Auditing and Cyber Security

Blake Bryant

7 December 2017

KU ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
SCHOOL OF ENGINEERING

Agenda

- Introduction
- Auditing in Cyber Security
- Incident Response Framework Overview
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Breach Consequences
- Questions

Introduction: Who Am I

- Professional Background
  - Current Professor of Practice at University of Kansas
  - Previous experience as:
    - Cyber Security Consultant
    - SOC Operations Manger
    - SIEM Engineer
    - Network Engineer
    - Security Analyst
- Education:
  - BS Information Systems Engineering USMA
  - MS Information Technology and Security University of Kansas
  - Enrolled in Doctoral program at University of Kansas
- Certifications:
  - CISSP
  - Microsoft Certified Professional (multiple disciplines)
  - Cisco: CCNA, CCNA Security
  - COMPTIA (Security+, Network+)
  - SIEM: (LogRhythm, Qradar, Splunk)
  - Offensive Security (7Safe CSTA)

Auditing in Cybersecurity (1 of 3)

- An **information technology audit**, or **information systems audit**, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. - Wikipedia

Auditing in Cybersecurity (2 of 3)

- Why conduct auditing?
  - Prove you are doing the right thing:
    - Verify due diligence in securing assets
    - Verify adherence to approved methodologies/regulations
  - Find someone doing the wrong thing:
    - Identify/Confirm past security breaches
    - Verify health of information systems

Auditing in Cybersecurity (3 of 3) :

ISACA: 10 things auditors should know about cyber security

- Leverage existing frameworks/guidelines
- Consider forthcoming legislation
- All risks are subjective
- Users are (and will always be) the biggest security risk
- Basic information security controls still hold true
- Need a cyber incident response policy and plan that is fully tested
- Cyber security strategy needs to be agile – landscape is “mutating”
- Cyber security awareness depends on the right training
- Everything is connected to everything
- Be aware of credential theft techniques

Source: http://www.isaca.org/Knowledge-Center/Research/Documents/Auditing-Cyber-Security-Infographic_ifg_eng_0217.pdf

Incident Response Frameworks: What is Incident Response? (1 of 4)

- Incident response is a methodical approach to dealing with adverse or abnormal events experienced within an information system or network.

Incident Response Frameworks (2 of 4)

NIST Cyber Security Framework

- Identify
- Protect
- Detect
- Respond
- Recover

NIST 800-61 r2 – Computer Incident Handling Guide

- Prepare
- Detect
- Respond (contain, eradicate, recover)
- Post incident (lessons learned, evidence retention)

Incident Response Frameworks (3 of 4)

NIST 800-37– Applying the Risk Management Framework

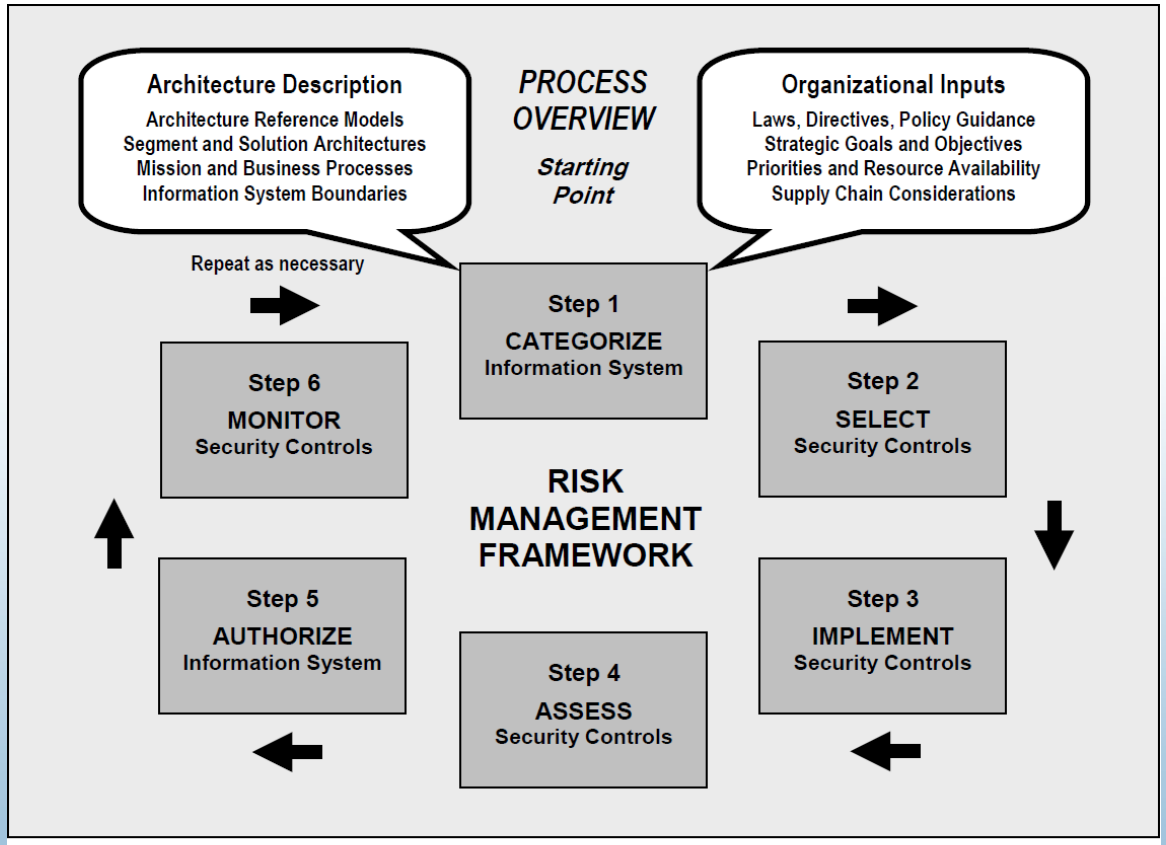


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

Incident Response Frameworks (4 of 4)

NIST 800-86 - Guide to Integrating Forensic Techniques into Incident Response

- Data Collection
- Examination
- Analysis
- Reporting
- Recommendations

Identify: Definition (1 of 4)

- The identification phase consists of Identifying: assets, threats, controls, and risk
  - Assets: things of value to the organization (data, systems, bandwidth, capital etc.)
  - Threats: things that may damage assets or impede business operations (hackers, natural disasters, power outages, regulatory audits etc.)
  - Risk: probability that a threat will impact an asset
  - Controls: administrative or technical processes or systems that may reduce risk to systems

Identify: Assets (2 of 4)

