CLOUD INCIDENT RESPONSE + SJU ACM CLUE PT 2

SJU ACM STUDENT CHAPTER

SJU ACM
Student Chapter

SIGN IN FORM:

INTRO TO CLOUD INCIDENT RESPONSE

WHAT IS AZURE?

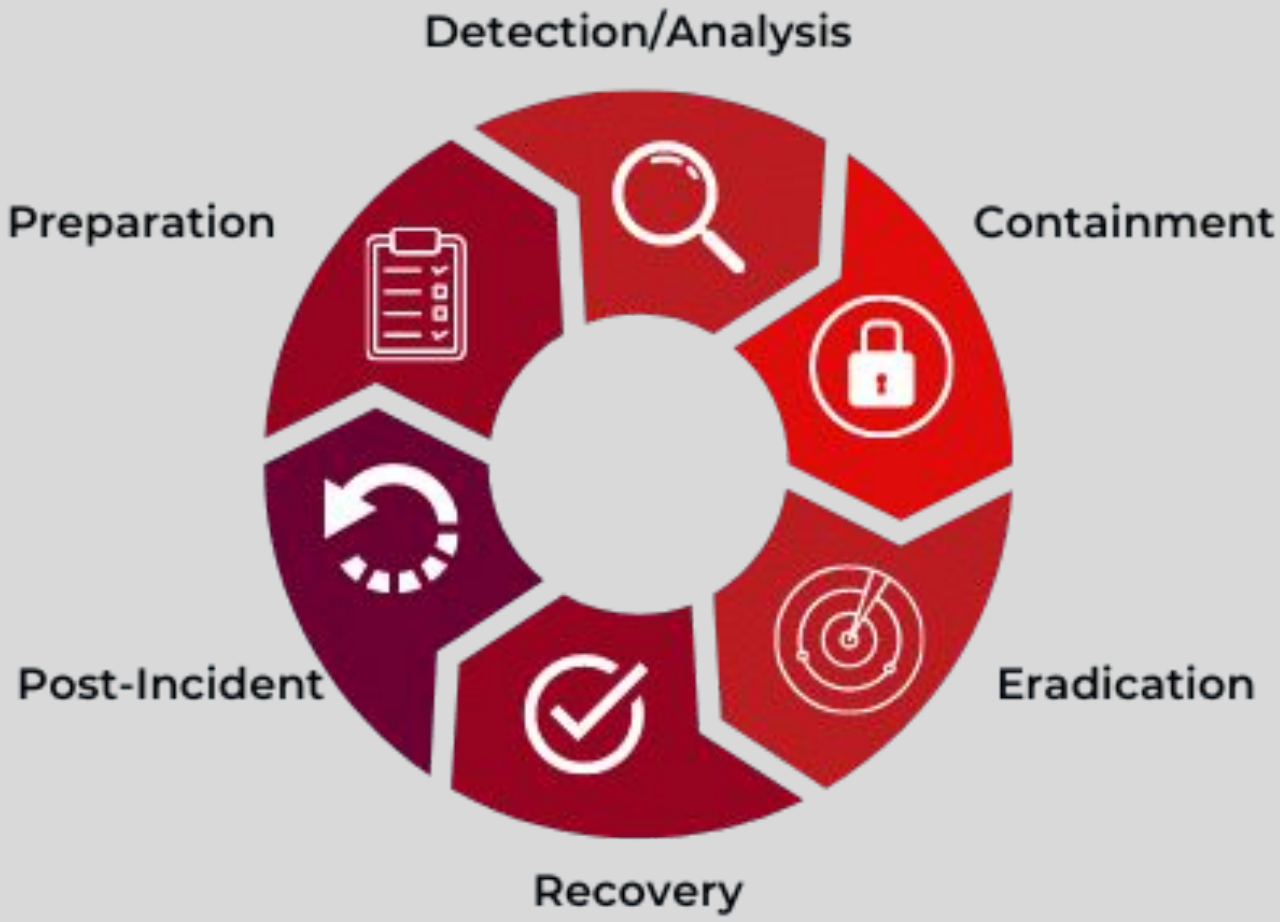
- AZURE IS MICROSOFT'S CLOUD PLATFORM
  - EQUIVALENT TO AWS OR GOOGLE CLOUD
- BEST HYBRID CLOUD DUE TO MICROSOFT'S MARKET PRESENCE IN PHYSICAL DEVICES AND THE WINDOWS OPERATING SYSTEM
- EXCELS IN SECURITY DUE TO SENTINEL, ITS CLOUD-NATIVE SIEM

WHAT IS SENTINEL?

- MICROSOFT'S CLOUD-NATIVE SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PLATFORM
- AGGREGATES LOGS FROM ACROSS AZURE RESOURCES TO A CENTRALIZED PLACE
- DETECTS SECURITY INCIDENTS VIA CUSTOMIZABLE LOG ANALYTICS RULES
- CAN ENABLE AUTOMATED RESPONSES TO INCIDENTS

AWS Security Hub = Microsoft Sentinel = Chronicle

Incident Response Lifecycle



LAB PREP

CREATING YOUR AZURE ACCOUNT

1. GO TO: HTTPS://AZURE.MICROSOFT.COM/EN-US/FREE/STUDENTS
2. CLICK “START FREE” AND LOG INTO YOUR MICROSOFT ACCOUNT
3. ENTER YOUR PERSONAL INFORMATION
4. PROVIDE US WITH YOUR ST. JOHN’S EMAIL TO GET ADDED TO THE AZURE ENVIRONMENT
5. ACCEPT EMAIL INVITATION
6. DOWNLOAD MICROSOFT AUTHENTICATOR APP
7. SET UP AUTHENTICATOR AND COMPLETE MFA LOGIN
8. SEARCH FOR “RESOURCE GROUPS” AND MAKE SURE YOU CAN SEE “ACMCLOUDRG”. IF IT’S NOT THERE, REFRESH THE PAGE A COUPLE OF TIMES

LAB BRIEFING

SJU ACM CLUE

An Incident in the Cloud

THE INCIDENT

The day is Wednesday, April 17. The St. John's ACM Student Chapter e-board is collaborating on their cloud platform to design a new workshop for their members. Upon logging in, they're met with an alert in their SIEM indicating that one of their workstations may have been infected with malware! The alert shows that a mysterious command was run on David's workstation, however, David claims that he was not logged into his workstation at the time of the alert and suspects that someone else on the e-board must have been the one behind this incident. The members of SJU ACM have agreed to investigate the alert in hopes of uncovering the true identity of the culprit. It's up to you to figure out who did it, where they did it, and what malware they used.

THE SUSPECTS

RAYMOND RAMDAT

JAKE ENEA

DAVID ROSOFF

TOMAS SANTOS YCIANO

BEN HANIM

FAIROOZ EHSAN

AQUEENA ALEXANDER

AMRITA KAUR

THE BUILDINGS

THE MALWARE

THANK YOU!