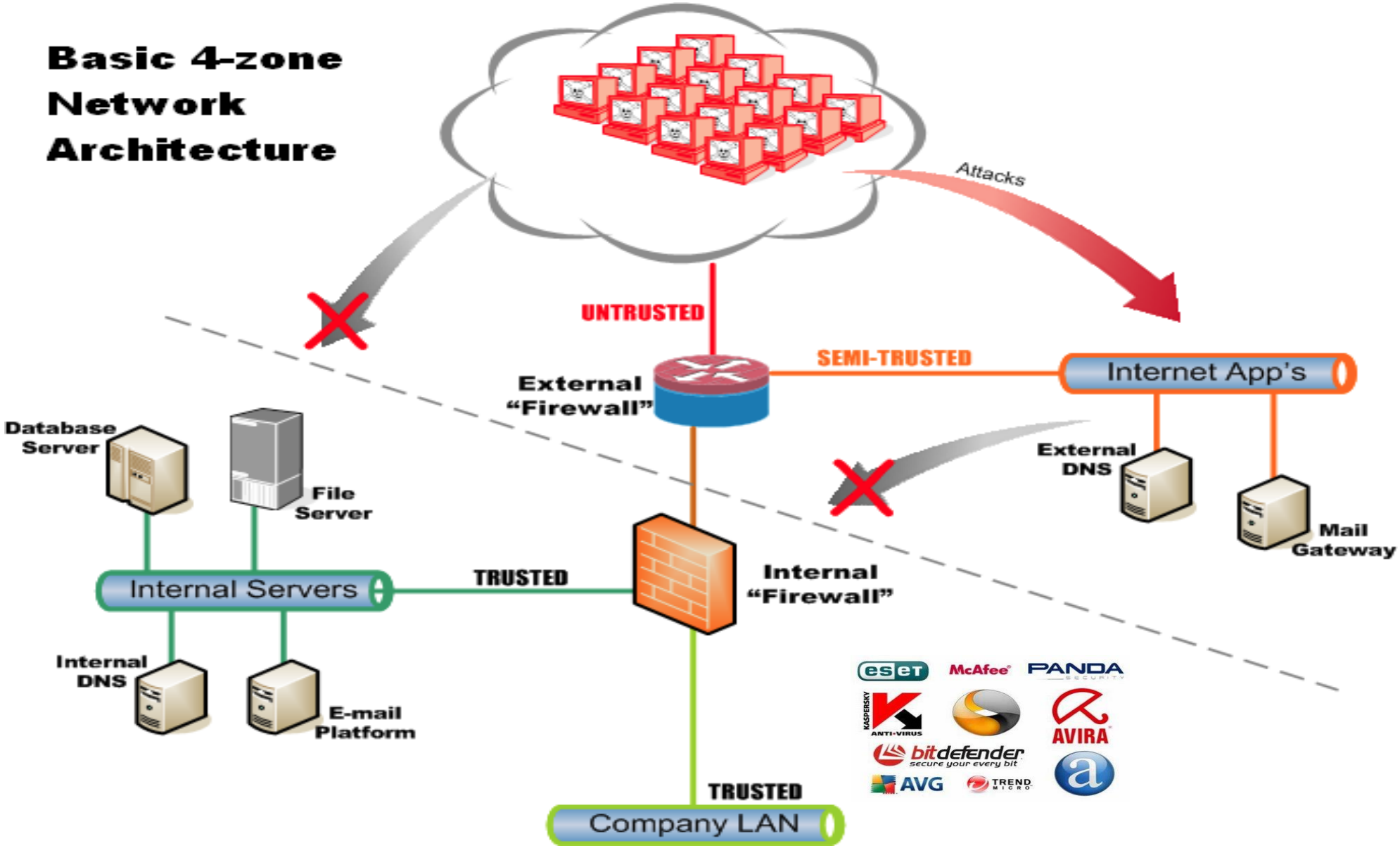
- Introduction
- Preparation
- Protections
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post Incident/Lessons Learned
- Wrap Up