Open Systems Interconnection (OSI) Model

Application	to:person@mail.com			
Presentation	<!doctype html><html itemscope="" itemtype="http://schema.org/SearchResultsPage" lang="en">			
Session	Session ID: D30200006A3E0CB4785A869922514DC3657AC5177D4			
Transport	to:person@mail.com	TCP		
Network	to:person@mail.com	TCP	IP	
Data	to:person@mail.com	TCP	IP	ETHERNET
Physical	10001110101			

Identify: Threats (3 of 4)

Each Layer of the OSI Model is Susceptible to an Attack



Application	Virus, Trojan, Buffer Overflow
Presentation	SQL Injection, XSS
Session	Session Hijacking
Transport	Protocol Spoofing, DNS Poisoning
Network	IP Spoofing
Data	ARP Poisoning, MAC-Address Spoofing
Physical	Wire Tapping, Cross-Domain-Violation, Signal Interception



Identify: Controls (4 of 4)

Protection Systems/Mechanisms Typically Focus on a Specific Layer

Application	Anti-Virus, Application Permissions
Presentation	Proxy, Input Validation, Code Signing
Session	Public Key Infrastructure (PKI)
Transport	Firewall
Network	Firewall, Intrusion Detection System
Data	Port Security, Wireless Encryption
Physical	Secure Conduit, Locks, Cages, Spectrum Management

Protect: Definition (1 of 3)

- Protection is the implementation of security controls to reduce risk within an environment.
- Must evaluate risk first
  - Risk = threat x vulnerability x impact
- Quantify risk in terms of cost to business
- Determine how to address risk
  - Avoid: Remove vulnerable systems entirely
  - Mitigate: Implement controls (administrative/technical)
  - Transfer: Coordinate with a third party to assume some or all of the risk (outsource, insurance etc.)

Protect: Risk Management Framework (2 of 3)

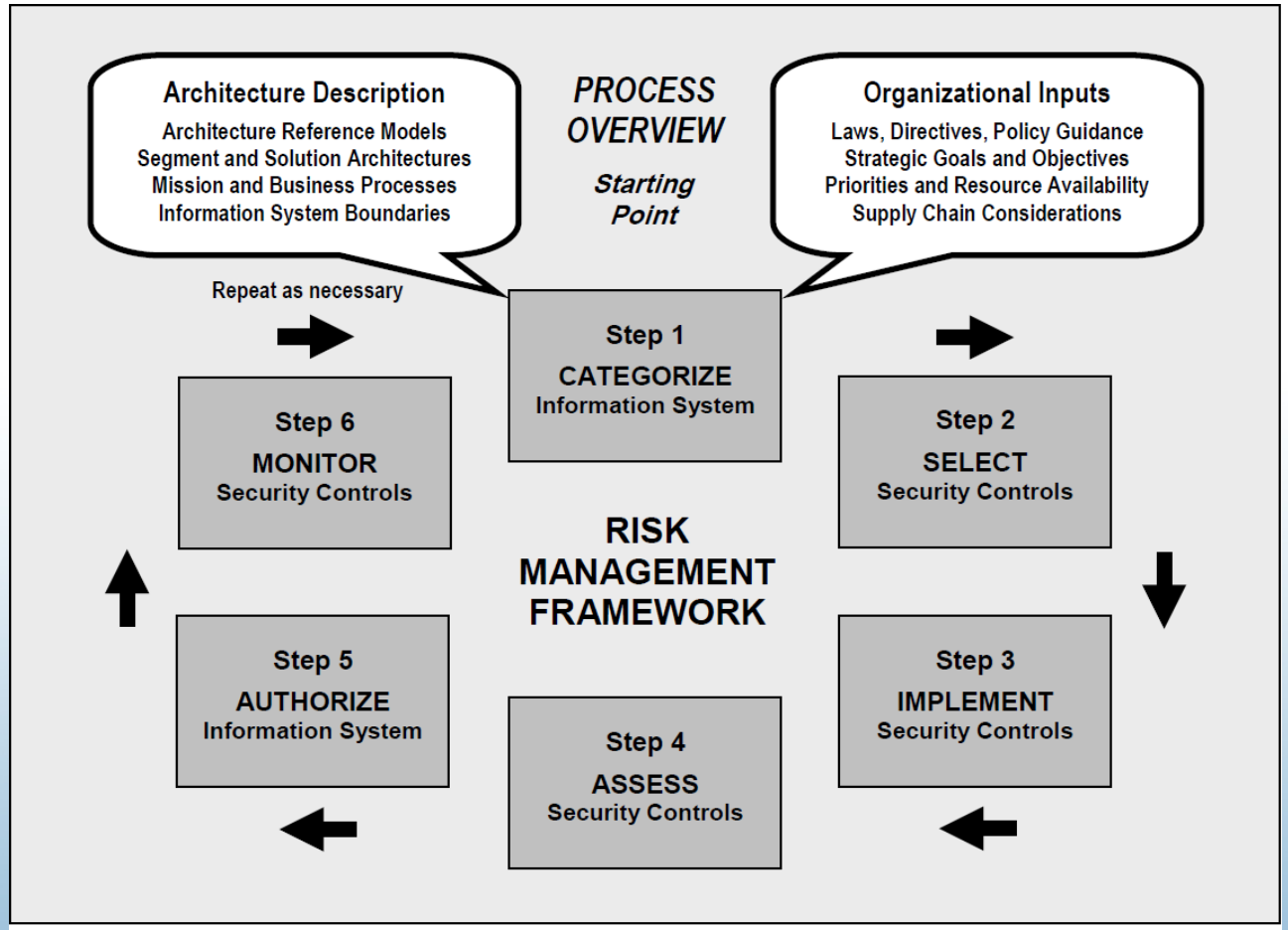
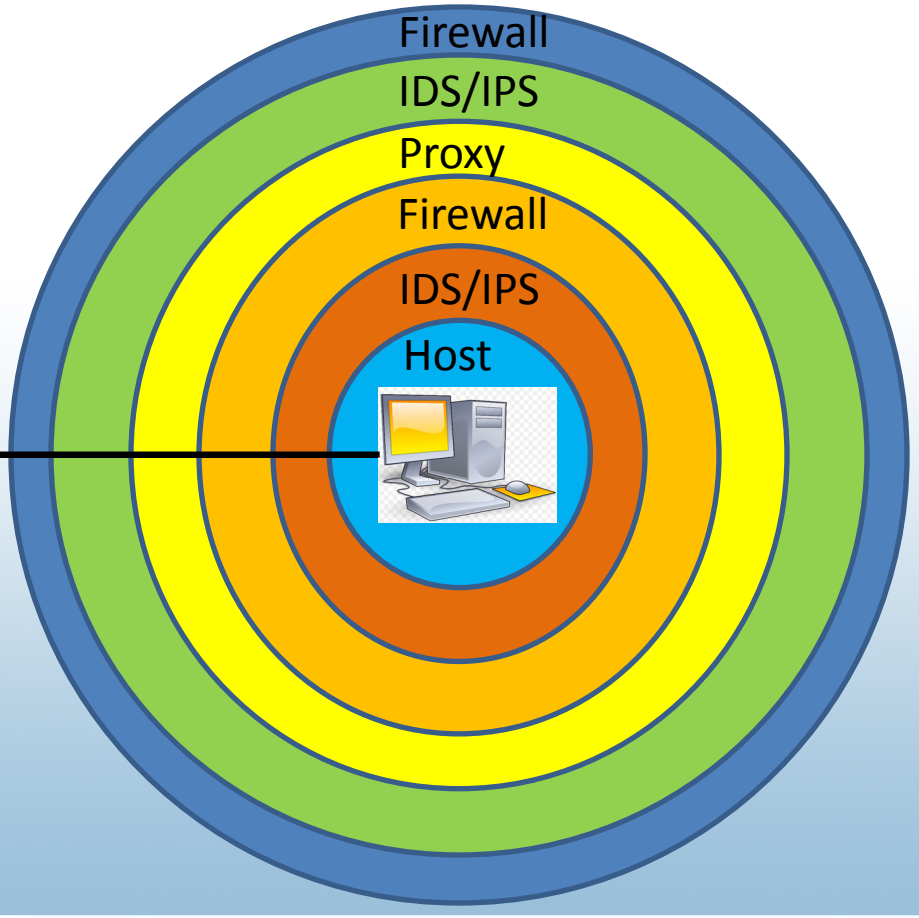


