CYBER-INCIDENT RESPONSE – AN OVERVIEW

WILLIAM (THE GONZ) FLINN

M.S. INFORMATION SYSTEMS SECURITY MANAGEMENT; COMPTIA SECURITY+, I-NET+, NETWORK+; CERTIFIED PATCHLINK ENGINEER

ENTERPRISE INFORMATION SYSTEMS SECURITY MANAGER

HTTP://WWW.GONZOSGARAGE.NET

BILL@GONZOSGARAGE.NET

@COLORADOPREPPER

WHAT IS CYBER-INCIDENT RESPONSE?

- Definition
  - "Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs."
- Essentials of an incident investigation
  - Who, what, where, when, why, and how.
- Qualities of an investigator
  - Curiosity, intuition, problem solving skills, diligence, communication, concise documentation.
- Investigative tools
  - Firewall Logs, SIEM, IDS/IPS, Vulnerability Scanners, Forensics Tools, Anti-Malware, etc.
- CIRT – Computer/Cyber Incident Response Team
  - Investigators and incident handlers, privacy officers, legal staff, public information staff

AGENDA

- The Incident Response Key Players
- Examples of Incident Types
- Incident Handling Process/Phases Overview
- Preparation Phase
- Identification Phase
- Containment Phase
- Eradication Phase
- Recovery Phase
- Lessons Learned
- What You Can Do!
- Resources
- Q&A

THE INCIDENT RESPONSE KEY PLAYERS

- US-CERT - United States Computer Emergency Readiness Team
  - Send alerts and vulnerability information to organizations
- Security Operations Center (SOC)
  - Scans/Monitors the organization's network for malicious/suspicious traffic
  - Originates incidents for the incident handlers
- Computer Incident Response Team (CIRT)
  - Investigates incidents created by the SOC, as well as incidents identified by internal and external customers.
- Service Desk/Help Desk
  - Completes requests created by incident handlers.

THE INCIDENT RESPONSE KEY PLAYERS

- Public Relations/Public Affairs
  - Press releases, announcements, media coordination.
- Legal Staff
  - Advising on legal issues surrounding network breaches, data loss, or PII exposure
- Human Resources
  - Assisting with disciplinary proceedings if misconduct is identified
- Physical Security and Facilities Management
  - Some breaches may be related to physical attacks, unauthorized entry
- Users
  - Savvy and informed users reduce the number of cyber breaches