Basic 4-zone Network Architecture



We Have A Problem

It Gets Worse…

Worldwide Information Security Spending

Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015

Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016

Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017

60%

IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

23%

OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

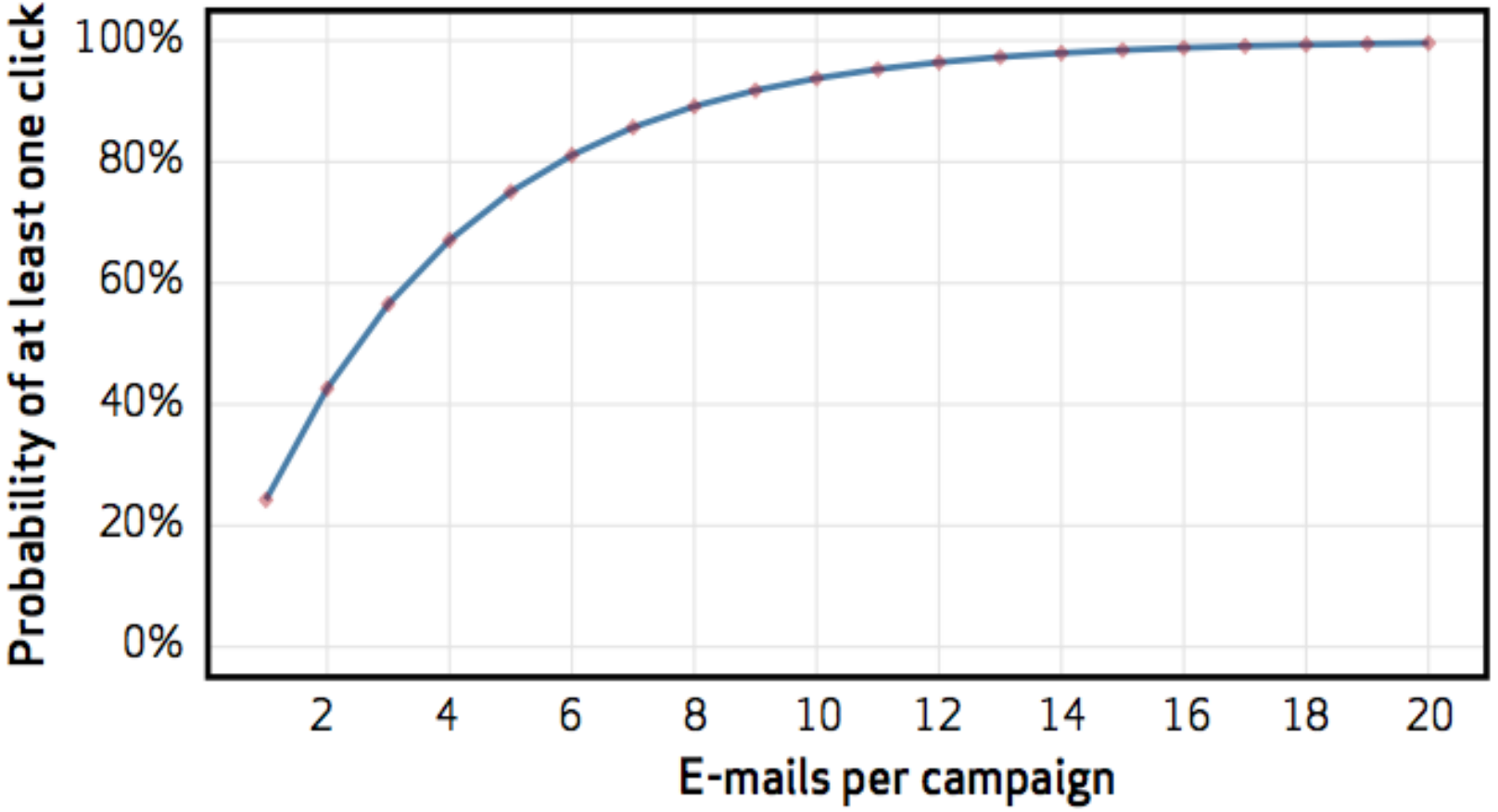
99.9%

OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.

MORE THAN 95% OF ALL ATTACKS TIED TO STATE-AFFILIATED ESPIONAGE EMPLOYED PHISHING AS A MEANS OF ESTABLISHING A FOOTHOLD IN THEIR INTENDED VICTIMS' SYSTEMS.

Why Phishing?

