THREAT HUNTING IN THE CLOUD NOTES

Bennett Wiley

Part One Notes:

Chapter 1: Introduction to Threat Hunting

- Threat Hunting: A solution to fight against cyber criminals. It's considered a proactive solution because it's a process that helps identify an attacker's TTP within an environment.
- TTP: Tactics, Techniques, and Procedures
- How to find an attacker's TTP: Look for signatures and indexes that stand out.
- Types of Cyber Attacks:
    - Phishing
    - Ransomware
    - Nation State
- The Necessity of Threat Hunting: When it comes to the digital environment it is always rapidly changing. It is best to assume that your organization will be attacked and be prepared. Attackers' digital fingerprints are always changing so by the time an organization figures out that they are compromised it may be too late.
- Assume Breach: *"Is an approach that assumes that your enterprise is already breached and vulnerable. The focus is to change the security posture of the organization to be proactive, knowing adversaries are monitoring their digital assets."* p.g 15
- Threat Hunting Framework:
    - Purpose of the hunt
    - Where the hunt will occur
    - Desired outcome of the threat hunt
- Threat Modeling: Threat Hunting at its core has Threat Modeling. Threat Modeling needs to update and upgrade overtime and expand coverage. The three main components of threat modeling include Threat Intelligence, Security Controls and Their Effectiveness, Asset Inventory and Their Vulnerabilities
- The Threat Hunting Maturity Model:
    - Level 0: Initial - *Relies primarily on automated alerting.*
    - Level 1: Minimal - *Incorporates that intelligence indicator searches.*
    - Level 2: Procedural - *Follows data analysis procedures created by others.*
    - Level 3: Innovative - *Creates new data analysis procedures.*
    - Level 4: Leading - *Automates the majority of successful data analysis procedures*.
- Threat-Hunting Team Structure: When you are working in a team environment for threat hunting, the structure of the team may vary depending on the size of the team. This includes External Model, Dedicated Internal Hunting Team Model, Combined/Hybrid Team Model and Periodic Hunt Teams Model.

Chapter 2: Modern Approach to Multi-Cloud Threat Hunting

- Multi-Cloud Structure: In recent years Multi-Cloud structures have been on the rise. This includes using multiple cloud vendors such as AWS, Azure, and Google to help store organizations data, software, and assets to get rid of reliance and create more flexibility.
- Multi-Cloud Threat Hunting: Cloud Threat Hunters focus more on authentication/authorization. Some things can only be accessed in the cloud via authentication or having authorization. Attackers will see what data can only be viewed by authorized people and will be curious on how to access this.
- Threat Hunting in Multi-Cloud and Multi-Tenant Environments: There are a lot of risks when it comes to using Multi-Cloud and Multi-Tenant environments and organizations need to know this before using it. This includes the security of data and the privacy of it.
- A Security Operations Center (SOC): *"An organization function or a centralized unit with various security roles, such as Security Analyst, Threat Hunter, Red Team/Blue Team members, etc. It deals with defending and protecting the organization against various security-related issues using a variety of tools."* p.g 41
- Security Information and Event Management (SIEM): *"Is a tool that collects, normalizes, and analyzes application logs and events against the set of correlation rules. When these rules are triggered, they create a series of events that human analysts analyze and respond to."* p.g 41
- SOC Models: There are three different types of SOC Models which include on site, remote, and hybrid option where its on site and remote mixture.
- Threat-Hunting Goals and Objectives: In Threat Hunting, it is important to know what environment that you are in and what exactly you are looking for. You need to rely on Threat hunting to help reduce the negatives in SOC. This helps SOC prioritize what to look for.
- Threat Modeling in SOC: In order to have a successful SOC model, it is important to look at threat modeling. It helps determine the range and select the right tools for the SOC.
- Cyber Resiliency: Helps reduce and protect from cyber risks, reduce the number of attacks, and secure organizations to operate.
- Threat-Hunting Data Collection Steps:
    - Data Collection
    - Data Refining
    - Defining New Procedure
    - Hunting
    - Optimizing
    - Automating & Maintaining

Chapter 3: Exploration of MITRE Key Attack Vectors

- MITRE ATT&CK Framework: It's an accessible database that provides techniques and tactics from real world examples. It can help find specific threats and provide various methodologies to help prevent specific attacks. This was first introduced in 2013 and has since then grown in popularity.
- Tactics: "*Tactics describe what the attacker is trying to do at any given phase of the attack, not how they are specifically going about it.* p.g 67
- Techniques: *Describe the various technical ways attackers have developed to employ a*

given tactic." p.g 67

- Threat Hunting Using Five Common Tactics:
    1. Privilege Escalation
    2. Credential Access
    3. Lateral Movement
    4. Command & Control
    5. Exfiltration
- Zero Trust: Zero trust is not a tool or a product. It is a methodology that people should use when handling sensitive data by trusting no one other than yourself. If people adapt to this methodology it is a good first step on making sure attackers don't get valuable data.
- Build Cloud-Based Defense-in-Depth: It is important to know the three aspects of zero trust which include verify explicitly, least privilege access, and assume breach. Make sure to always test the security because this will help you stay ahead of upcoming threats.
- Control Number Filters:
    - Control One: *Filters 80% of Evil.*
    - Control Two: *Filters 30% of Evil.*
    - Control Three: *Filters 80% of Evil.*
    - *97.2% of Evil dumped at this point.*
- Microsoft Azure Sentinel:
    - Collect - *Security data across your enterprise.*
    - Detect - *Threats with threat intelligence.*
    - Investigate - *Critical incidents guided by AI.*
    - Respond - *Rapidly and automate protection.*
- Amazon CloudWatch: *"Is the core service for monitoring an AWS environment, because it is easy to get up and running and provides basic metrics, alarming, and dashboards."* p.g 93
- Amazon Athena: This amazon service allows consumers to use and run SQL queries. Consumers may build virtual data tables to log data using SQL programs that need to be managed which Amazon Athena does.