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

Protect: Selection (3 of 3)

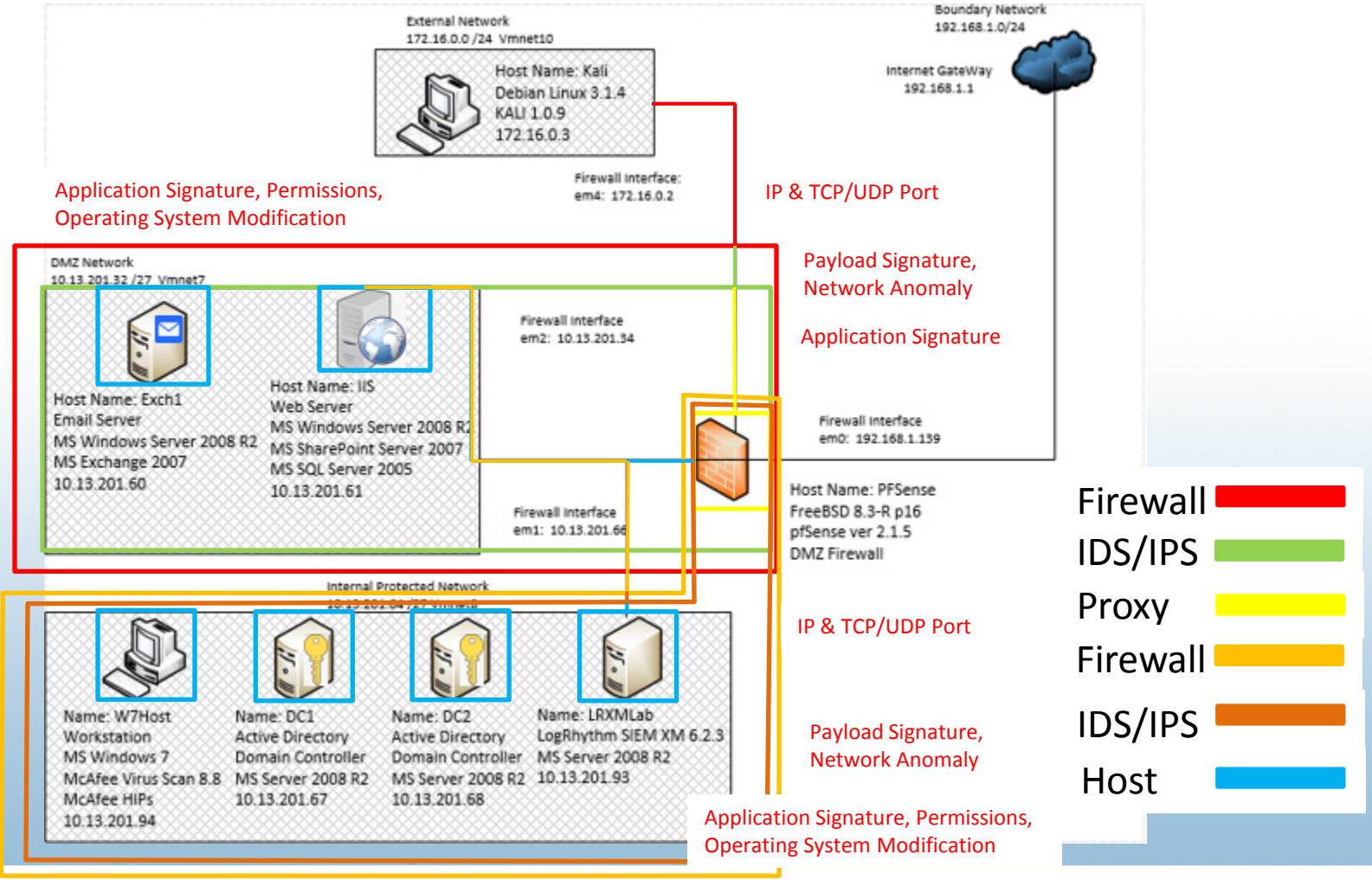
- Network Firewall
- IDS/IPS
- Proxy/Bastion Host
- Network Segmentation
- Host Based IDS/IPS
- Host Based Anti-Malware
- Operating System Permissions



Detect: Definition (1 of 2)

- The detect phase consists of confirming whether or not an incident has occurred
- This phase is highly dependent upon:
  - Network topology
  - Security control deployment
  - Audit log configuration (volume, coverage, verbosity)
  - Alerting/Correlation systems
  - Analyst expertise
  - Organizational policies, procedures, and discipline

