

# Lesson 17

## Performing Incident Response

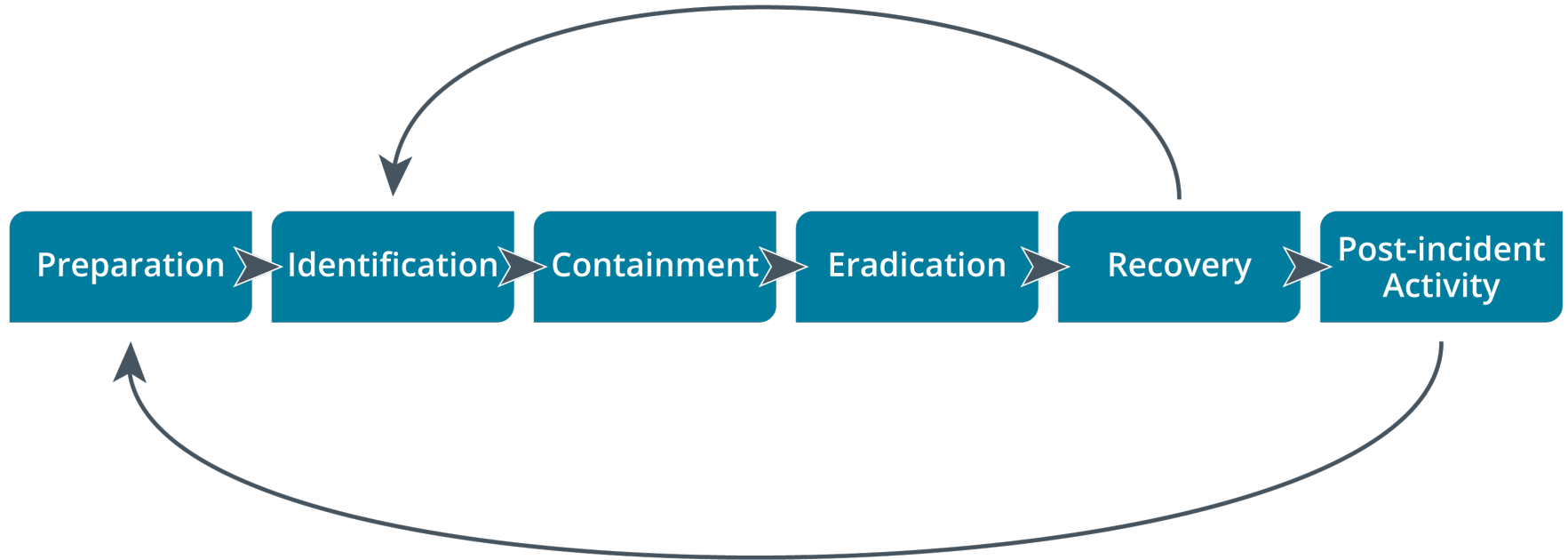
# Topic 17A

## 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

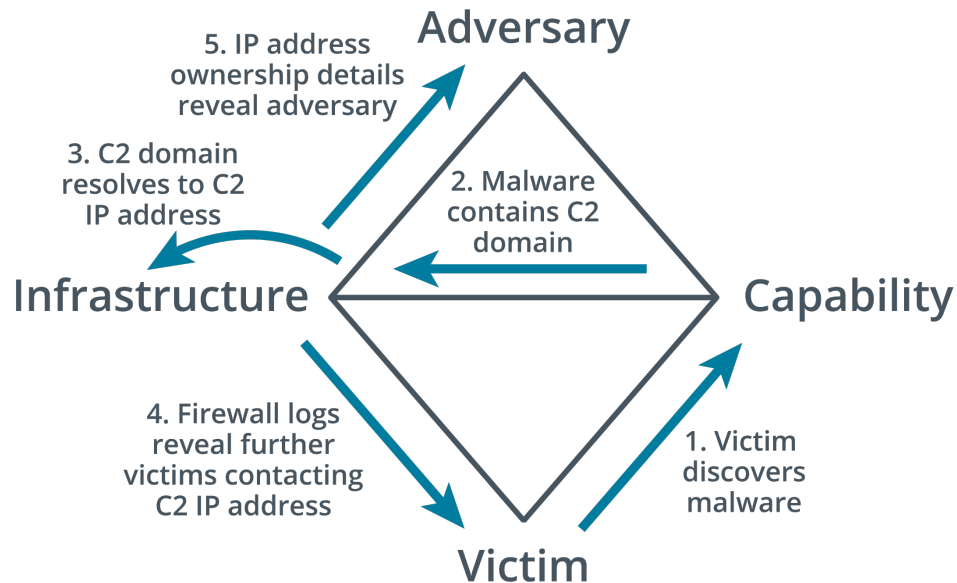
# Cyber Kill Chain Attack Framework





# 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](https://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

The screenshot displays the SGUIL-0.9.0 interface, connected to a local host. The top navigation bar includes 'Applications', 'Places', and 'Sguil.tk'. The main window is titled 'RealTime Events' and shows a table of events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The events list shows various alerts related to HTTP traffic, PHP access, and DNS updates.