Figure 28: The inevitability of the click



Security Feels Like This Today…

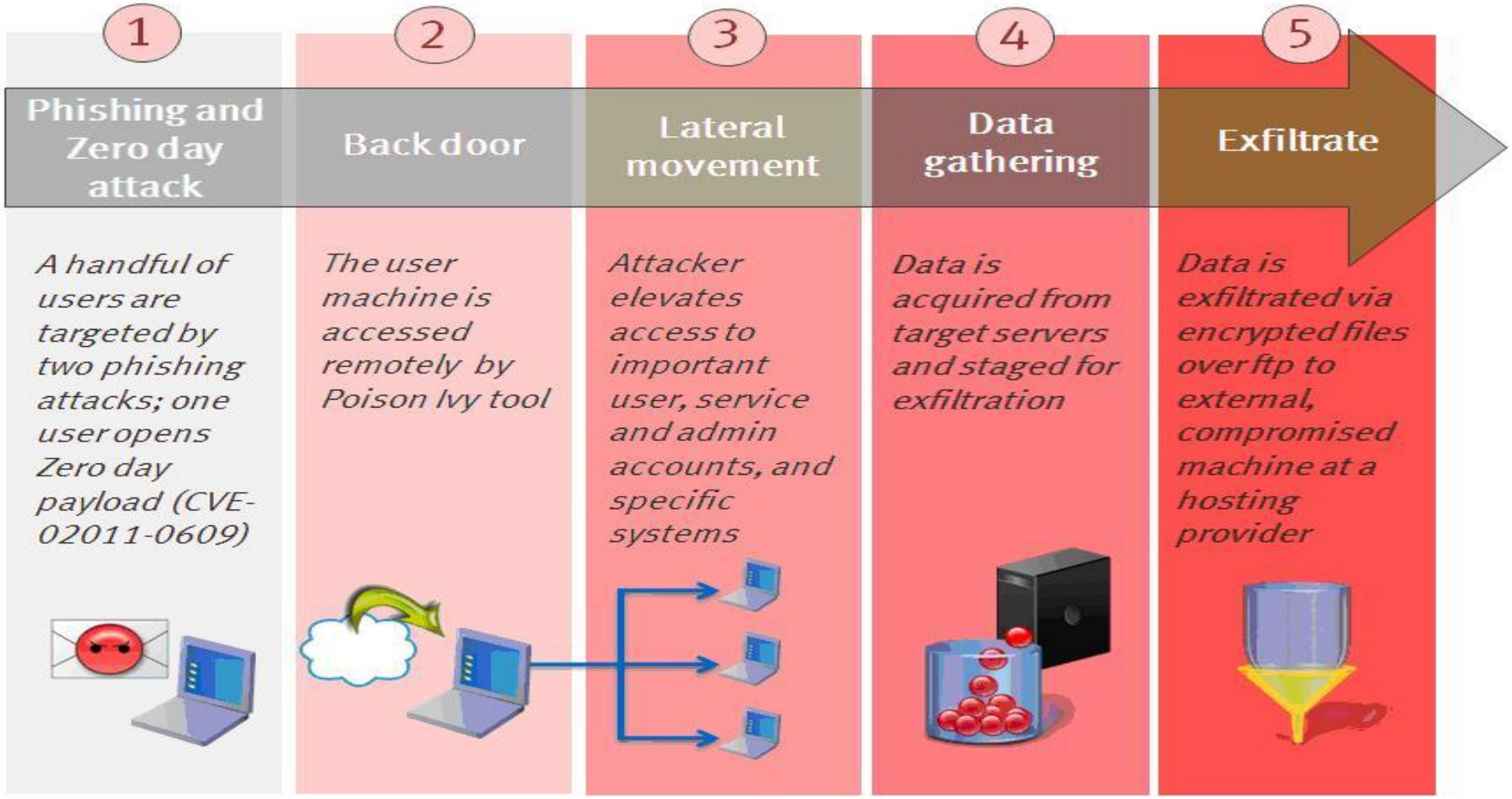
Opportunistic Attacks vs. Targeted Attacks

- Little Planning Involved
- Looking for "Low Hanging Fruit"
- "You" Are Not Targeted
- Only Criteria is a Vulnerable System
- Exploit Not Developed for You
- Not Vulnerable? They Move On

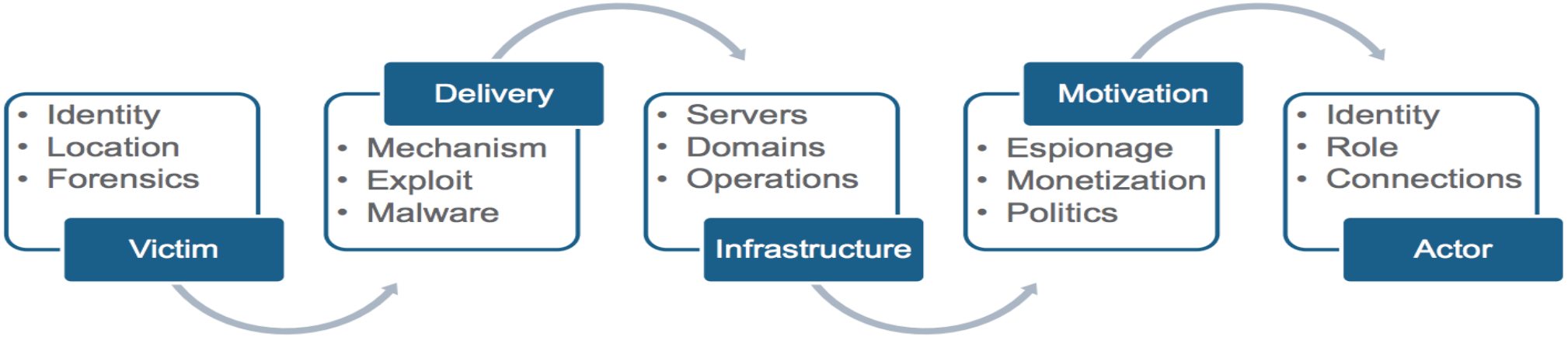
Advanced Attacks

- Different from other attacks
- Not everyone is a target
- Conventional protections are not working

