Crowe Horwath.

Smart decisions. Lasting value.℠

Developing Your Core Incident Response Capabilities

North Texas ISACA

April 2018

Introductions

- Kiel Murray
  - Crowe Horwath Dallas office
  - 10 years experience in Info Sec
  - Public and Private Sectors
  - Pen Testing, Cybersecurity Assessment, Incident Response, Forensics

Objectives

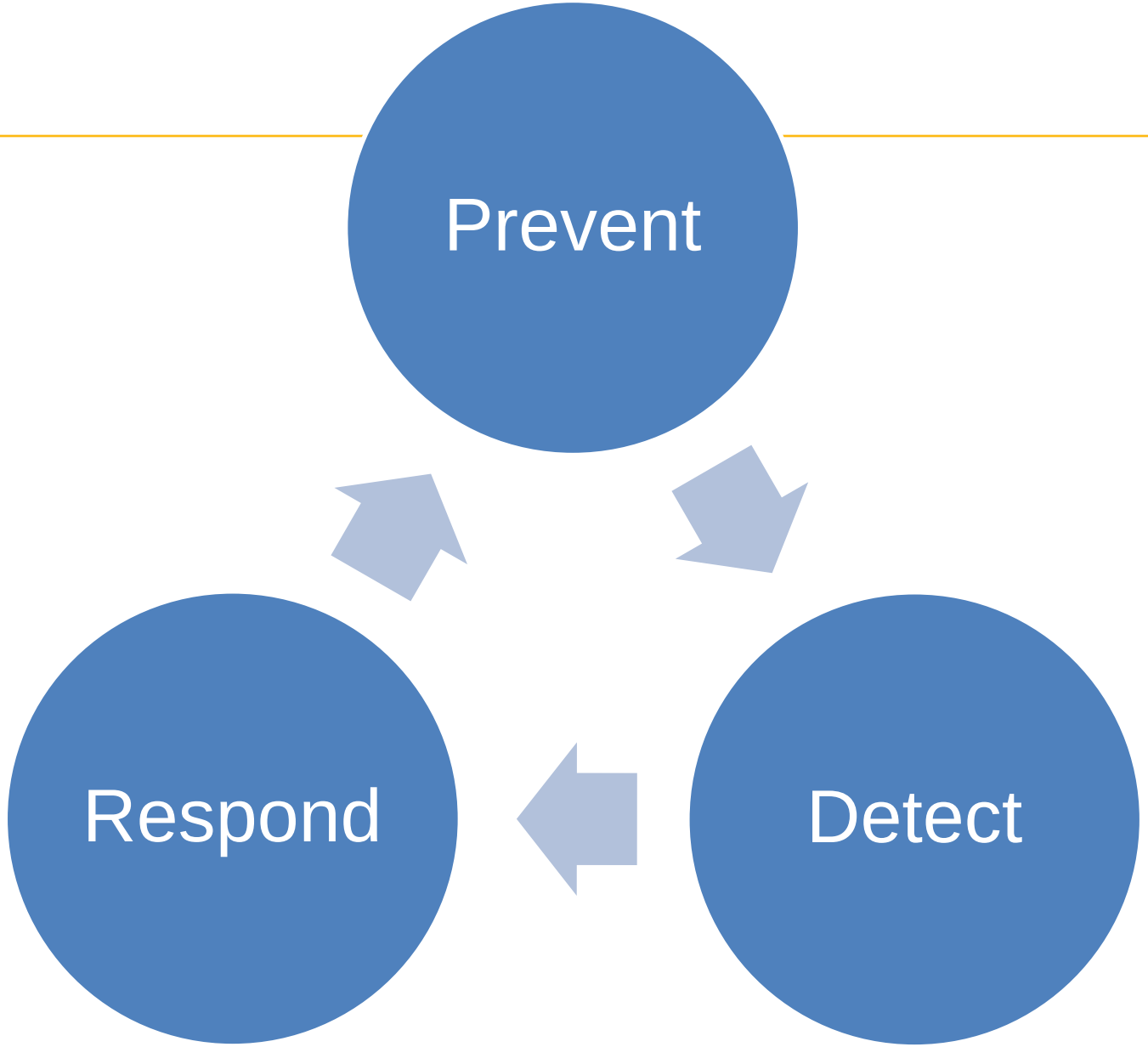
- Identify the National Institute of Standards and Technology (NIST) Incident Response (IR) process
- Key elements of a good incident response plan
- What skills and capabilities are necessary for an effective IR program
- Techniques for overcoming skills or capability shortfalls

