ways Command and Control may happend:
  - Sending a phishing email to trick the user into following a link to a malicious website or opening an attachment that executes malicious code.
  - Using password spray attacks to gain access to the environment.
  - Through any security vulnerability in the end-user browser plug-ins.
  - Via infected and compromised software.

- Detecting Data Exfiltration: This can be done remotely or manually and it is hard to identify when due to it resembling a normal behavior. Common techniques used are USB thumb drive, a smartphone, and a laptop. The Microsoft Cloud App Security (MCAS) app can help detect when this type of an attack happens.
- Microsoft Investigate, Response, and Recover Features:
    - Azure Security Center: *We covered this service in the previous section of this chapter.*
    - Azure Sentinel: *We covered this service in the previous section of this chapter.*
    - Azure Monitor logs and metrics: *This service delivers a comprehensive solution for collecting and analyzing and allows you to take action on telemetry from your cloud and on-premises environments. Azure Monitor collects and aggregates data from a variety of sources into a common data platform where it can be used for analysis, visualization, and alerting.*
    - Azure AD reports and monitoring: *Azure AD reports provide a comprehensive view of activity in your Azure cloud environment. AD Monitoring lets you route your Azure AD activities logs to different endpoints.*
    - Azure AD PIM audit history: *This audit history shows all roles, assignments and activations within the past 30 days of all the privileged roles.*
    - Microsoft Cloud App Security: *MCAS provides tools to gain a deeper understanding of what is happening in your cloud environment; it also helps you manage the risky apps, risky users, and data leakage. p.g 157*
- Detecting Threats and Proactively Hunting with Microsoft 365 Defender: This is a query based threat hunting tool that can analyze raw data up to 30 days. This helps you analyze and inspect potential threats and the behavior in your network and notifies you were to locate these threats. It also supports datasets from Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Cloud App Security, and Microsoft Defender for Identity
- Overview of Fusion Detections: “*This combines low and medium alerts from Microsoft and third-party security products into high severity incidents. Fusion is enabled by default. Because the logic is hidden and therefore, not customizable, you can only create one rule with this template.” P.g 173*

Chapter 5: Microsoft Cybersecurity Reference Architecture and Capability Map

- Microsoft Security Architecture:
    - The Identify Function: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management.
    - The Protect Function: Identity Management - Authentication - Access Control, Awareness and Training, Data Security, Protective Technology, Information Protection Processes and Procedures, Maintenance
    - The Detect Function: Anomalies/Events, Security Continuous Monitoring, Detection Processes
    - The Respond Function: Response Planning, Communications, Analysis,

Mitigation, Improvements
    - The Recover Function: Recovery Planning, Improvements, Communications
- Using the Microsoft Reference Architecture: Also known as (MCRA), This is a page that pops up and provides security solutions and what solutions would be most effective.
- Protecting the Hybrid Cloud Infrastructure: Microsoft makes sure to invest a lot into Azure Marketplace because they want to guarantee customers the access to certain features from popular vendors and it is common for consumers to use existing controls for on-site cloud infrastructure.
- Protecting Endpoints and Clients: *"Managing risk, health, and compliance across a broad spectrum of device plat- forms and ownership (BYODs, corporate devices, Macs, as well as unmanaged and mobile devices) is one of the most important priorities of the security and IT team. Many organizations take advantage of built-in Windows features and system management to provide basic security hygiene like patching and Active Directory account security and group policy." p.g 206*
- Protecting SaaS Apps: SaaS Apps is a software as a service application. The most frequent challenge when trying to protect this type of application is concerning governance, risk, and compliance. MCAS can help with these common challenges and can help secure MCAS as a third party and provide CSAB additional capabilities.
- Protecting Data and Information: Microsoft is dedicated to protecting data and information but can protect data and information has its challenges. To help tackle these challenges Microsoft offers a wide range of services which include Azure Purview, Microsoft Information Protection (MIP), and Advanced eDiscovery.
- Threat Modeling for the Azure IoT Reference Architecture:
  Main area of focus includes…
    - Devices and data sources
    - Data transport
    - Device and event processing
    - Presentation
- Attack Simulator: This is a tool that is used to help train employees to defend against attackers trying to get sensitive data and information from their organization. It can emulate real attacks and shows employers what to do in case a real attack happens. It's a simulation in Microsoft defender for Office 365.
- Communication Compliance: Like Attack Simulator, Communication Compliance is another Office 365 tool that helps find risks from the inside and provide solutions. It can provide recommendations across communication applications such as Microsoft Teams, exchanging email or third party communication applications.

Hey Evan,

What I did this week was read Threat Hunting in The Cloud Part Two and took notes. Again I have attached a PDF of part two notes to this email. Some of the blockers I had this week was again trying to make sure to focus on parts of the reading that can be applied our project and highlight those parts of both chapters 4 & 5 in the notes that I included, again let me know if they are alright and let me know what I can work on for next week!

Thanks