Advanced Attack Methodology



Advanced Threat Campaigns



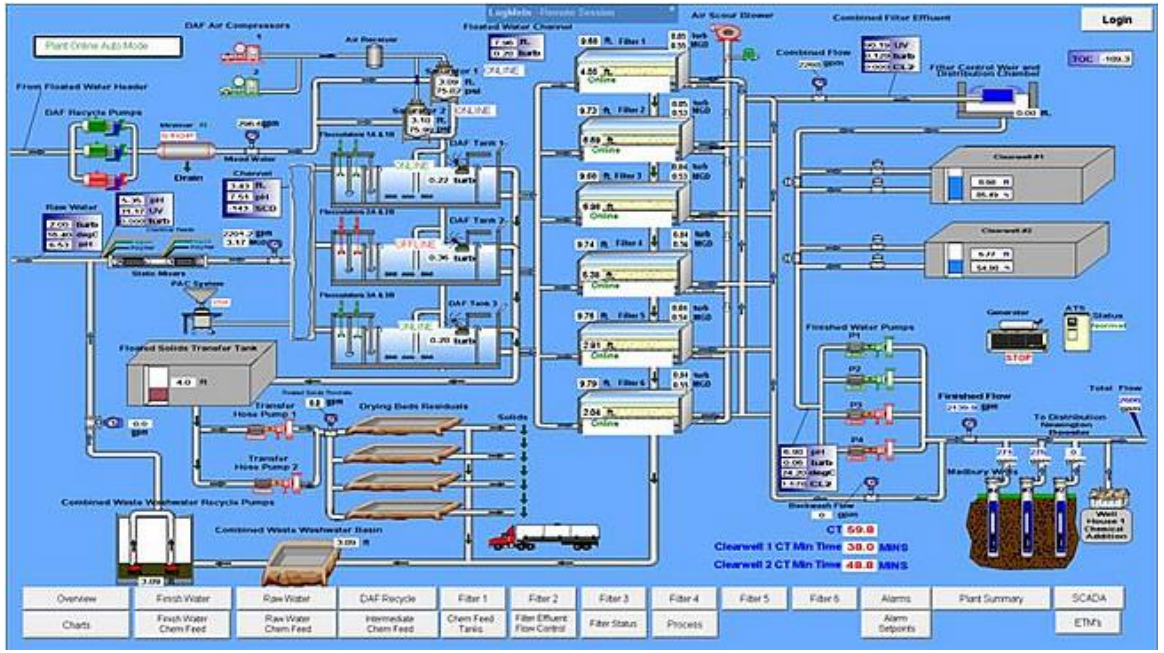
- The total "campaign" involved in an advanced threat scenario has many "moving parts"
- Understanding all of these can help your threat intelligence function immensely

Become a 'Difficult' Target

- We must change our preparation and response
- We must choose the correct tools and leverage available threat intel
- What are you protecting and from who?

