Lesson 17

Performing Incident Response

CompTIA

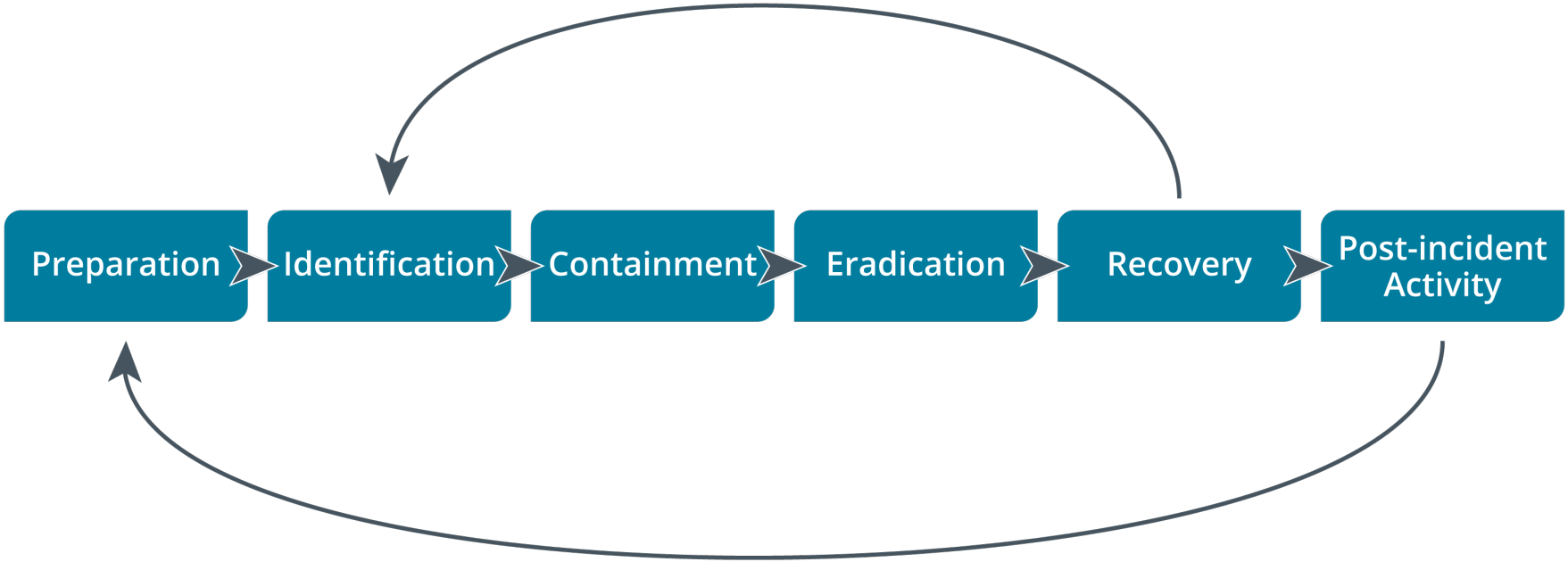
Topic 17A

Summarize Incident Response Procedures

Syllabus Objectives Covered

- 4.2 Summarize the importance of policies, processes, and procedures for incident response

Incident Response Process



Cyber Incident Response Team

- Reporting, categorizing, and prioritizing (triage)
- CIRT/CERT/CSIRT/SOC
- Management/decision-making authority
- Incident analysts
- 24/7 availability
- Roles beyond technical response
  - Legal
  - Human Resources (HR)
  - Marketing

Image credit: John Mattern/Feature Photo Service for IBM.

Communication Plan and Stakeholder Management

- Prevent inadvertent disclosure
- Call list identifying trusted parties
- Communication plan
  - Share data on a need to know basis
  - Out-of-band communications—avoid alerting intruder
- Stakeholder management
  - Communication with internal and external stakeholders
  - Notification and reporting

Incident Response Plan

- Lists the procedures, contacts, and resources available to responders for various incident categories
- Playbooks and runbooks
- Incident categorization
- Prioritization factors
  - Data integrity
  - Downtime
  - Economic/publicity
  - Scope
  - Detection time
  - Recovery time

Cyber Kill Chain Attack Framework

Other Attack Frameworks

- MITRE ATT&CK
  - Database of TTPs
  - Tactic categories
  - No explicit sequencing
- The Diamond Model of Intrusion Analysis
  - Framework for describing adversary capability and infrastructure plus effect on victim