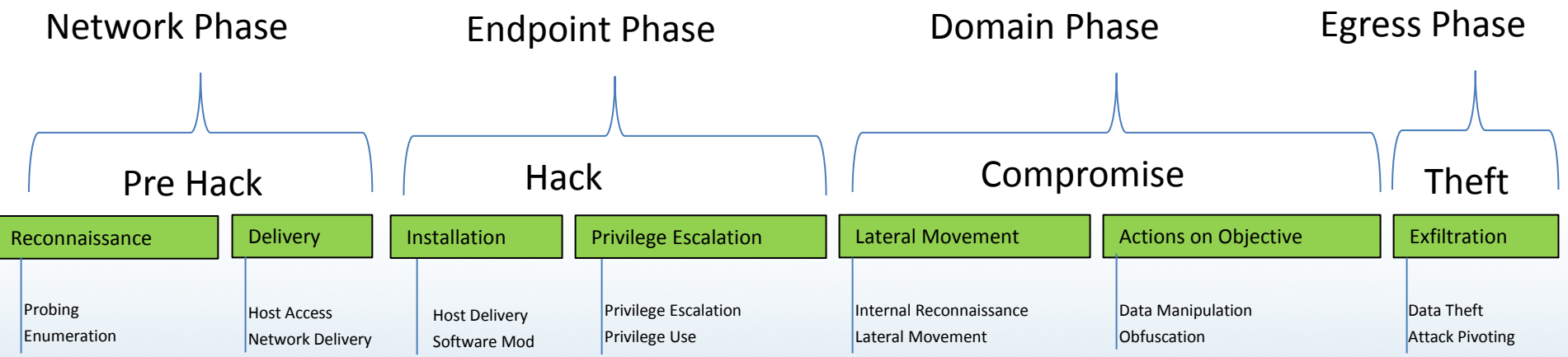
Detect: Example Data Flow (2 of 2)



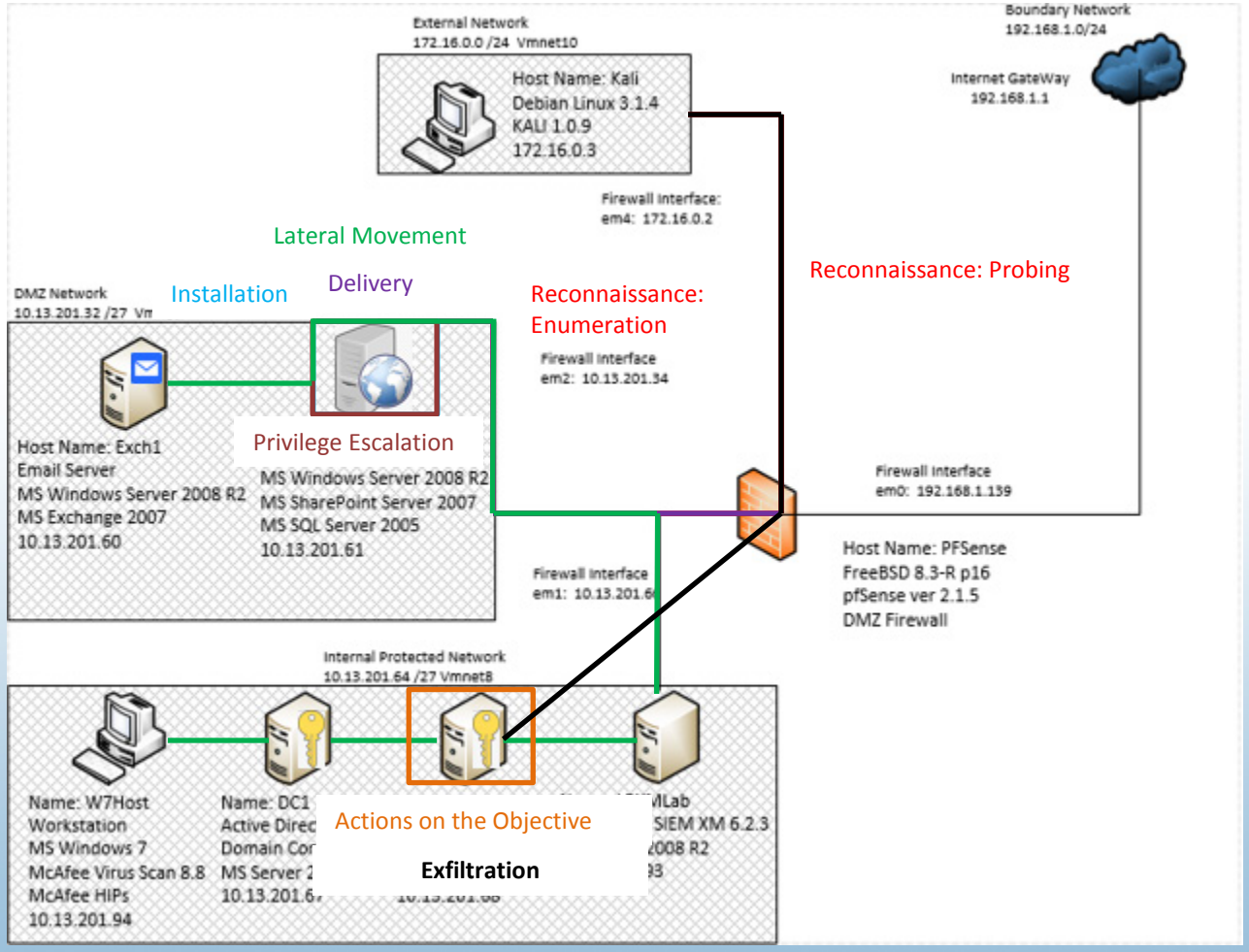
Respond: Definition (1 of 5)

- The response phase consists of actions taken to: interrupt, contain, and eradicate threats.
  - Interrupt: Stop the threat from increasing damage or privilege within a system/network.
  - Contain: Prevent the spread of infection or compromises across the network or system(s).
  - Eradicate: Remove threat presence from the network or system(s).