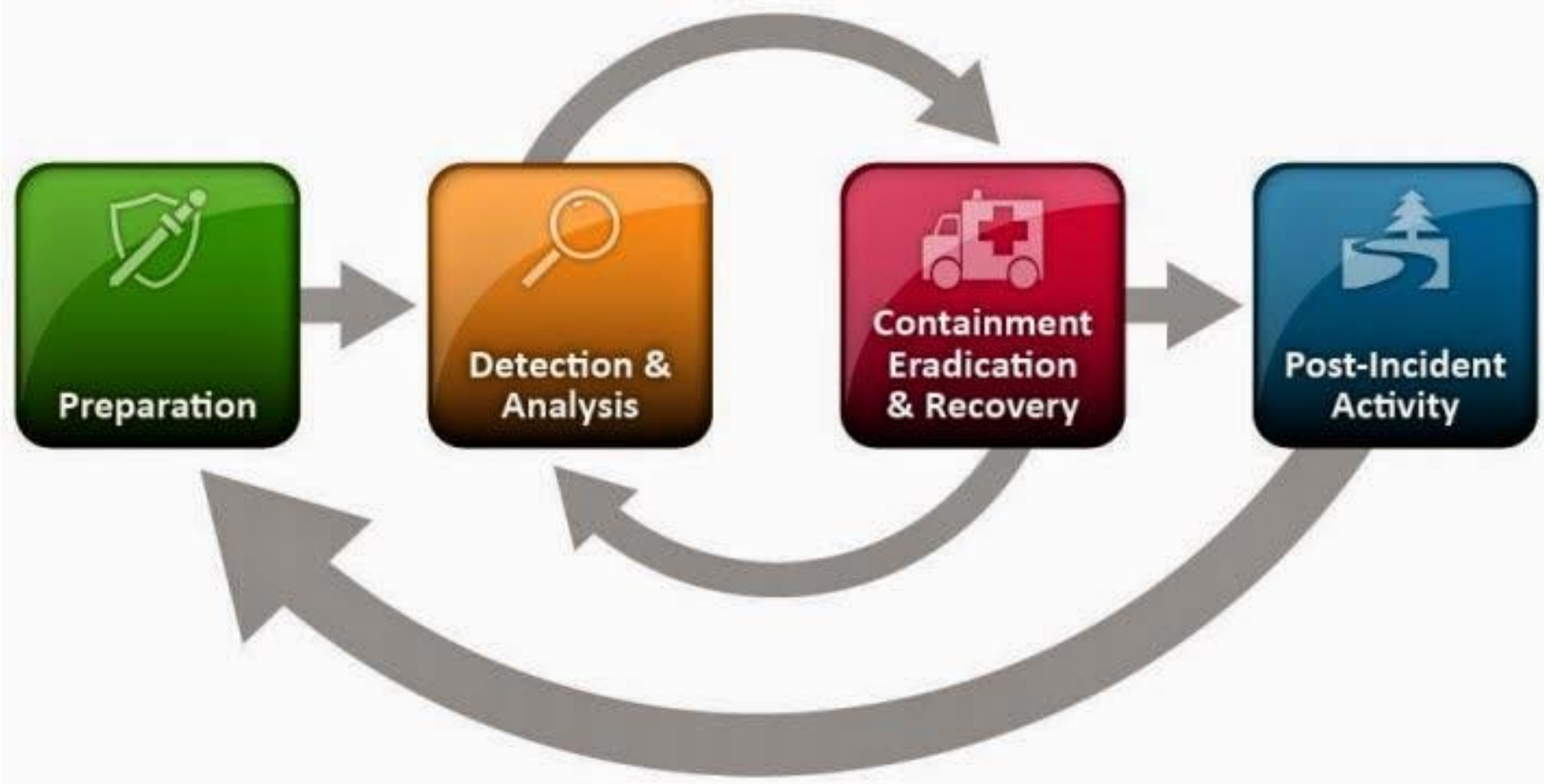
What You Are Not Protecting

What You Are Protecting



Detection and Response - 2001

The “Steady State” Model



- Introduction
- Preparation
- Protections
- Detection and Analysis
- Containment, Eradication and Recovery
- Post Incident/Lessons Learned
- Wrap Up

Preparation

- Develop a Program
  - Incident response can be a high-stress time. A well documented policy/procedure, that is easy to follow, can greatly reduce the anxiety
- Develop a call tree and notification procedures
  - Brainstorm likely scenarios
  - Identify general information needed in most scenarios ahead of time
  - Make checklists and playbooks for as much as possible

Preparation

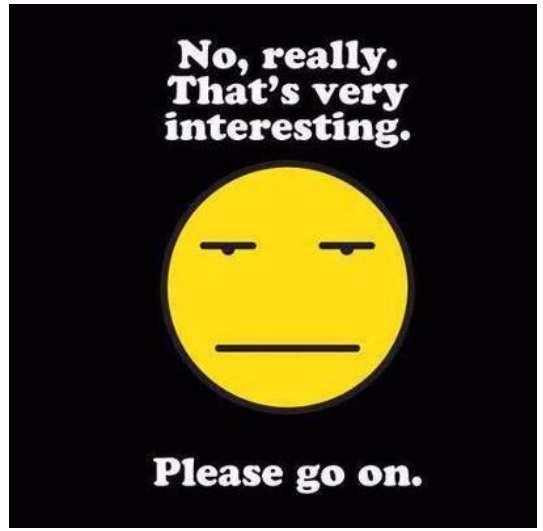
- Identify the “Core Team”
  - Technical (IT, InfoSec and System Owners)
  - Management
  - Legal Department
  - Forensics
  - Public Relations
  - Human Resources
  - Physical Security and Maintenance
  - Telecommunications

Preparation

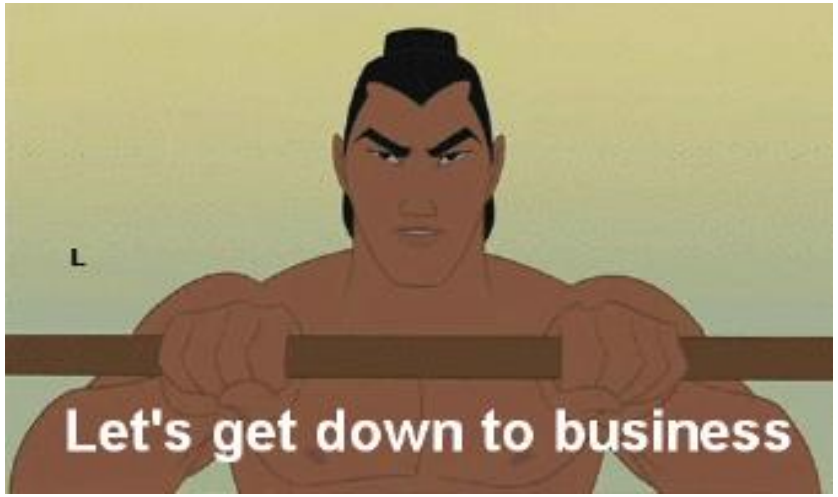
- Organizing Individuals
  - All members of the CSIRT team should know their role and how they will interact with the other members
  - Outsourced or “third party” members should have contracts in place
  - Contacts for Law Enforcement should be known and situations for their involvement discussed

Preparation: Policies

- Protect the organization from legal liability and allow investigators to do their job
- Warning Banners are readily displayed
- Search policy is detailed in employee manual
- Human Resources and Legal have signed off
- Employees have acknowledged knowing their expectations on privacy



Incident Definitions



- What types of incident definitions do you have?
  - "Events" vs. "Incidents"
  - "Compromise" vs. "Breach"
- What categories do you use, if any?
  - Ransomware, DDoS, BEC, data exfil, malware, fraud, insider, etc.
  - Severities?
- What different procedures will you establish for each type?