EXAMPLES OF INCIDENT TYPES

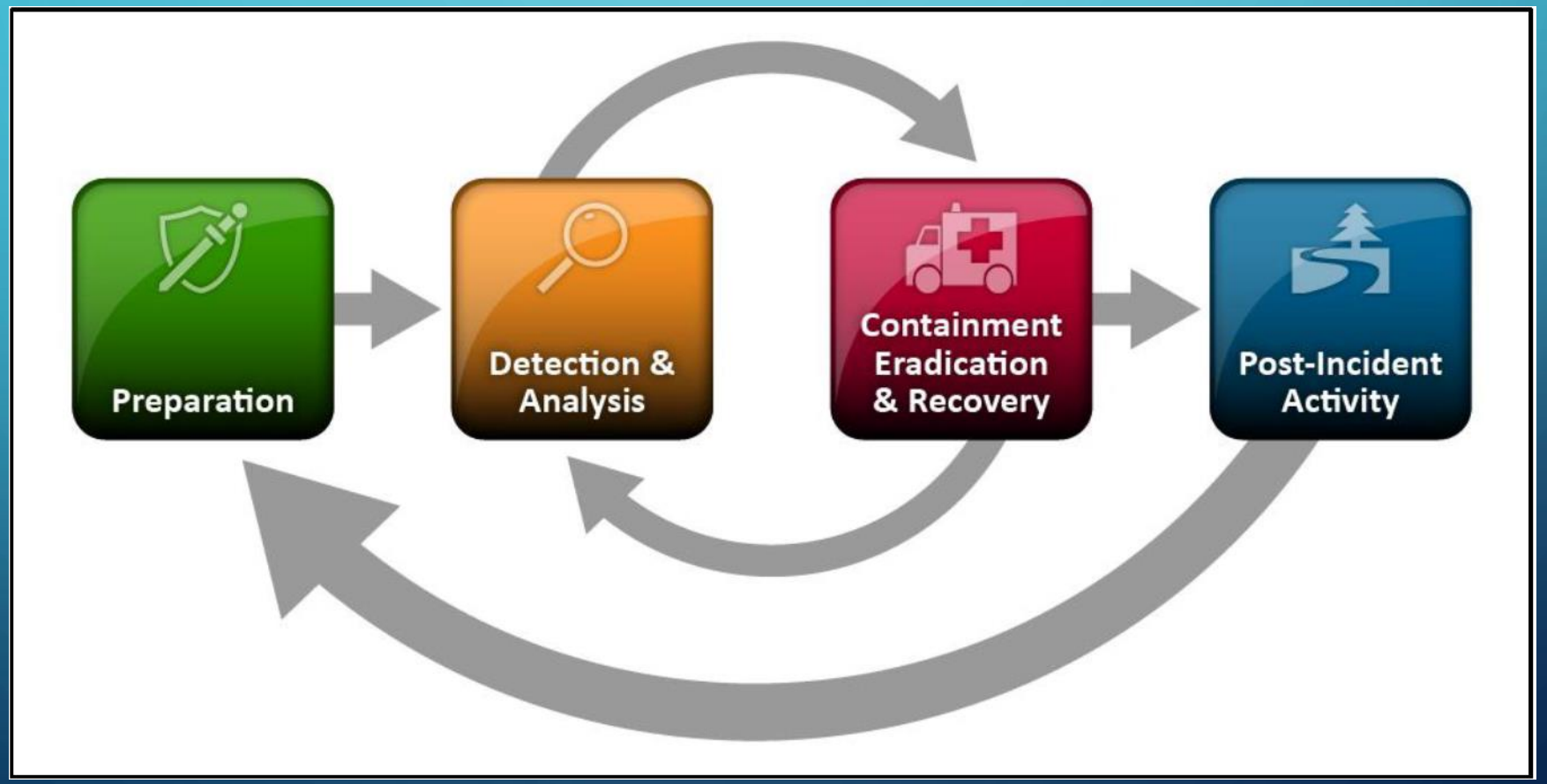
- Cyber Investigations
  - Malware - Trojans, Adware, Ransomware, etc.
  - Data exfiltration
  - Server/Network breaches
  - DoS attacks
- Improper Use Investigations
  - Porn, Gambling, Pirated content, Streaming, Tor, etc.
- Social Engineering Campaigns
  - Phising emails
  - Fake tech support calls
- Personally Identifiable Information (PII) Compromises
  - Exposure of employee or public PII
- Lost/Stolen Hardware
  - May contain corporate proprietary data or personnel information.
  - SmartCards, phones, laptops, tablets, etc.

INCIDENT HANDLING PROCESS/PHASES OVERVIEW

- Preparation
  - Training
  - Developing plans
- Identification
  - Identify the device and/or user involved.
  - Some of this information supplied by the SOC. The rest is derived from other tools
- Containment
  - Prevent the problem from getting worse.
  - Remove computer from network, disable access, etc.
- Eradication
  - Permanently remove the threat.
  - Remote wipes, malware scans, reimaging hardware, etc.
- Recovery
  - Make the system whole again.
  - Issue new devices, return cleaned hardware to network, adjust access controls, etc.
- Lessons learned
  - What happened and how can it be prevented from happening again.
  - Thoughts on policies, procedures, and tools.