Below the events list, the 'Show Packet Data' and 'Show Rule' tabs are active. The 'Show Rule' tab displays a rule definition for 'alert top \$EXTERNAL\_NET any -> \$HOME\_NET \$HTTP\_PORTS'. The 'Show Packet Data' tab shows a detailed packet capture for the selected event, including IP, TCP, and DATA sections.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion...	3.156	2020-01-06 16:30:16	10.1.0.102	1811	10.1.0.10	443	6	ET POLICY HTTP traffic on port 443 (OPTIONS)
RT	2	seconion...	3.157	2020-01-06 16:30:16	10.1.0.102	1812	10.1.0.10	443	6	ET POLICY HTTP traffic on port 443 (POST)
RT	1	seconion...	3.179	2020-01-06 16:30:17	10.1.0.102	1829	10.1.0.10	443	6	ET POLICY HTTP traffic on port 443 (PROPFIND)
RT	3	seconion...	3.227	2020-01-06 16:30:32	10.1.0.102	1859	10.1.0.10	80	6	ET WEB_SERVER WEB-PHP phpinfo access
RT	1	seconion...	3.228	2020-01-06 16:30:32	10.1.0.102	1859	10.1.0.10	80	6	ET WEB_SERVER PHP Easteregg Information-Di...
RT	1	seconion...	3.230	2020-01-06 16:30:32	10.1.0.102	1859	10.1.0.10	80	6	ET WEB_SERVER PHP Easteregg Information-Di...
RT	2	seconion...	3.316	2020-01-06 18:41:19	10.1.0.102	1978	10.1.0.1	53	6	GPL DNS named version attempt
RT	2	seconion...	3.317	2020-01-06 18:41:19	10.1.0.102	2021	10.1.0.1	464	6	ET POLICY Outbound MSSQL Connection to Non...
RT	1	seconion...	3.318	2020-01-06 18:41:24	10.1.0.1	3389	10.1.0.102	2026	6	ET POLICY RDP connection confirm
RT	14	seconion...	3.384	2020-01-07 09:45:03	10.1.0.2	53304	10.1.0.1	53	17	ET POLICY DNS Update From External net
RT	5	seconion...	3.386	2020-01-07 09:45:07	10.1.0.105	49407	10.1.0.1	53	17	ET POLICY DNS Update From External net
RT	6	seconion...	3.400	2020-01-07 11:07:03	10.1.0.105	57145	10.1.0.1	161	17	GPL SNMP public access udp
RT	4	seconion...	3.435	2020-01-10 14:35:42	10.1.0.106		192.168.1.254		1	GPL ICMP_INFO PING 'NIX
RT	123	seconion...	3.439	2020-01-11 00:28:16	192.168.2.192	52308	10.1.0.10	80	6	OS-OTHER Bash CGI environment variable injectio...
RT	2	seconion...	3.562	2020-01-11 00:29:32	192.168.2.192	52702	10.1.0.10	80	6	SERVER-WEBAPP MvPower DVR Shell arbitrary ...

- 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

Screenshot courtesy of Security Onion ([securityonion.net](http://securityonion.net).)



# 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

```
<5>Mar 12 05:11:40 LX1 kernel: [ 8399.702841] netfilter - ACCEPT
IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=10.1.0.102 DST=10.1.0.10
LEN=88 TOS=0x00 PREC=0x00 TTL=128 ID=11507 DF PROTO=TCP SPT=1901 DPT=22 WINDOW=32767 RES=0x00 ACK PSH URGP=0
<5>Mar 12 05:11:46 LX1 kernel: [ 8404.945586] netfilter - ACCEPT
IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=10.1.0.102 DST=10.1.0.10
LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=11510 DF PROTO=TCP SPT=1906 DPT=80 WINDOW=65535 RES=0x00 SYN URGP=0
<4>Mar 12 05:12:07 LX1 kernel: [ 8426.739265] netfilter - DROP
IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=10.1.0.102 DST=10.1.0.10
LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=11613 DF PROTO=TCP SPT=1911 DPT=21 WINDOW=64240 RES=0x00 SYN URGP=0
```

# 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//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

# 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