Preparation

- Preparation: Security analysts build processes and policies, and also train in advance of actual incidents
- Common aspects of the preparation phase:
  - Practicing with tools
  - Learning about new attacks
  - Unannounced penetration tests
  - Building channels of communication with law enforcement, peer groups, and internal stakeholders

Preparation

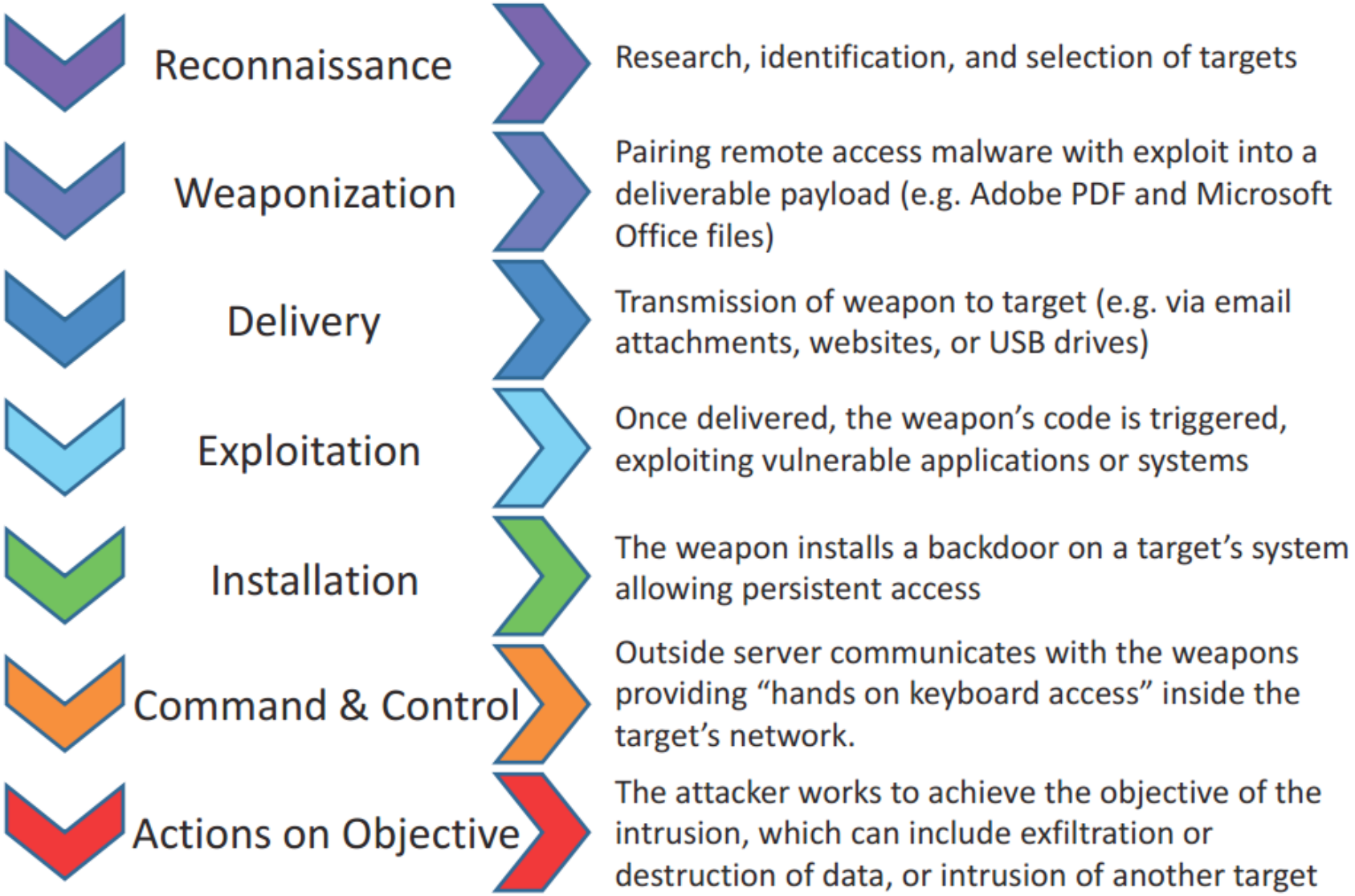
- Communication
  - Communication is incredibly important during an incident
  - Not only the people involved, but the method which it is done
- Updates should be frequent
- Out-of-Band Communications are very important.
  - Secure Bridge Lines
  - Cell Phones
  - Be careful with smartphones, especially Android devices

