Lesson 3 – My Learnings and Hands-On Experience

Lesson 3 was where I transitioned from learning about SOC concepts to actively applying them in simulated, real-world scenarios. I practiced using Microsoft Security Copilot and other Microsoft security tools to detect, investigate, and respond to cybersecurity incidents.

I learned that effective incident handling requires both technical expertise and quick decision-making under pressure. While AI-powered tools streamline detection and provide rapid insights, I experienced firsthand that human judgment is critical for validating findings and determining the right course of action.

How should a SOC address security incidents?
Incident handling and decision-making are critical components of an organization's cybersecurity strategy. When an alert or potential security threat occurs, SOC teams must quickly assess the situation and take decisive actions. AI-powered tools can help automate threat detection and provide insights, but human expertise is essential for making the final decisions on how to respond.

Addressing security incidents requires a blend of knowledge, quick thinking, and continuous learning. As security threats

evolve, your ability to respond effectively depends on staying informed and adaptable.

Incident Handling Scenarios – My Experience

I took on the role of a SOC analyst and worked through a variety of incident response exercises:

1. Respond and Remediate – In this simulation, I received an active security incident and had to determine if it was malicious. Using Microsoft Defender XDR and Security Copilot, I analyzed alerts, examined impacted systems, and took swift remediation actions such as isolating endpoints and revoking compromised credentials. This exercise reinforced my ability to act quickly without overlooking critical details.

2. Triage Incidents – I reviewed multiple security alerts to decide which required immediate escalation. I used Security Copilot to process large volumes of contextual data rapidly, filter out false positives, and prioritize the most urgent threats. This improved my efficiency in distinguishing between routine anomalies and genuine high-risk incidents.

3. Investigate Suspicious Entities – I examined suspicious files, URLs, and system logs to determine potential malicious activity. Using Defender XDR's deep analysis tools, I traced the activity back to its source, identified the threat type, and created clear remediation steps for stakeholders. This taught me the importance of thorough investigation and precise

communication during active security events.

Gamified Cybersecurity Practice

To further strengthen my decision-making skills, I engaged in several hands-on, gamified cybersecurity challenges:

- KC7 Cyber Detective Game – I investigated unusual network activity using Microsoft Defender XDR Threat Intelligence. This game sharpened my pattern-recognition skills and improved my ability to follow complex investigative trails.

- Minecraft Education Cyber Defender – Through a tower defense format, I applied layered security concepts to protect virtual assets. It helped me visualize the importance of multiple defense layers against evolving threats.

- Minecraft Education Cyber Expert – I tackled challenges in encryption, social engineering, and malware defense, while also exploring cybersecurity career paths. This made technical concepts more engaging and memorable.

- TryCyber – I worked through realistic cybersecurity workforce tasks aligned with the NICE Framework, including vulnerability scanning, incident classification, and remediation planning. This exercise gave me a better sense of industry expectations and best practices.