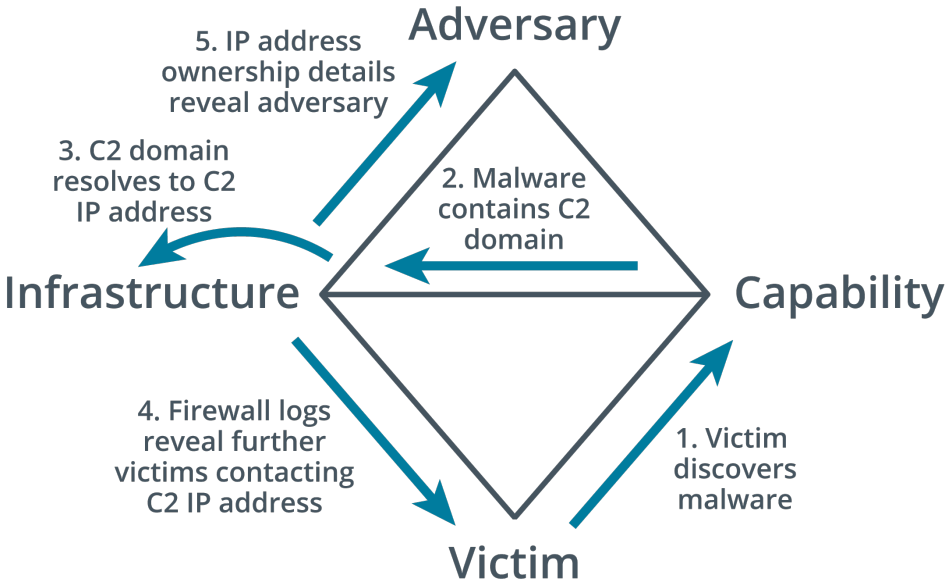


Image: Released to public domain by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz (activeresponse.org/wp-content/uploads/2013/07/diamond.pdf.)

Incident Response Exercises

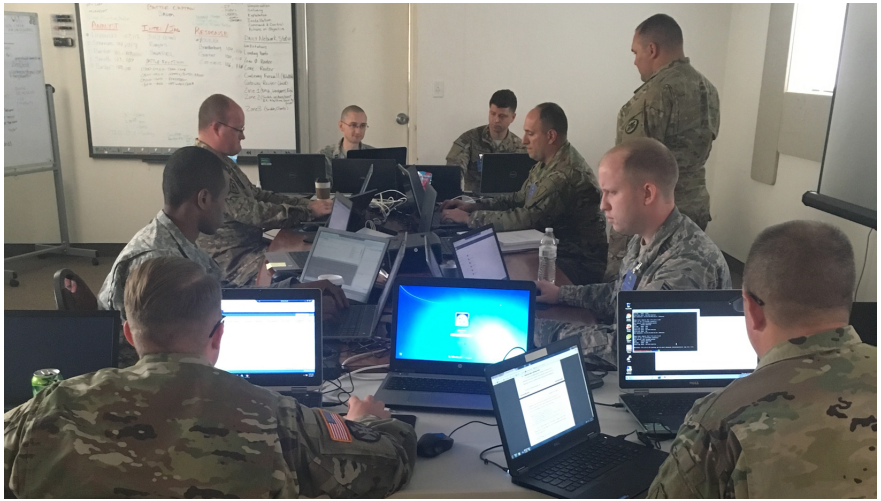


Image © 2017 Kentucky National Guard.

- Tabletop
  - Facilitator presents a scenario
  - Does not involve live systems
- Walkthroughs
  - Responders demonstrate response actions
- Simulations
  - Red team performs a simulated intrusion

Incident Response, Disaster Recovery, and Retention Policy

- Incident response versus disaster recovery and business continuity
  - Disaster recovery plan
    - Response and recovery planning for major incidents
  - Business continuity plan
    - Making business procedures resilient
  - Continuity of operation planning (COOP)
- Incident response, forensics, and retention policy
  - Digital forensics requirements
  - Retention policies for evidence preservation

Topic 17B

Utilize Appropriate Data Sources for Incident Response

Syllabus Objectives Covered

- 4.3 Given an incident, utilize appropriate data sources to support an investigation

