10. Incident Response

Simona Buchovecká, Tomáš Čejka

Faculty of Information Technology, CTU in Prague

simona.buchovecka@fit.cvut.cz, tomas.cejka@fit.cvut.cz

December 2, 2019

Event & Incident (NIST framework)

- **Event** is any observable occurrence in a system or network
- **Adverse events** are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data
- **A computer security incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- Security Incident != Operations (ITIL) incident (different objectives — security: stop the data exfiltration, minimize damage; operations: get it back to operation)

Security incident . . . in other words. . .

- Intent to cause harm
- Performed by a person
- Involves computing resource

- Examples
  - Data theft
  - Theft of funds - bank access, credit card and wire fraud
  - Extortion
  - Unauthorized access to computing resources
  - Presence of malware
  - Possession of illegal or unauthorized materials

What exactly is an incident response?

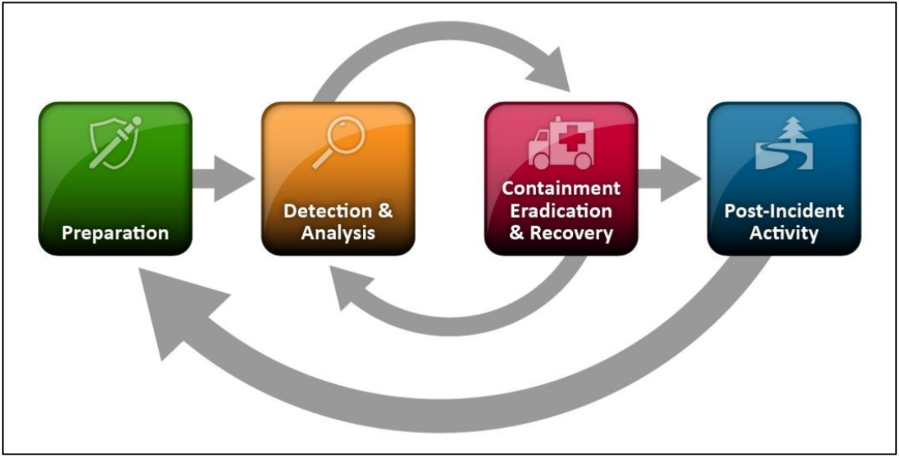
- Confirm whether or not an incident occurred
  - False positives x True positives
  - False negatives x True negatives
- Provide rapid detection & containment (isolation of the threat/infection)
- Determine and document the scope of the incident
- Minimize the disruption to the business
- Minimize the damage
- Restore normal operations
- Allow for criminal or civil actions against attackers
- Educate senior management
- Enhance security posture. . .

Need for Incident Response

- Incidents happen (no matter how secure environment is)
- Criminals work with little risks
- Efficient and timely response to the incident can minimize the financial or reputation damage
- If there is data leak, we need to know what was leaked
- Ensure that incident is remediated properly (and attackers are out of your network)

Handling an Incident

It's critical to follow the process and not skip the phases!



Preparation

- Prepare to handle incidents
  - Incident Response Policy, Plan, and Procedure Creation
    - Sharing information/reporting to 3rd parties (e.g., Incident involving personal data)
    - Management buy-in, set-up expectations, communication matrix, escalation paths, . . .
    - Setting up dependencies: Management, Information Assurance, IT Support, Legal Department, Public Affairs and Media Relations, Human Resources, Business Continuity Planning
  - Communications and Facilities: Contact information, incident reporting mechanism, issue tracking system, war room, . . .
  - Hardware and Software: digital forensic workstations and/or backup devices, laptops, blank removable media, . . .
  - Resources: Documentation, network diagrams, list of critical assets, baselines, . . .
- Preventing incidents - any activity that helps you prevent incidents (network security, endpoint security, user awareness)

Incident Response vs. Business Continuity

Ongoing incident may have serious impacts on business operations, e.g., DoS

Incident Response Planning

- Security-related threats to systems, networks & data
- Data confidentiality
- Non-repudiable transactions

Business Continuity Planning

- Disaster Recovery Plan
- Continuity of Business Operations
- IRP is part of BCP and can be the first step

Preparation, Preparing the Incident Response Team (IRT)

- Central IRT: one team in organisation having the authority
- Distributed Incident Response Team — useful for large organisation, e.g., one IRT per division; one IRT per geographic location to enable follow-the-sun model
- Coordinating team — team providing the advice to other teams without having authority
- Staffing models
  - Internal Employees
  - Partially Outsourced
  - Fully Outsourced

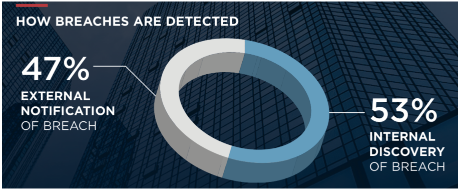
Detection and Analysis

Detection &
Analysis

- Attack Vectors
  - External/removable media
  - Social Engineering: email/phishing, web, ...
  - Brute force attacks
  - Impersonation
  - Improper usage
  - Loss/theft of equipment, ...
- Signs of an incident — precursor, indicator
- Detection?
- Real-time alerts — monitoring
- Users (phishing),
  IT admins (know their systems; observes a suspicious behavior)
- 3rd parties — government CERTs; partner organisations observing suspicious traffic outgoing from your network

