FROM DETECTION TO RESOLUTION:

A Forensic Guide to Incident Response

NIST FRAMEWORK FOUNDATIONAL ELEMENTS

- Identify
  - The quality of work in this category will dramatically affect Respond & Recover outcomes
    - Asset Management
    - Crown Jewel Applications
    - Logging and Monitoring standards
    - Business Critical Data, etc.
- Protect
  - Controls applied to reduce risk
- **DETECT**
  - What's the scenario?
  - Outsourced MSSP or In House Security Operations Centre?
- **RESPOND & RECOVER**
  - Incident Response and Threat Mitigation

DETECTION - SCENARIOS

- Insider Threat (Focus is on supporting legal action)
  - Departing Employee Stealing Intellectual Property
  - Disgruntled Employee Sabotage
- Cyber Attack (Focus is on damage control & recovery)
  - Ransomware
  - Data exfiltration / Beaconing
  - Business interruption

DETECTION – OUTBOUND TRAFFIC

- Create 3 Top 20 lists from your outbound traffic logs
  - IP's with the highest number of outbound connections
  - IP's with the longest connection time
  - IP's with the highest amount of transmitted data
- Any IP Addresses that appear on all three lists have a very high probability of being compromised systems

RESPOND - MANAGING THE INCIDENT

ALL INCIDENT TYPES HAVE COMMON ELEMENTS

1. **The Lack of a well thought out incident response plan will provide disastrous results when an incident occurs.**
   - People panic. They revert to self-preservation mode and stop working together under these conditions.
   - Untrained executives, under pressure from the Board of Directors for action will act rashly to appear decisive. Resulting in huge sums of money and critical time wasted on off-target solutions that fail to achieve goals.

2. **The lack of proper administrator training can severely undermine investigations & legal proceedings.**
   - Untrained administrators can unwittingly destroy evidence by:
     - Rebooting servers, destroying volatile memory content.
     - Altering configurations of compromised assets in ways that can make the forensic investigation far more difficult, or, in some cases, impossible.

3. **Appoint an Incident Commander (Tightly Control the flow of Information)**
   - Empowered by senior management to run the incident, in accordance with requirements.
   - Everyone, including senior management, needs to follow this person's directions.

RESPOND – WITH AN OUTSOURCED MSSP

- All costs are transactional, and providers want huge retainers for forensics on demand.
- The period of greatest risk is between the moment an incident is discovered, to the moment forensics staff arrive. During this period, you're reliant on untrained staff, who often lack the expertise to understand what the forensics team will need to be successful.
- Basic Incident Management awareness training for your administrators can make the Incident Management and investigative experience go far more smoothly.

RESPOND - WITH AN IN-HOUSE SOC

- This depends heavily upon the level of in-house capability available. If you lack forensics capabilities, then your action plan will be similar to above. Have this worked out in advance!
- The period of greatest risk is still between the moment an incident is discovered, to the moment forensics staff commence their work.
- Basic Incident Management awareness training for administrators is still critical.

RESPOND - THE FORENSIC PROCESS

(ISO/IEC 27037 ; SEE CYBERCRIME MODULE 4 ON INTRODUCTION TO DIGITAL FORENSICS)

- Collection
- Examination
- Analysis
- Preservation

FIVE RULES FOR COLLECTING DIGITAL EVIDENCE

THERE ARE FIVE GENERAL RULES OF EVIDENCE THAT APPLY TO DIGITAL FORENSICS AND NEED TO BE FOLLOWED IN ORDER FOR EVIDENCE TO BE USEFUL. IGNORING THESE RULES MAKES EVIDENCE INADMISSIBLE, AND YOUR CASE COULD BE THROWN OUT.

- Admissible
- Authentic
- Complete
- Reliable
- Believable

RESPOND – SUCCESS COMES FROM PREPARATION

The first three steps are prepare, prepare and prepare. Identify roles and responsibilities

Time is everything – Need to discover the stage and scope of the attack quickly

Be agile

Remote evidence collection can present challenges

Assets located in geographically dispersed locations. What if the network is down?

Being able to access assets remotely for evidence collection will be critical

If using a third party forensics provider have this relationship established in advance

Discover what your provider will need, in the event of an incident to do their job

- Budget for the retainer that will most likely be required
- Agents installed on servers, network access, etc
- Have this all worked out in advance,to avoid losing valuable time

Know the Privacy, Legal and Reporting Compliance requirements for your jurisdiction

Penalties for publicly traded companies that fail to comply can be substantial

RESPOND - THE MITRE ATT&CK FRAMEWORK

(MITRE ATT&CK (ADVERSARIAL TACTICS, TECHNIQUES, AND COMMON KNOWLEDGE)

MITRE ATT&CK Matrix – 3 Variants - Enterprise, Mobile & ICS (Industrial Control System)

Determine where your attacker is at in the ATT&CK chain

- Reconnaissance (Enterprise, ICS)
- Resource Development (Enterprise, ICS)
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access (Enterprise, Mobile)
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration (Enterprise, Mobile)
- Impact
- Network Effects (Mobile-only)
- Network Service Effects (Mobile-only)
- Inhibit Response Function (ICS-only)
- Impair Process Control (ICS-only)
- Preservation

RECOVER – RESTORE BUSINESS FUNCTION

WHERE THE QUALITY OF IDENTIFY & PROTECT EFFORTS WILL SHOW

Disaster Recovery / Business Continuity.

- Good planning and regularly scheduled live BCP/DR exercises will pay off at this stage.
- In a Ransomware recovery scenario, the main problem isn't recovering applications and data as much as it is having to recover everything, all at once. IT staff can get overwhelmed with the size and scope of the demands for fast recovery.
- Immutable backup strategy with offline backup data storage
- Well thought out network and data segmentation will be what saves you. Limit the blast radius.
  - Single Data repositories, with multi-site replication will not provide a good recovery scenario.
  - Segment Data. Segment networks and segment business critical applications
- **KNOW YOUR CROWN JEWEL APPLICATIONS!!!**
  - Have specific plans to protect and restore their business function based on their priority levels