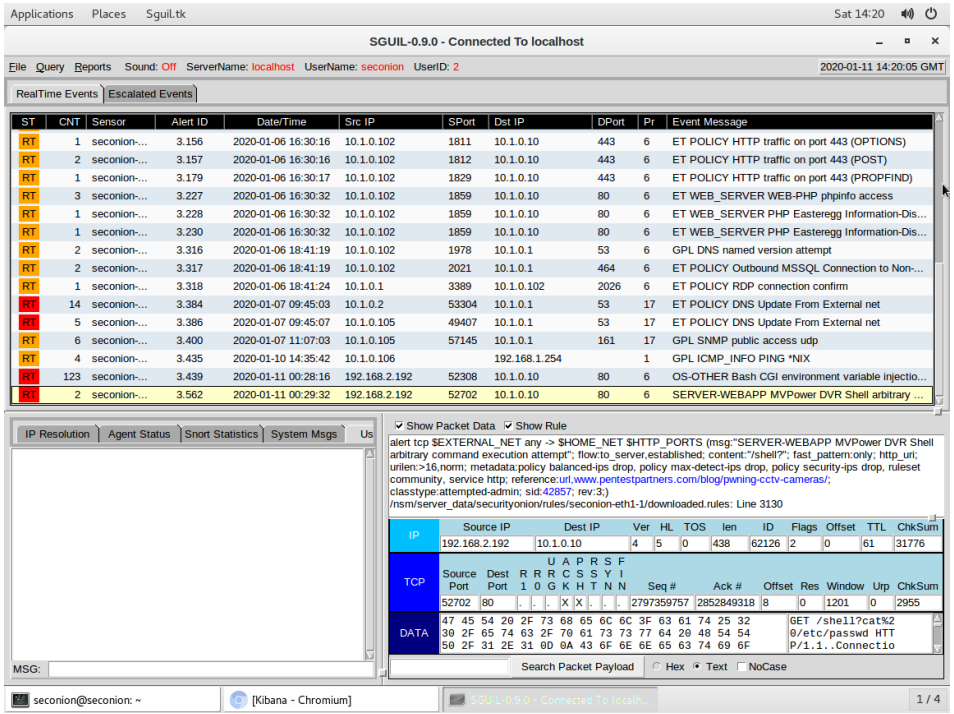
Incident Identification

- Precursors and detection channels
  - Security mechanisms (IDS, log analysis, alerts)
  - Manual inspections
  - Notification procedures
  - Public reporting
  - Confidential reporting/whistleblowing
- First responder
  - Member of CIRT taking charge of a reported incident
- Analysis and incident identification
  - Classify and prioritize
  - Downgrade low priority alerts to log-only

Security and Information Event Management

- Correlation
  - Static rules and logical expressions
  - Threat intelligence feeds
  - AI-assisted analysis
- Retention
  - Preserve evidence of attack
  - Facilitate threat hunting and retrospective incident identification

SIEM Dashboards



Screenshot courtesy of Security Onion (securityonion.net.)

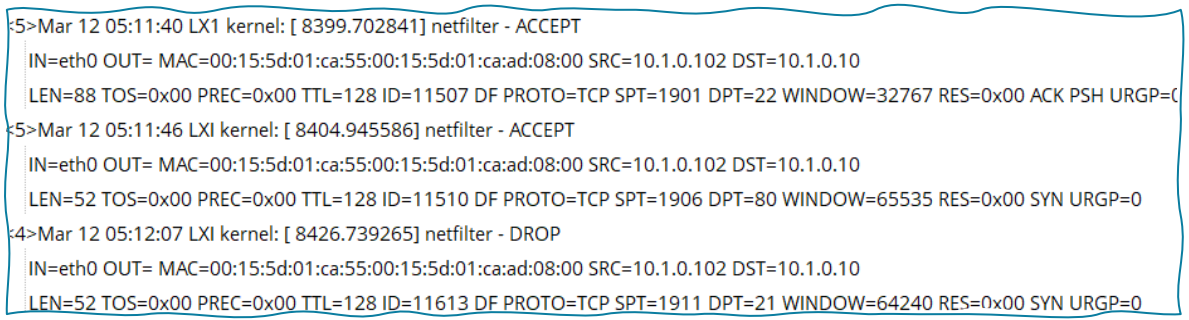
- Analyst dashboard
  - Console of alerts that require prioritization and investigation
- Manager dashboard
  - Overall status indicators
- Sensitivity and alerts
  - Log only/alert/alarm
- Sensors
  - Source for network traffic data
  - Aggregate data under one dashboard
  - Per-sensor dashboards

Trend Analysis

- Detecting indicators over a time series
- Prediction of future events
- Visualization
- Frequency-based
  - Number of events per period
- Volume-based
  - Increasing or decreasing size
- Statistical deviation
  - Identify anomalous data points

Logging Platforms

- Syslog
  - Logging format, protocol, and server (daemon) software
  - PRI – facility and severity
  - Timestamp
  - Host
  - Message part
- Rsyslog and syslog-ng
- journalctl
  - Binary logging
- Nxlog
  - Log normalization tool



Network, OS, and Security Log Files

- System and security logs
  - Application
  - Security/audit
  - System
  - Setup
  - Forwarded events
- Network logs
  - Traffic and access data from network appliances
- Authentication logs
  - Security log or RADIUS/TACACS+ application logs
- Vulnerability scan output