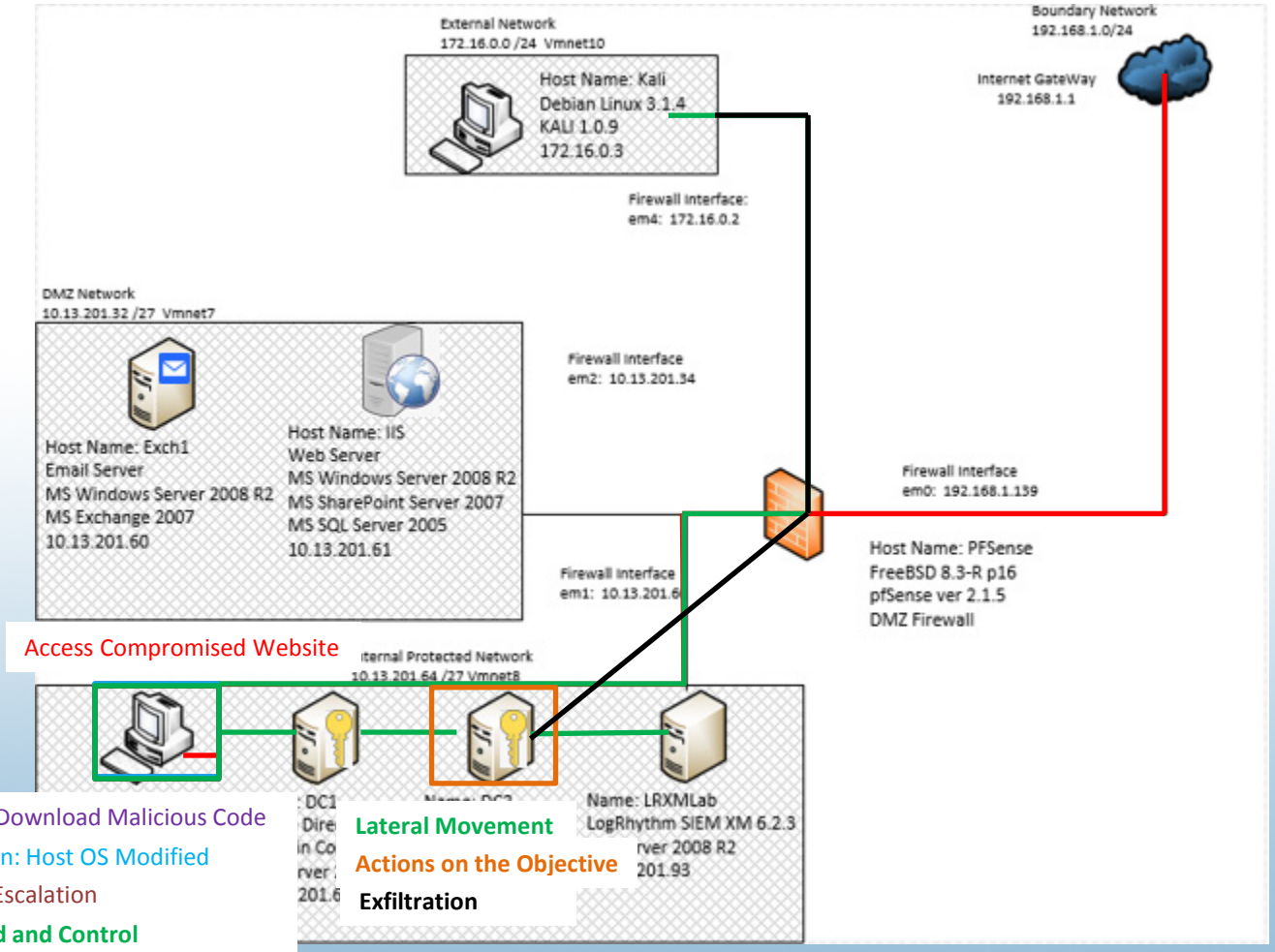
Respond: Interrupt (2 of 5)



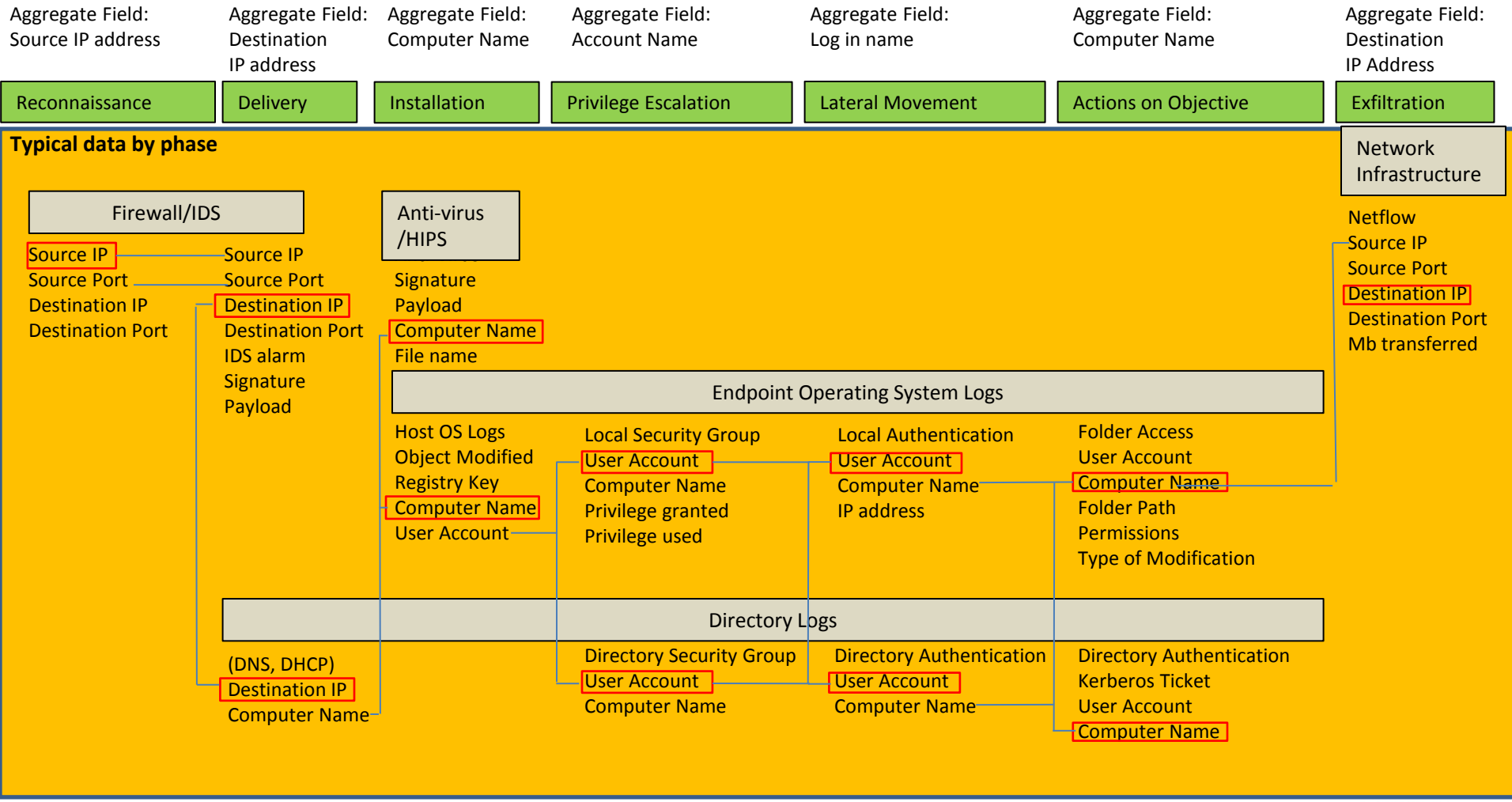
Respond: Contain (3 of 5): Brute Force



Respond: Contain (4 of 5): Victim Operated



Respond: Eradicate (5 of 5)



Recover: Definition (1 of 3)

- The recover phase consists of actions taken to restore systems to pre-incident status and address regulatory requirements. This includes:
  - Implementing the disaster recovery (DR) and/or business continuity plan (BCP) .
  - Contacting external agencies
  - Organizing evidence for regulatory requirements or follow on legal actions

Recover (2 of 3)

Implement Business Continuity / Disaster Recovery Plan

- Restore from backups
- Reset passwords/ revoke account privileges
- Reimage machines

Contact External Entities

- Prepare press release
- Seek legal counsel
- Notify affected parties (clients, employees, business partners etc.)
- Contact External Entities

Retain Evidence

- Chain of custody (sterile collection, data integrity, hashing etc.)