Agenda

- IR Lookback and Reflections
- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery

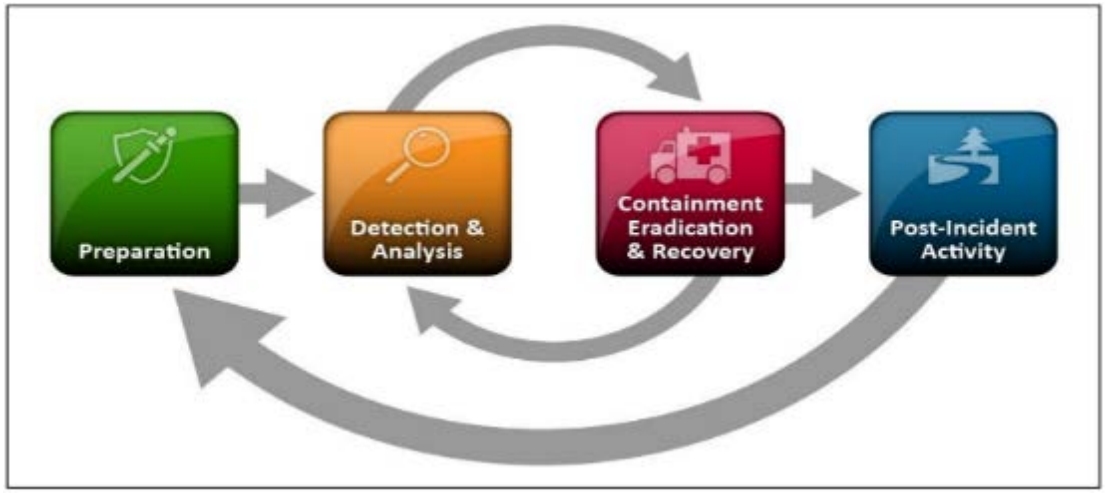
Incident Response Review

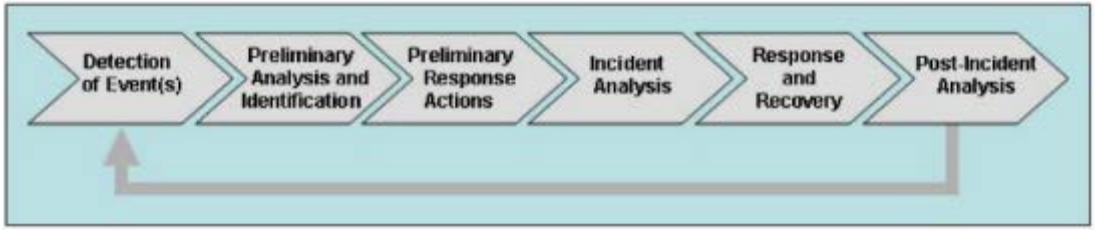
- 2017 Incident Response Update
  - Patching – Apache Struts and WannaCry
  - Ransomware – Continues to be a threat
- 2016 IC3 Report
  - Business Email Compromise – wire fraud
  - Tech support fraud
  - Extortion



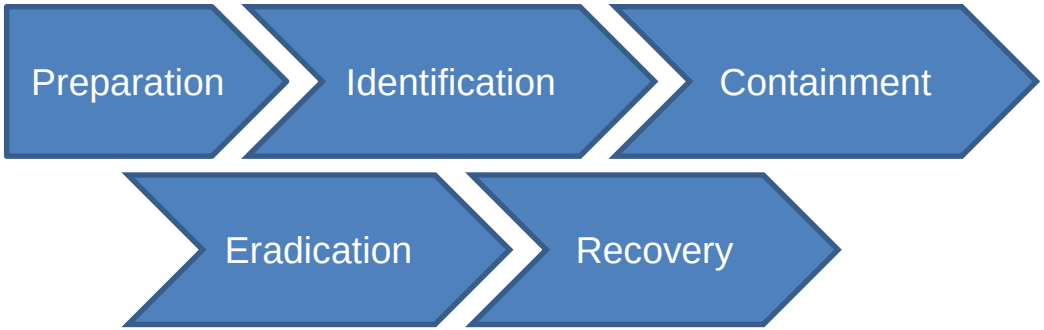
Incident Response Process

NIST





SANS



Preparation – Things YOU can do

- Threat Assessment
  - 2018 DBIR Incident Categories
- Skills Assessment
- Develop a Plan
- Open lines of communication internally and externally
  - Inter-departmental – Legal, HR, PR
  - Law Enforcement
  - Regulators
  - Media
  - Insurance Providers
- Secure Storage

Threat Assessment

- Threat Actors – Nation State, Cyber-criminals, script kiddies, Hacktivism
- Threat Vectors – Social Engineering (phone, email, physical), web sites, 3rd party vendors, malicious insiders, lost/stolen mobile device, wireless
- Threat Impact (Data Classification) – What are the most sensitive data and systems? How can my organization be hurt the most?