Application Log Files

- DNS event logs
  - Types of queries made by clients
  - Hosts using suspicious IP address ranges or domains
  - Statistical anomalies
- Web/HTTP access logs
  - HTTP status codes
  - HTTP headers
- VoIP and call managers and Session Initiation Protocol (SIP) traffic
  - Log endpoint connections
  - Type of connection
  - Via headers
- Dump files
  - Data from system memory

Metadata

- File
  - Date/time and security attributes
  - Extended attributes and properties
- Web
  - Request and response headers
- Email
  - Internet header listing message transfer agents
  - Spam/security analysis
- Mobile
  - Call detail records (CDRs)

```
Return-Path: hostmaster@515web.net
Received: from smtp.openmail.foo (Unknown [192.168.2.192])
    by mail.515support.com with ESMTP
    ; Wed, 26 Feb 2020 13:16:13 -0800
Received: from [IPv6:::1] (localhost [IPv6:::1])
    by smtp.openmail.foo (Postfix) with ESMTP id 9182A1A027D
    for <sam@515support.com>; Wed, 26 Feb 2020 13:16:02 -0800 (PST)
To: sam@515support.com
From: hostmaster <hostmaster@515web.net>
Subject: Web configuration tool
Message-ID: <9320fb62-9092-4ac4-3c06-f3af4644181f@515web.net>
Date: Wed, 26 Feb 2020 13:16:02 -0800
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
 Thunderbird/60.9.0
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="------------51B63E3EB325EF18E1F0170F"
Content-Language: en-US

This is a multi-part message in MIME format.
--------------51B63E3EB325EF18E1F0170F
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 7bit

--------------51B63E3EB325EF18E1F0170F
Content-Type: application/x-msdos-program;
 name="evilputty.exe"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="evilputty.exe"

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Network Data Sources

- Protocol analyzer output
  - Pivot from alert event to per-packet or frame analysis
  - Extract binary data
- Netflow/IPFIX
  - Records traffic statistics
  - Flows defined by endpoints and ports (keys)
  - Netflow exporters and collectors
- sFlow
  - Uses sampling to estimate statistics
- Bandwidth monitor



Topic 17C

Apply Mitigation Controls

Syllabus Objectives Covered

- 1.2 Given a scenario, analyze potential indicators to determine the type of attack
- 4.4 Given an incident, apply mitigation techniques or controls to secure an environment

Containment Phase

- Response must satisfy different or competing objectives
  - What is the loss or potential for loss?
  - What countermeasures are available?
  - What evidence can be collected?
- Isolation-based containment
  - Remove the affected system
  - Disconnect hosts from power
  - Prevent hosts communicating on network
  - Disable user accounts or applications
- Segmentation-based containment
  - Use sinkhole or sandbox to analyze attack



Incident Eradication and Recovery

- Eradication of attack tools and access methods
- Recovery of systems to restore the operation of business workflows
- Reconstitution of affected systems
- Re-audit security controls – what could have prevented the intrusion?
- Notification and third-party impacts

Firewall Configuration Changes

- Analyze attack to determine vector
- Reduce attack surface through configuration changes
  - New security control
  - Update existing control configuration
- Egress filtering for firewall rules
- Detection of other covert channels

Content Filter Configuration Changes

- Secure web gateway for egress filtering
  - Update URL/content filtering using threat data
- Data loss prevention (DLP)
  - Identify whether DLP mechanisms were circumvented
- Mobile device management (MDM)
  - Identify whether MDM mechanisms were circumvented
- Update or revoke certificates
  - Remove compromised root certificates from trust stores
  - Revoke certificates on compromised hosts
    - Re-key certificate



Endpoint Configuration Changes

- Re-assess attack surface and attack vectors
  - Social engineering
  - Vulnerabilities
  - Lack of security controls
  - Configuration drift
  - Weak configuration
- Application allow lists/block lists
  - Change to least privilege
  - Identify failure of controls to prevent execution
- Quarantine
  - Isolate suspect systems for analysis in sandbox

Security Orchestration, Automation, and Response

- Automation versus orchestration
- Security orchestration, automation, and response (SOAR)
  - Incident response
  - Threat hunting
- Integrates SDN/SDV APIs, orchestration tools, and cyber-threat intelligence (CTI) feeds
- AI-assisted user and entity behavior analytics (UEBA)
- Runbooks versus playbooks

Adversarial Artificial Intelligence

- Machine learning relies on training data to develop analysis capability
- Threat actor may be able to submit tainted samples
- Adversarial AI
- Security of machine learning algorithms

Lesson 17

Summary