Recover (3 of 3)

Data Retention Policies

- Tied to regulatory compliance
- Not all data is equal (forensic value)
- Storage costs on systems varies
- Query performance heavily dependent on search period

General guidelines (1 of 4)

- Rehearse:
  - Incident response plans are only effective if they are executed in a scalable and repeatable manner.
  - Rehearsals or “table top exercises” help identify potential friction points, additional stake holders, or gaps in processes/systems.
- Encrypt sensitive data
- Hash log data to prove integrity
- Don’t record everything
  - Counter intuitive; however, logging everything often results in delayed search times, increased costs, and useless systems.
  - Regulatory compliance may require additional data, which is not overtly useful to security investigations.

General guidelines (2 of 4)

- Implement Centralized Logging Solution:
  - Aggregate data in centralized location
  - Improves query speed and visibility
  - Decreases license costs (less agents required)
  - Often provides filtering of data
- What is worth logging?:
  - User Authentication events: (Windows logon types: 2, 7, 10, 11)
  - Security group modifications
  - Process execution: (filtered via whitelist)
  - Failed internal network connections
  - Security device alerts (requires significant tuning, especially for perimeter systems)

General guidelines (3 of 4)

- How much space do logs take up?
  - Log storage= events/second X 250 bytes/event X 86,400 seconds/day
  - 100 events/second ~ 2 GB per day
- How many logs do devices generate:
  - Windows workstation: ~0.5 events/sec
  - Web-facing application server: ~20 events/sec
  - Web-facing firewall/IDS/IPS ~75 events/sec
  - Internal application server(low vol) ~5 events/sec
  - Internal AD, IIS, Email (high vol) ~20 events/sec
  - Internal network device ~2 events/sec

* Source: Tenable Security LCEv5.0_Complete_UserGuide.pdf

General guidelines (4 of 4)

- Validate:
  - Third party penetration tests may assist in evaluating security personnel response procedures or security control effectiveness.
- Update:
  - Maintain documentation to reflect improvements or changes to the plan (contact rosters, system changes etc.)
  - Tune detection systems for optimized performance.

Breach Consequences: Regulatory Fines-HIPAA (1 of 6)

Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100-$50,000	$1,500,000
(B) Reasonable Cause	1,000-50,000	1,500,000
(C)(i) Willful Neglect-Corrected	10,000-50,000	1,500,000
(C)(ii) Willful Neglect-Not Corrected	50,000	1,500,000

* source: www.federalregister.gov Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules - 2013

Breach Consequences: High Profile HIPAA Breaches (2 of 6)

Entity Fined	Fine	Violation
CIGNET	$4,300,000	Online database application error.
Alaska Department of Health and Human Services	$1,700,000	Unencrypted USB hard drive stolen, poor policies and risk analysis.
WellPoint	$1,700,000	Did not have technical safeguards in place to verify the person/entity seeking access to PHI in the database. Failed to conduct a tech eval in response to software upgrade.
Blue Cross Blue Shield of Tennessee	$1,500,000	57 unencrypted hard drives stolen.
Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates	$1,500,000	Unencrypted laptop stolen, poor risk analysis, policies.
Affinity Health Plan	$1,215,780	Returned photocopiers without erasing the hard drives.
South Shore Hospital	$750,000	Backup tapes went missing on the way to contractor.
Idaho State University	$400,000	Breach of unsecured ePHI.

* source: www.truevault.com

Breach Consequences: Regulatory Fines- PCI-DSS (3 of 6)

- Noncompliance Fines- The consequences of not being PCI compliant range from $5,000 to $500,000, which is levied by banks and credit card institutions.

- Breach Consequences- Even if a company is 100% PCI compliant and validated, a breach in cardholder data may still occur. Cardholder Breaches can result in the following losses for a merchant.
  - $50-$90 fine per cardholder data compromised
  - Suspension of credit card acceptance by a merchant's credit card account provider
  - Loss of reputation with customers, suppliers, and partners
  - Possible civil litigation from breached customers
  - Loss of customer trust which effects future sales

Breach Consequences: Regulatory Fines- PCI-DSS (4 of 6)

- Example PCI-DSS fees from Visa

Month	Level 1 (6 mil + transactions)	Level 2 (1-6 mil transactions)
1 to 3	$10,000 monthly	$5,000 monthly
4 to 6	$50,000 monthly	$25,000 monthly
7 and on	$100,000 monthly	$50,000 monthly

* source: www.focusonpci.com

Breach Consequences: High Profile Breaches (5 of 6)

Year	Company	Breach	Estimated Cost
2015	Anthem	80 million patient records stolen	$100 million
2015	Ashley Madison	33 million users account information stolen (email, First/Last name, phone #)	$850 million
2014	Ebay	145 users account information stolen	$200 million
2014	JP Morgan Chase	Financial data for 76 million families and 7 million small business stolen	$1 billion
2014	Home Depot	56 million credit cards stolen	$80 million
2014	Sony	3,000 employees PII stolen	$35 million
2013	Target	40 million credit cards stolen	$252 million

* source: www.bankrate.com/

Breach Consequences: High Profile Breach Common Issues (6 of 6)