RANSOMWARE INCIDENT

USER ACCOUNT INVESTIGATION

BUSI
EM
COMP

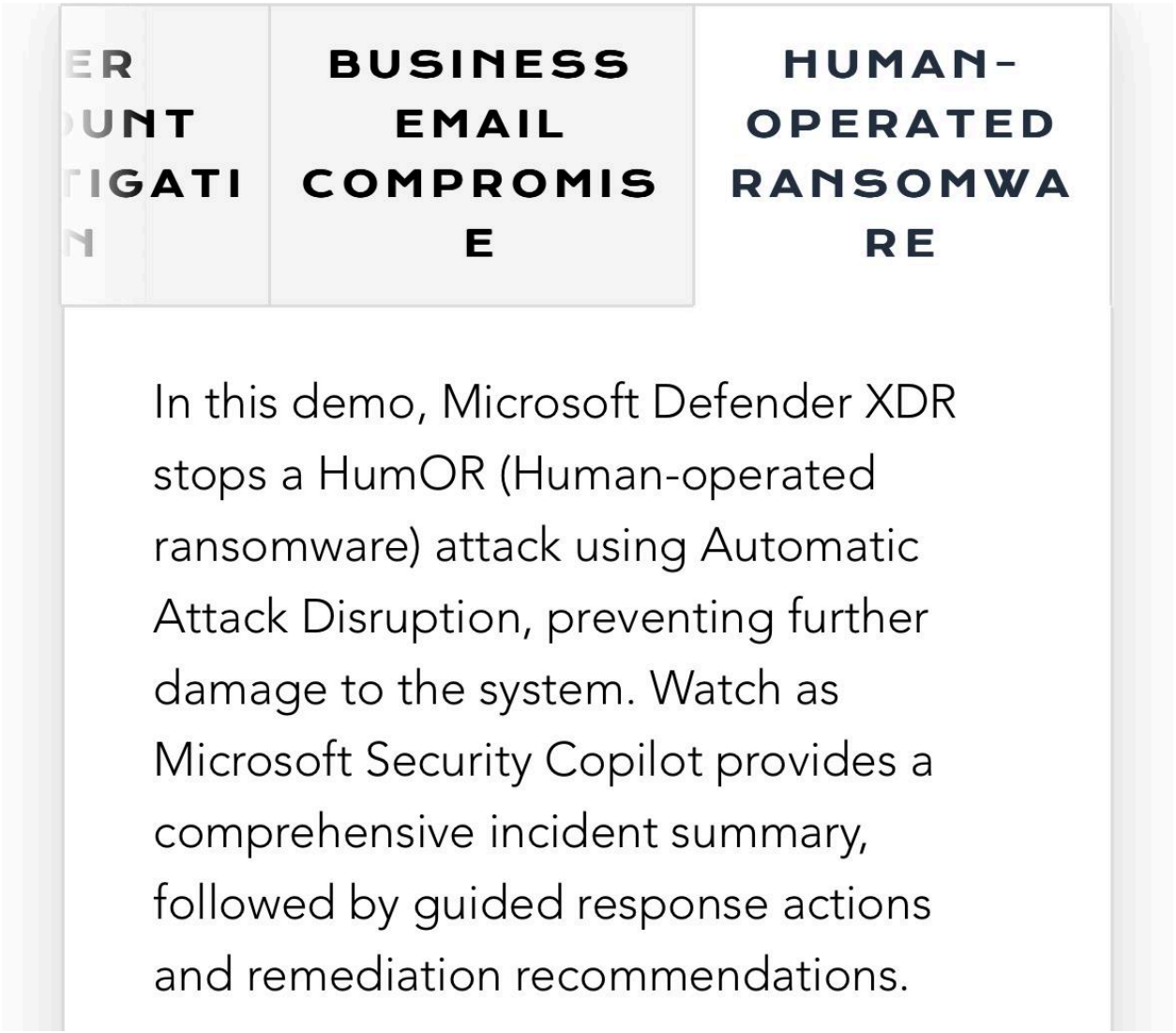
In this demo, Security Copilot leverages Microsoft Sentinel, Intune, Defender Threat Intelligence, and Purview to investigate a user account anomaly. Watch as Security Copilot accelerates account investigation and reporting, streamlining the process and enhancing a SOC's ability to identify potential security risks.

RANSOMWARE INCIDENT	USER ACCOUNT INVESTIGATION	BUSI EM COMP

In this demo, Microsoft Defender XDR with data from Microsoft Defender for Cloud is used to respond to a ransomware incident, showcasing its capabilities in detecting threats, providing actionable insights, and managing security in real-time. Watch as Security Copilot helps identify and mitigate ransomware attacks, offering SOCs enhanced visibility and faster response times.

USER ACCOUNT INVESTIGATION | BUSINESS EMAIL COMPROMISE | HUMAN-OPERATED RANSOMWARE

In this demo, Microsoft Defender XDR uses Automatic Attack Disruption to effectively stop a Business Email Compromise (BEC) attack. Watch as Microsoft Security Copilot summarizes the incident and provides guided response actions, along with recommendations for remediation.



AI in SOC Operations – My Observations

Through the simulations, I saw how AI enhances SOC performance by:

- Automating repetitive tasks like alert triage.

- Detecting subtle anomalies that indicate early stages of an attack.

- Providing clear, natural-language insights that speed up investigation.

However, I also learned that AI is most effective when paired with skilled human analysts who can apply context, weigh business impact, and make nuanced decisions that automated systems cannot.

Final Reflection

By completing Lesson 3, I gained practical, hands-on experience in SOC operations, from initial detection to final remediation. I developed stronger investigative skills, learned to prioritize effectively, and practiced using Microsoft's advanced security tools in high-pressure scenarios. These exercises not only reinforced my technical knowledge but also boosted my

confidence in handling real-world security incidents.