Skills Assessment

- Red Team / Aggressor capability
- Simulation and exercise facilitation
- Disk image capture and analysis
- Memory image capture and analysis
- Network traffic capture and analysis
- Malware analysis
- Reverse Engineering
- Indicators of Compromise (IOC) searching
- Threat Intelligence enrichment
- Chain of Custody

Developing a Plan

- Can be done with external help
- Key Elements
  - Purpose/Objective
  - Applicability
  - Responsibility
  - Expected Participants
  - Definitions – Incident, Event, Investigation
  - Incident Lifecycle
  - Requirement to test
  - Documentation
- Optional – Threat Intel, Info Sharing, Testing types, Authority

Preparation – External Help

- Table Top Exercises
  - Scenario development and execution
  - Cross section of Threat Actors, Vectors and Impact
- Live Fire tests
- Possible plan development?

Detection – Things YOU can do

- User education and training
  - Users are a sensor!
- Logging – firewall, netflow, Windows & Active Directory, critical servers, cloud services (O365)
  - Consolidate logs, establish retention period
  - Identify baseline – what does “normal” look like?
- External Notification – Bug Bounty, Responsible Disclosure, Law Enforcement

Detection – External Help

- MSSP – First line of analysis on log data
  - Don’t simply rely on their built in rules
- Penetration Testing / Red Teaming / Purple Teaming
- SIEM and Log Management Review
  - Inputs, Reports, Alerts, Architecture

Detection – Shortcuts – Alerting

- Excessive number of successful logins from same source or same account
- Excessive number of failed logins from same source
- Hostname doesn’t follow naming convention
- Excessive number of administrative logins
- SQL logins from unauthorized systems
- Logins to IT systems with unauthorized account

Analysis – Things YOU can do

- Uptime and Utilization
- Log Analysis – running queries
- Disk Imaging – bare metal, virtualized, cloud, appliance, encryption
- Memory Capture – time sensitive and can hold the only artifacts to an attack

Analysis – External Help

- Disk Image Analysis – timelines, web history, local logs, deleted files, launched programs
- Memory Analysis – running processes, injected binaries, loaded DLLs, active connections
- Malware Analysis – dynamic/static analysis, IOC identification
- Forensic soundness, expert witness testimony

Analysis – Shortcuts

- Malware Analysis – Sandboxes
  - Internal with open source software – Cuckoo
  - Externally Hosted – Free
    - Lenny Zeltser's blog
  - Externally Hosted – Paid

Containment – Things YOU can do

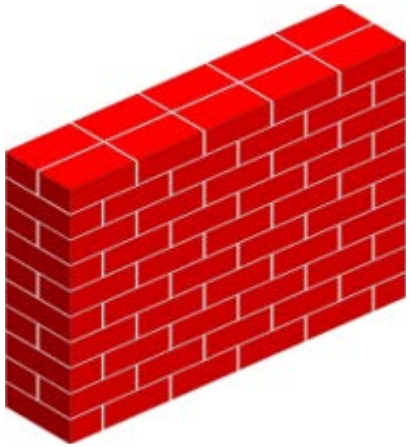
- Physically identify and isolate system based on IP address, MAC address, hostname
- Emergency Patch Deployment
- Mass password reset
- Span port setup
- Identification and Purging of malicious emails
  - Who all just received an email with the subject of “Invoice”

Containment – External Help

- Casting a wider net
- Enterprise wide searching for compromised machines
  - Indicators of compromise
  - Hashes, filenames, processes, active connections
- Network traffic analysis

Eradication

- IP address blocking
- Domain name blocking
- System re-imaging
- Restore from backup
- Rapid Change Control Process
- Approval for business impact



Recovery

- Restoration of normal procedures
  - You took good notes during the incident right?
- External communication
  - Public disclosures, announcements on home page, formal press releases, etc.
- Lessons Learned
- Documentation

Conclusion

- IR Lookback and Reflections
- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery

Q&A

- **Kiel Murray, CISSP, GPEN, GWAPT**
  - Senior Manager
  - kiel.murray@crowehorwath.com

Crowe's Cybersecurity Watch Blog
https://www.crowehorwath.com/cybersecurity-watch/

Thank you for attending!