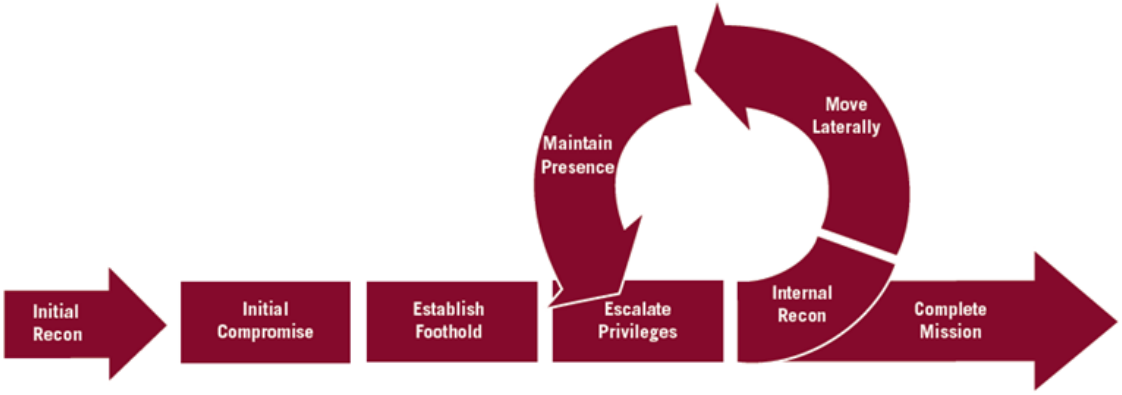
- Breach was discovered by external entity
  - Security researcher
  - Business partner
  - Media
- Poor communication plans
  - Damage to reputation
  - Decline in sales
- Little emphasis on security prior to breach
  - Poor security governance
  - Focused on regulatory compliance rather than security (PCI, HIPAA, SOX etc.)

Questions/Comments

Backup Slides

Anatomy of An Attack

The Lockheed Martin Intrusion Kill Chain Model (Hutchins, et al., 2013)

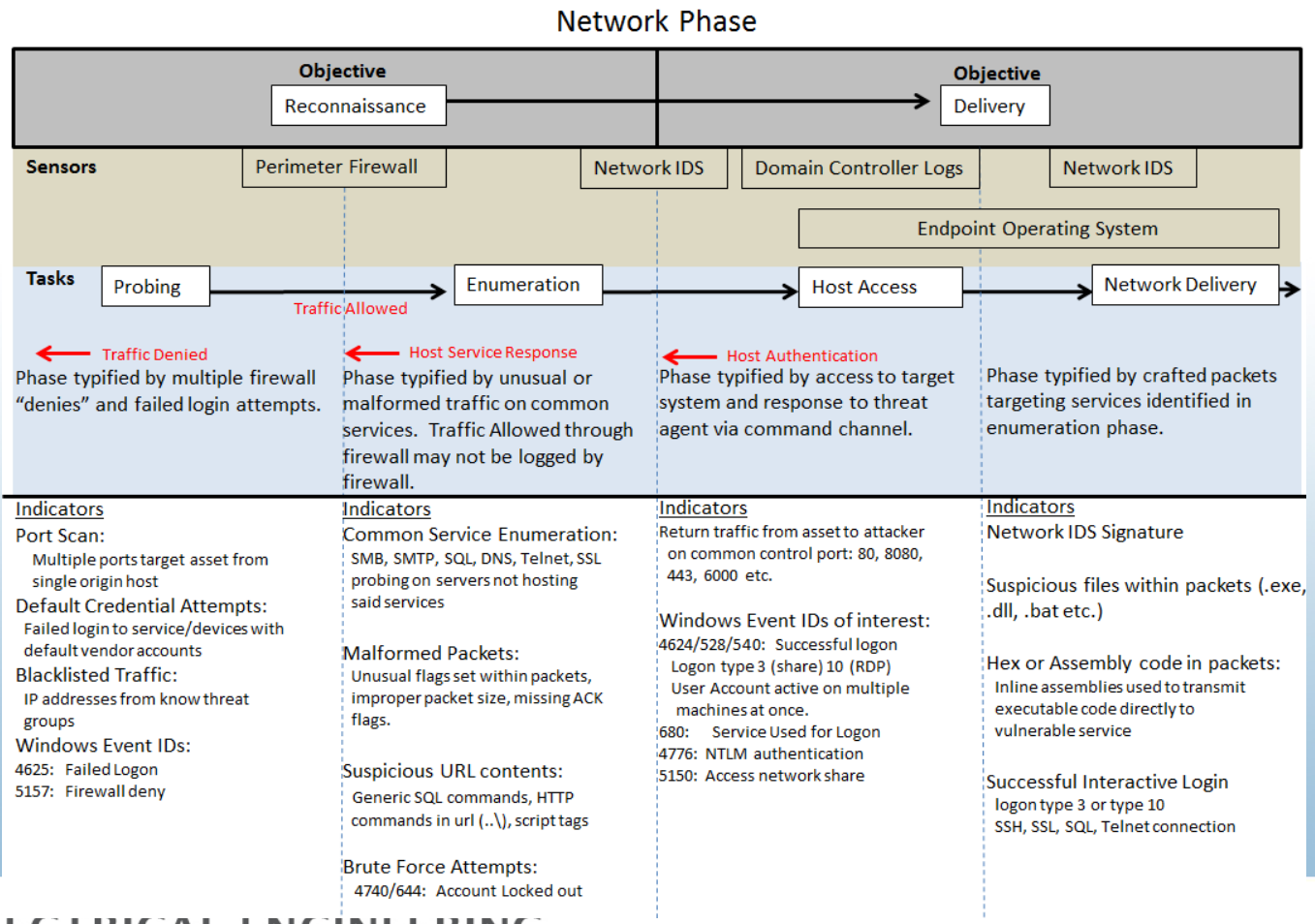


Mandiant's Attack Lifecycle Model (Mandiant, 2013)