Preparation: Gathering Resources

- Incident analysts should have all information ready and be able to respond to the incident
  - Procedures, Checklists and Forms are available
  - Access credentials are available or individuals with them are known
  - System information, network diagrams, software and intellectual property are documented thoroughly
- Tabletop Exercises

- Introduction
- Preparation
- Protections
- Detection and Analysis
- Containment, Eradication and Recovery
- Post Incident/Lessons Learned
- Wrap Up

Phases of the Intrusion Kill Chain



“Old School” Protections

- Anti-virus
- Firewalls
- IDS/IPS
- HIPS/HIDS
- Web Content Control
- WAF
- DDoS Protections
- Spam Filters
- Honeypots / Honeynets

“Emerging” Protections

- NextGen Firewalls
- Binary Detonation (FireEye, Wildfire, etc.)
- Application Isolation/Virtualization
- Whitelisting
- NextGen AVs (Cylance, Crowdstrike, etc.)
- Threat Intelligence
- Upstream WAF and DDoS Protection
- Endpoint Visibility (Crowdstrike, Carbon Black, etc.)

- Introduction
- Preparation
- Protections
- Detection and Analysis
- Containment, Eradication and Recovery
- Post Incident/Lessons Learned
- Wrap Up

Detection: Define the Types of Attack

- What type of attack may you be facing?
  - Network scans and recon
  - DDoS
  - Automated malware (worms, bots)
  - More advanced malware
  - Targeted attacks
  - Application exploits and data loss
  - Social engineering (Phishing, Pre-texting, etc)
  - Insider attacks

Detection Challenges Today

- Lots of disparate tools and platforms are generating an overwhelming amount of data
- Security teams are trying to incorporate numerous controls with detection events into their response processes, and it can be easy to miss events and indicators of compromise in all the noise
- Many security teams are also using manual processes to initiate incident investigations and follow through with containment and elimination steps
  - This can be a slow process!

“Global” Detection Technologies

- Proactive Detection includes:
  - Network Intrusion Detection/Prevention System (NIDS/NIPS)
  - Host Intrusion Detection/Prevention System (HIDS/HIPS)
  - Includes Personal Firewalls
  - Security Information and Event Management (Logs)
  - Vulnerability Assessments/Penetration Testing
- Reactive Detection: Reports of unusual or suspicious activity

Client-Side Detection Tools

- Antivirus: Security analysts may still find value in antivirus quarantine for containment
- Malware Tools: Sometime AV doesn't cut it and more reactive scans are needed
- HIPS (i.e. SEP)
- Other techniques:
  - Endpoint Visibility
  - Virtualization containment
  - Files encrypting
  - Machine Learning (Next-Gen AV)

Detection: Suspicious Events

- Unexplained Occurrences
  - New Accounts or Files
  - IDS Triggers
  - Firewall Log Entries
  - Poor Performance/Unresponsive services
  - System Instability
  - Large Egress File Transfers
  - Google Flags You As “Dangerous”
  - Files Encrypting

Detection: Stop Being Passive!!

- Look For Your Own Incidents
  - Majority of Notification is Third Party.. Don't be a Statistic..
  - Leverage Quality Threat Intelligence (if You Can)
  - Retain and Analyze Netflows (Full Packet Capture Rocks)
  - Look for "Bad" Binaries Across the Board
  - Hunt for the Malware Compromises

Analysis: Forensic Analysis

- Who needs to know?
- What visibility do you have?
- What forensic evidence do you have? Not have?
- Preserve the evidence you have!
- What forensics tools do you have?
- What forensics expertise do you have?
- If an active intrusion, do you know how to not "alert" the adversary?
- Do you need third party help?

- Introduction
- Preparation
- Protections
- Detection and Analysis
- Containment, Eradication and Recovery
- Post Incident/Lessons Learned
- Wrap Up

Eradication

- Eradication: The eradication phase is centered on remediation and removal of attacker artifacts
  - Response teams will stop processes, remove files, terminate connections, or wipe systems entirely
- When do you eradicate?
  - Immediately?
  - After all evidence acquired?
  - Once root cause is identified?

- If your approach is “watch and learn”, eradication may not take place for some time

Containment: Proceed Carefully

- Containment: The containment phase is focused on "stopping the bleeding" during an incident
  - Quarantine and isolate affected systems and determine the source(s) of attack generation
  - "Watch and observe" or "contain and terminate"
  - Network tools, host-based controls, and virtualization can help
  - Forensic evidence acquisition is key **PRIOR TO THIS PHASE COMPLETING**

Containment: What should you choose?