Part Three Notes:

Chapter 6: AWS Cloud Threat Prevention Framework

- The Five Pillars of the Well-Architected Framework:
    1. Operational Excellence
    2. Security
    3. Reliability
    4. Performance Efficiency
    5. Cost Optimization
- The Shared Responsibility Model: This model highlights what responsibility that the customer has and what responsibility AWS has. For example customers have the responsibility of Customer Data which include Platform, Applications, Identity and Access Management. AWS is responsible for Software which include Compute, Storage, Database, and Networking. Another thing AWS is responsible for is Hardware /AWS

Global Infrastructure. This focuses on Regions, Availability Zones and Edge Locations. A more simple way of knowing who is responsible for what is that Customers are responsible for security 'IN' the cloud and AWS is responsible for security 'OF' the cloud.

- AWS Services for Monitoring, Logging, and Alerting: These three policies help increase the chances of finding harmful behavior on a system and networks. This is mostly important on the customer's side of the responsibility. Monitoring helps improve three things. Reliability, availability and performance.
- AWS CloudTrail: This is a service that helps you keep track and log while continuously viewing and help gather account activity that may correlate to actions across an AWS infrastructure. It also provides a timeline of your AWS account and activity which includes actions through the AWS Management console.
- Amazon VPC Flow Logs: This is a feature that helps you view data about the IP traffic between network interfaces in a VCP. Once a flow log has been built, you can grab and analyze its data in a chosen destination. Flow logs can help you with three things…
    - *Diagnosing overly restrictive security group rules*
    - *Monitoring the traffic that is reaching your instance*
    - *Determining the direction of the traffic to and from the network interfaces*
- Amazon GuardDuty: Is another security monitor service that can use data sources such as VPC Flow Logs, AWS CloudTrail event logs, CloudTrail S3 logs and DNS logs. What is used to find potential threats is identifying IP addresses/domains that have bad intent and finding unauthorized and suspicious activity in an AWS environment.
- AWS Security Hub: This feature provides you a list of security alerts that come up across various AWS accounts. This feature is nice because it's one access point that helps organize and prioritize security threats and alerts.
- AWS Detection Features: This feature is aways monitoring because it's important to finding potential suspicious activity. This should be able to predict cyber attacks and be able to grab resources in order to respond to those attacks.
- How You Can Detect Data Exfiltration: There are techniques that are used to help grant access to higher level data that requires permission on a system. Techniques that are used to help bypass permission is by looking at weaknesses, misconfigurations, and vulnerabilities.
- Amazon Macie: Is a service that can manage data security and data privacy. What it uses is machine learning to help protect sensitive data. This is used to help detect unsecured credentials.

Chapter 7: AWS Reference Architecture

- Amazon NIST Cybersecurity Framework:
    - Identify: *Access Management, Business Environment, Governance, ect.*
    - Protect: *Access Control, Awareness & Training, Data Security, Maintenance, ect.*
    - Detect: *Anomalies & Events, Security Continuous Monitoring, ect.*
    - Respond: *Response Planning, Communications, Analysis, Mitigation,ect.*
    - Recover: *Recovery Planning, Improvements, Communications, ect.*
- AWS Config: This is a service that allows organizations to analyze configurations of their AWS. Benefits of this service is that it allows you to have continuous monitoring for configuration changes and it can track relationships between the resources.

- AWS Organizations: This helps take care of AWS resources if it scales up. Using this service it can help generate new AWS accounts and organize incoming resources by simplifying the process while your workload increases. It can also help with secure and audit your environment across accounts and efficiently look at resources across accounts.
- AWS Control Tower: Is considered the best way to examine and control a secured AWS environment that has multiple AWS accounts to it.
- AWS Trusted Advisor: This is a tool that is present when using it to help guide your resources in AWS best intentions. It also checks to help boost security, performance and it is one of the best options when trying to reduce overall cost.
- AWS Single Sign-On (SSO): This helps by accessing multiple AWS accounts and business applications from one place. AWS SSO also has a feature where the configuration wizard can extend the SSO to any other device as long as that device has SAML 2.0
- AWS Firewall Manager: This allows organizations to apply any firewall configurations to AWS accounts that are in AWS organizations.
- AWS Cloud HSM components:
    - *"AWS manages the hardware security module (HSM) appliance, but does not have access to your keys."*
    - *"You control and manage your own keys."*
    - *"Application performance improves (due to close proximity with AWS workloads)"*
    - *"Secure key storage in tamper-resistant hardware available in multiple Availability Zones (AZs)."*
    - *"Your HSMs are in your Virtual Private Cloud (VPC) and isolated from other AWS networks."* p.g 344
- AWS Private Link: This has two components when looking at it. The first component is VCP endpoint which focuses on creating an interface for the VPC endpoint. The second component is Network Load Balancer which will need to have a connection to an endpoint and the choice of service provider would be an option.
- Amazon Detective: This can help point out the source of security threats and attacks. This works by gathering log data from AWS accounts and uses machine learning to help find the route cause and make the process faster.