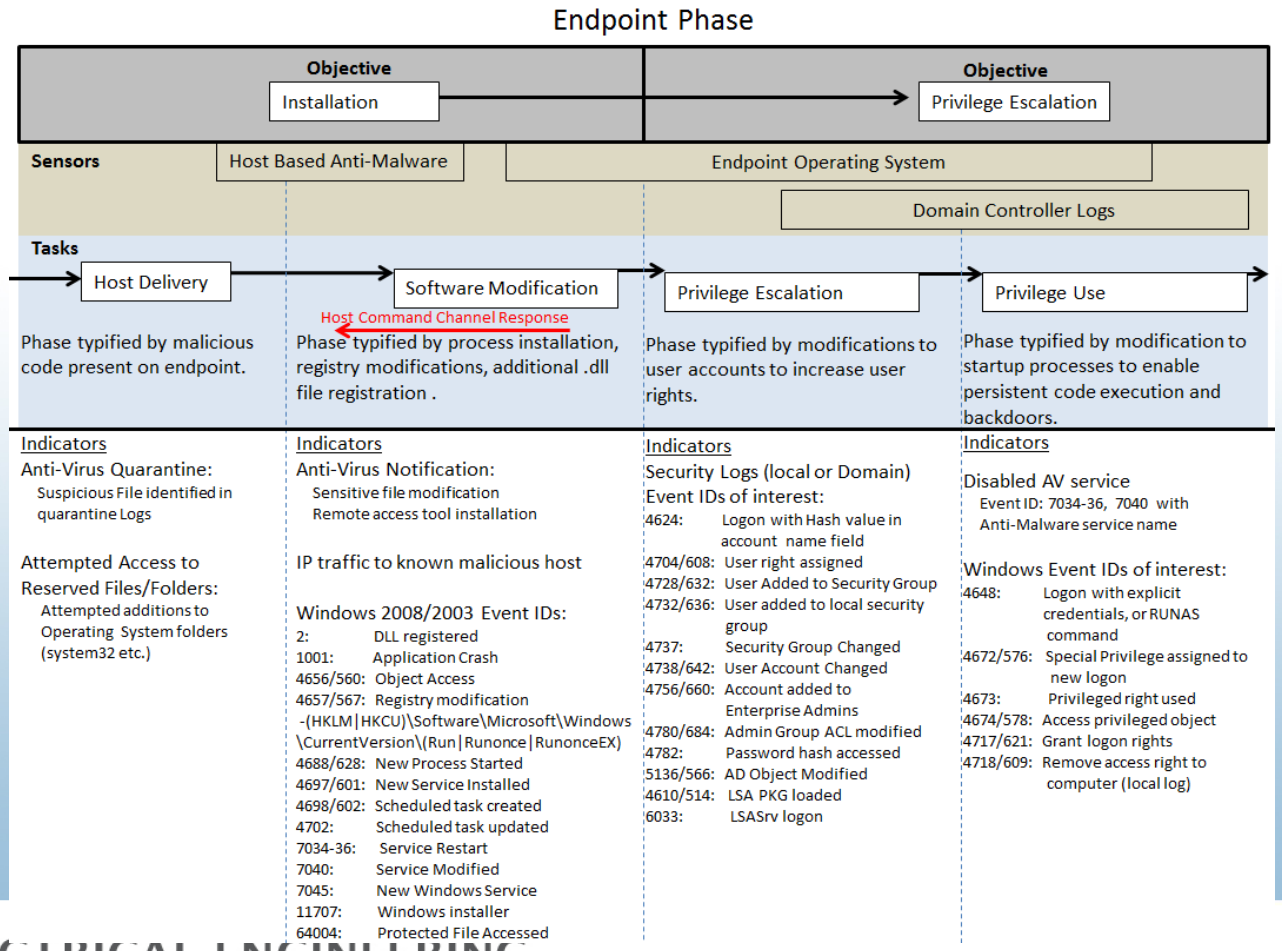
Reconnaissance	Delivery	Installation	Privilege Escalation	Lateral Movement	Actions on Objective	Exfiltration

Bryant Kill Chain (Bryant, 2016)

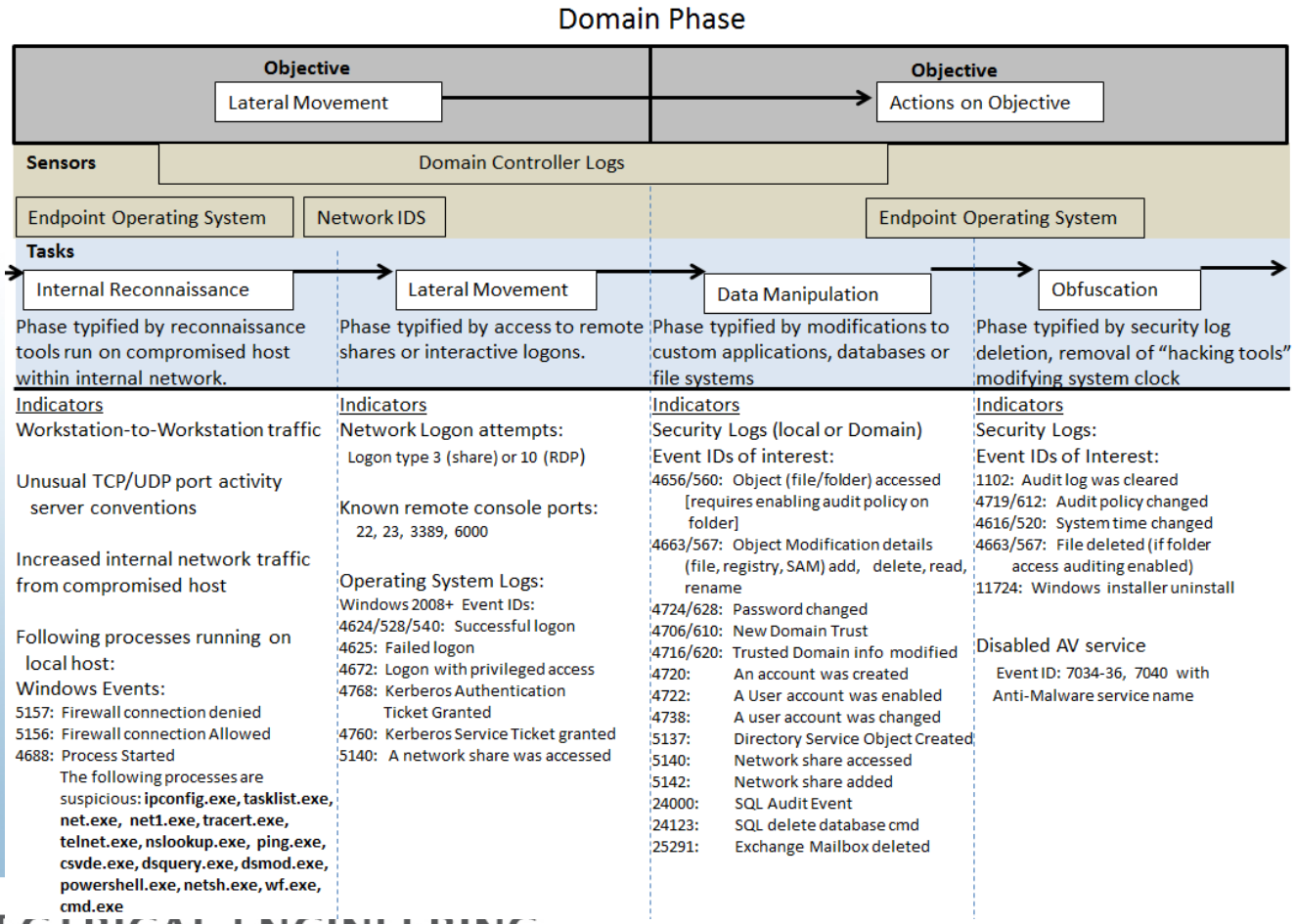
Advanced Network Forensics



Advanced Network Forensics



Advanced Network Forensics



Advanced Network Forensics