- Network isolation/blocking
- Host isolation/blocking
- Network or host anti-malware tools
- Physical disconnect or power shutdown
- Mission critical system…Deal with it
- Many define both Long-term and Short-term containment

Recovery

- Recovery: Incident response teams will facilitate systems and applications returning to normal production service
  - Operations teams will do much of the work
  - Incident handlers may implement new detection and alerting rules based on specific evidence
- Keys to success:
  - Workstations infected? Re-image after proper preservation (no more discussion)
  - Work closely with Ops
  - Monitor systems carefully, in "off hours" if possible
  - Harden and penetration test before deployment
  - Look for IOC signs – did you really resolve the issue?
  - Patience

- Introduction
- Preparation
- Protections
- Detection and Analysis
- Containment, Eradication and Recovery
- Post Incident/Lessons Learned
- Wrap Up

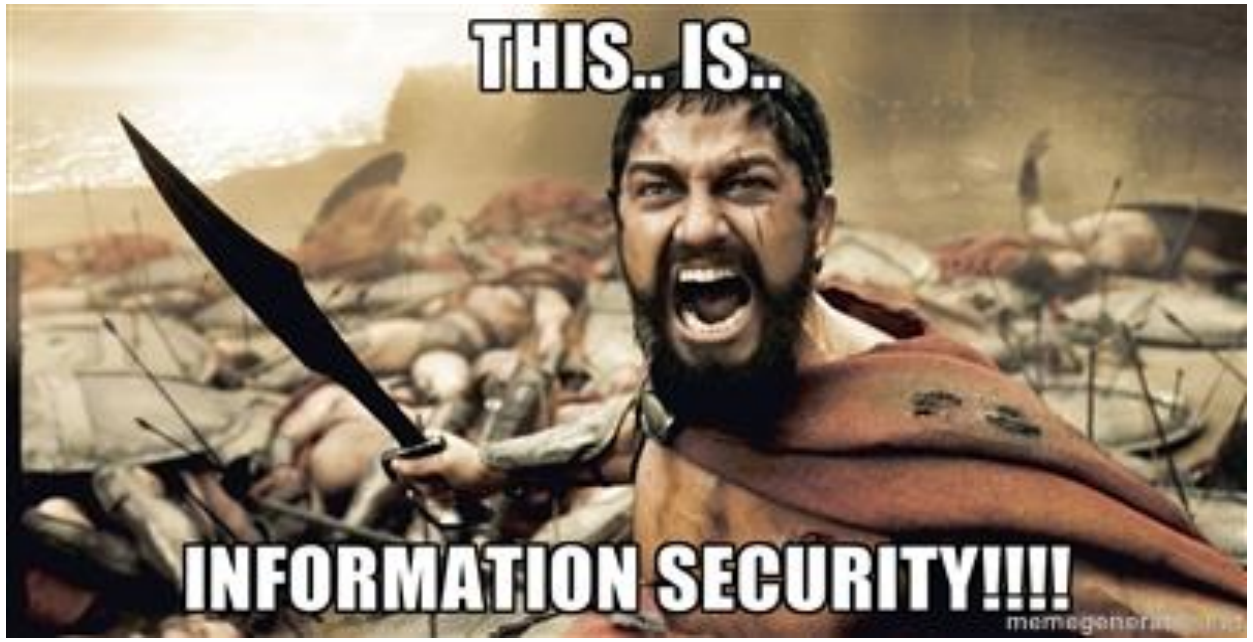
Post Incident/Lessons Learned

- Lessons Learned: Teams write up final investigations reports, documenting what happened and how (if known)
  - Next steps are also discussed, along with any potential shortcomings in security controls and process gaps that may have allowed the intrusion to occur
  - Final evidence is collected and/or disseminated, as well
  - What technology investment$ "may" prevent this in the future?
- These are critical steps that many gloss over
  - The "Big 5" – What?, When?, Where?, How? (Maybe "Who")
  - Budget may be acquired
  - Final reports and evidence are filed..Not a normal report

What's Next?

- 66% (or so) of organizations are breached for months or more before they realize it – we aren't doing *something* right
  - A renewed sense of urgency and broadening of scope in attack detection and response automation is happening
- How do we implement and apply incident response planning?
  - Identify stakeholders/participants
  - Develop a CSIRT project plan
  - Define range, scope, and type of services from CSIRT
  - Document the workflow
  - Develop policies and processes
  - Don't be passive
  - Practice!

- Introduction
- Preparation
- Protections
- Detection and Analysis
- Containment, Eradication and Recovery
- Post Incident/Lessons Learned
- Wrap Up



Questions?

armor up

Comprehensive defense for your data.

Bill Dean, CCE
bdean@lbmc.com
(865) 862-3051

LBMC Information Security - a full spectrum of services

Compliance and Audit Services

Navigate the complex maze of compliance regulations

- HIPAA / HITRUST
- Security Controls Assessment (SCA)
- CMS / FISMA / NIST
- FedRAMP / CSA CCM
- Service Organization Control (SOC)
- SOX / COSO
- Payment Card Industry (PCI)

Managed Security Services

Minimize threats and respond

- Intrusion prevention and detection services
- Security information and event management
- Incident response and forensics
- Vulnerability and threat management

Security Consulting

Tap in to our unaffiliated and objective assessments

- Risk assessment / current state assessments
- Security program design and implementation
- Penetration testing
- Web application assessments

LBMC INFORMATION SECURITY