LAB － Demo Tools and Use Cases

Labs/Use Cases - Introduction

- Break into team of ~ 5 students.
- Go through all five Lab Use Cases as team, leveraging the 8.3 Solution Center environment
- Practice Execution of the Use Cases, and document the answers
- At the end of the lab, the team will be required to demonstrate the use cases in front of the class.

Lab – Demo Tools and Use Cases

Use Case #1 - Threat Dashboard in NOC

- Customer wants the Threat Dashboard prominently displayed in their NOC. Customer would like to display the following
  - Top Row – **Top Malware Detections, Top Attacker Countries, Top Attackers**
  - Middle Row – **Top Attack Subcategories, Top Targets, Active Botnets**
  - Bottom Row – **Top High Risk Botnets, Top Applications, Top Attacks**
  - They are not concerned or want to see system or status data.
  - Where applicable, customer would like to filter by only the highest risk or rated data.

Lab – Demo Tools and Use Cases

Use Case #2 – Top Malware Detected

- Customer would like to identify the top unblocked and blocked malware detections, regardless of malware confidence. Provide the following information
  - Top Unblocked Malware in the last 48 hours
    - How many total detections have occurred?
    - The name of the malware as detected by McAfee' s Real-Time Emulation Engine?
    - The Javascript execution highlights as detected by McAfee' s Deep File Analysis?
    - List three IPS alerts that triggered due to this piece of malware:
    - Identify 3 target IP Addresses that were victimized by this piece of malware.
    - TAKE ACTION AND BLOCK THE MALWARE
  - Top Blocked Malware in the last 12 hours
    - How many total detections have occurred?
    - What is the md5 of the malware
    - The name of the malware as detected by McAfee' s Real-Time Emulation Engine?
    - List two malicious observed behaviors McAfee' s ATD identified
    - List one directory created and one registry modified by malware

Lab – Demo Tools and Use Cases

Use Case #3 – Tell me about my Apps

- Customer would like a better understanding of risky applications on his network
  - Identify all instant messaging programs in the instant messaging application category
    - Which instant messaging platform is seen the most on the network?
    - Which IPS alert is triggered the most by the this most popular messaging platform?
  - Customer feels Facebook is a conduit for attacks
    - Show customer the top attacks related to Facebook
  - Identify any endpoints that use yahoo mail that have been attacked by Russia

Lab – Demo Tools and Use Cases

Use Case #4 – Tell me about my Endpoints

- Help the customer understand which of his endpoint have the Highest Risk
  - Identify the endpoint that has triggered the most exploits
    - List the exploit and source IP address of the most triggered exploit against this endpoint
    - List the User, Operation System, and Dat file version of this endpoint
    - List any open ports and the last two AV events seen on this endpoint
  - Identify the endpoint that has issued the most number of call backs
    - List any CVE's this endpoint may be vulnerable to
    - List the MAC Address of this endpoint.
    - <UI step: Use Threat Explorer to explore this target IP>
    - Identify the top Botnet (by attack count), the attacking source IP and Country, and the top Malware file hash.

Lab – Demo Tools and Use Cases

Use Case #5 – Help me understand Botnets and the Network

- Help the customer understand any Botnets in his network
  - Identify the top two botnets infecting the customers network
  - For the top botnet, identify the top 3 zombies participating in the endpoint
  - For the top Zombie, use network forensics to identify:
    - Suspicious activities which this endpoint has been involved with.
    - The name and URL associated with one blacklisted executable on this endpoint
    - An email address and file name associated with this endpoint
  - For the DGA botnet, identify the malicious activities associated with the bot.