The Importance of Proactive Threat Hunting

Chapter 13

Episode 13.01

Threat Hunting and the Hypothesis

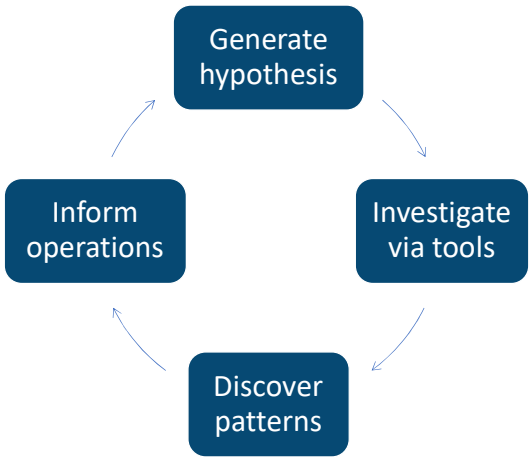
Objective: 3.3 Explain the importance of proactive threat hunting.

- Establishing a hypothesis

Threat Hunting Process

- Proactively searching environment for threats
- What is the purpose of the hunt?
- Where will it be conducted?
- What resources do I need to conduct the hunt?
- Who are the key stakeholders?
- What is the desired outcome of the hunt?

Threat Hunting Process



Threat Hunting

- Funding and support
- Initiation
  - Creation of the hypothesis

Establishing a Hypothesis

- Statement of expectation
  - Based on information
- Analytics-driven
  - Based on data
- Situational-driven
  - Situations change, resulting in vulnerabilities
- Intelligence-driven
  - Someone has provided intelligence
- Experience-driven
  - Based on familiarity with your environment

Episode 13.02

Threat Hunting Process

Objective: 3.3 Explain the importance of proactive threat hunting.

- Profiling threat actors and activities
- Threat hunting tactics
- Executable process analysis

Profiling Threat Actors and Activities

- MITRE ATT&CK framework
  - Initial access
  - Execution
  - Persistence
  - Privilege escalation
  - Defense evasion
  - Credential access
  - Discovery
  - Lateral movement
  - Collection
  - Command and control
  - Exfiltration
  - Impact

Threat Hunting Tactics

- High-impact TTPs
  - Initial access and discovery
  - Persistence
  - Lateral movement and privilege escalation
  - Command and control
  - Exfiltration
  - Searching
  - Clustering
  - Grouping
  - Stacking

Threat Hunting Tactics

- Executable process analysis
  - Reverse engineering

Episode 13.03

Results and Benefits

Objective: 3.3 Explain the importance of proactive threat hunting.

- Reducing the attack surface area
- Bundling critical assets
- Attack vectors
- Integrated intelligence
- Improving detection capabilities

Delivering Results

- Document the process
- Reduce the attack surface area
- Bundle critical assets
- Explore attack vectors
- Use integrated intelligence

Improving Detection Capabilities

- How do you convince stakeholders and financial department?
- Threat-hunting output benefits
  - Updated firewall and intrusion detection/prevention system (IDS/IPS) rules
  - Updated alert logic for SIEM platforms
  - Updated alert logic for endpoint detection and response (EDR) platforms
  - Improvements to sensor placement across the network
  - Improvements to asset visibility
- Other benefits to detection team
  - Changes in your organization's development process
  - Changes to security training across the organization
  - Changes to quality assurance and quality control processes