INCIDENT RESPONSE LIFECYCLE

SOURCE: NIST 800-61 REV 2



PREPARATION PHASE

- Planning
- Developing SOPs
- Training employees
- Incident response exercises and IR plan testing
- Using lessons learned to update plans and SOPs
- Staying up to date with subscriptions to cyber-threat announcement services

IDENTIFICATION PHASE

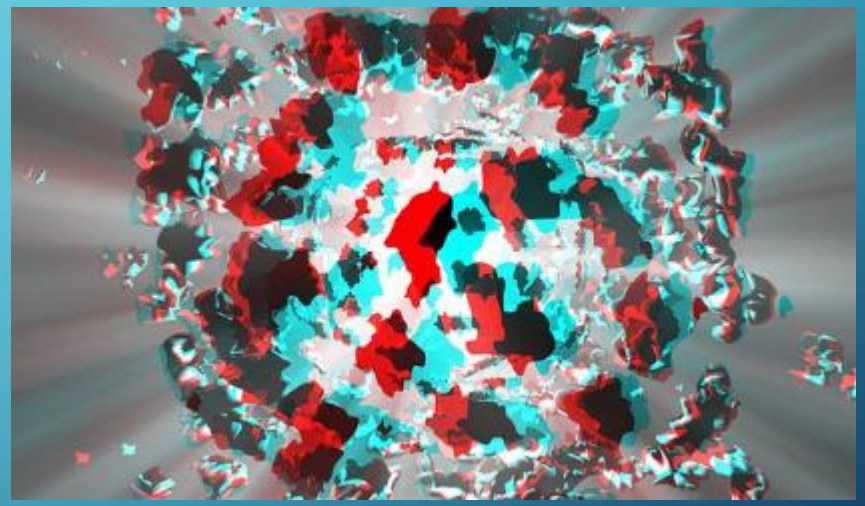
- Is it an event, or an actual incident?
- Looking for deviations from normal.
- Is it unusual activity or normal activity?
- Review SIEM, firewall, AV log files.
- Review computer event logs.
- Assess and prioritize.
- Notify the key players.

CONTAINMENT PHASE

- Stopping the attack, stop the bleeding.
- Minimizing damage.
- Decide whether to shut down the system or leave it operating so as to monitor activity so as to gather more evidence or learn about attack.
  - High value server versus “honeypot” for example.
- Isolating the system.
  - Pulling network cable but leaving unit turned on.
  - Pull logs, perform forensics.
  - Get memory dumps.

ERADICATION PHASE

- Get rid of malicious code.
  - AV tools.
  - Re-image.
- Disable/delete malicious users.
- Firewall and other network blocks.
- Mitigate exploited vulnerabilities.



RECOVERY PHASE

- Restore the system to normal operation.
- Rebuild to authorized baseline configurations.
- Restore clean backups.
- Continue to monitor for unusual behavior.
- Test the “fixes” to ensure that they work.
- Ensure that the incident is fully resolved.

LESSONS LEARNED

- Complete documentation, incident reports, after-action reports.
- How did this attack occur?
- What went well?
- What went wrong?
- What can be done to prevent future similar incidents?
- What can be incorporated into current practices?
- What needs to be done to improve the organization's security posture?

WHAT YOU CAN DO!

- Establish a formal incident response capability.
- Subscribe to organizations who send alerts about vulnerabilities, attack vectors, and emerging threats.
  - US-CERT
  - SANS/Internet Storm Center
  - iSight Partners
- Perform periodic tests and table-top exercises that involve various groups in your organization.
- Develop and regularly update incident response plans, policies, and standard operating procedures.
- Perform skills analysis and make sure your incident handlers have the right training and skills.
- Continually review “lessons learned” and incorporate into plans and procedures.

REFERENCES AND ADDITIONAL RESOURCES

- Dark Reading: The Six Stages of Incident Response
  - https://www.darkreading.com/vulnerabilities-and-threats/the-six-stages-of-incident-response/d/d-id/1059365
- Department of Homeland Security – National Cyber Indicent Response Plan
  - https://www.us-cert.gov/ncirp
- NIST SP800-61 Computer Security Incident Handling Guide (Rev 2)
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Tech Target: Incident Response
  - http://searchsecurity.techtarget.com/definition/incident-response
- US-CERT: Defining Incident response Teams
  - https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams
- SANS Institute: Inforsec Reading Room – Computer Incident Response Team
  - https://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641
- NIST Special Publication: NIST 800-61 R2
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf


Q&A