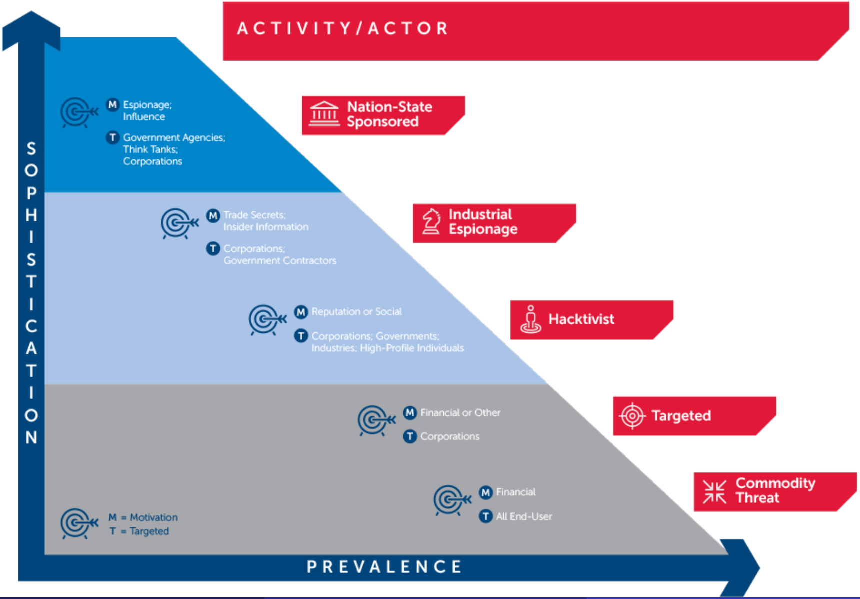
How we learn about the incident?

source: FireEye/Mandiant M-trends



- Dwell time: time from first evidence of compromise that an attacker is present on a victim network before detection
- The global median dwell time is significant: 146 days in 2015, 99 days in 2016, 101 days in 2017
- Actual global dwell times vary significantly, ranging from less than one week to over 2,000 days — depends on complexity of attack/threat actor & maturity of the IR processes and team

Threat Actors



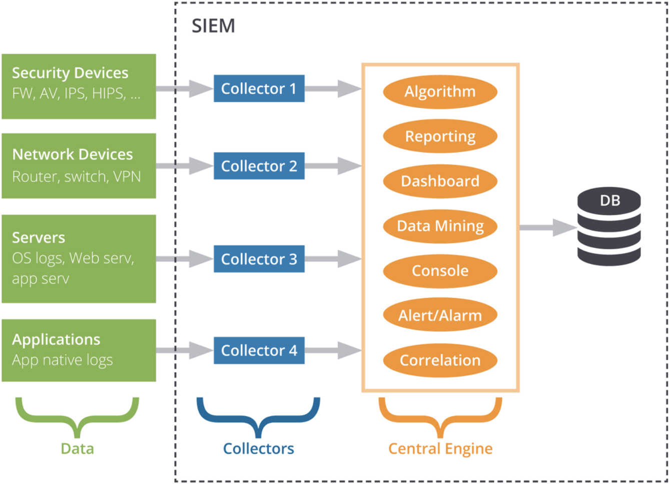
SIEM - Security Information and Event Management

Detection & Analysis

- SIEM solutions ingest log data from HW and SW systems, and analyze that data to correlate events and find anomalies or patterns of behavior that may indicate a security breach
- Event and log collection, log management
- Parsing
- Normalisation: reducing the records to just common event attributes (e.g., using data models); known data attributes are fed into a generic template
- Enrichment: adding supplemental information (like geo-location, transaction numbers, mapping known hostnames to IPs, etc.)
- Correlation: looking for patterns of suspicious activities
- *Logging* (continuous activity, no output) vs. *Reporting* (regular automated logs processing with output according to predefined template) vs. *Alerting* (real-time processing of logs)

Sources of Precursors and Indicators

Detection & Analysis



Examples of correlations rules

Detection & Analysis

- Detection of specific events, e.g., malware detected event from IDS; suspicious Powershell command observed on the machine; Mimikatz tool detected etc.
- Detection of specific characteristics in network traffic, e.g., large ICMP traffic observed, communication to known malicious domain
- Detection of set of events — multiple failed logons originating from single IP
- Statistical correlations — look for outliers, detect anomalies
- MITRE ATT&CK framework can be used as guidance for creating detections: `https://attack.mitre.org`

Incident Analysis

Detection & Analysis

- Determining if the event is an incident can be difficult
  - What can help?
    - Profile networks and systems
    - Understand normal Behavior
    - Log retention policy
    - Perform event correlation
    - Keep all host clock synchronized
    - Maintain and use knowledge base, documentation
    - Filter the data
    - Cooperate
- Documentation — once there is suspicion that incident occurred, all the facts regarding the incident should immediately be recorded
- Do not proceed with further steps, until the Analysis is completely finished and the incident properly scoped — missing just one infected machine will allow the re-compromise of the environment again

Containment, Eradication and Recovery

- *Containment* — actions necessary to prevent further damage (disconnecting system, revoking user access, changing passwords. . .)
    - First aid: stop the bleeding
    - Even if incident is contained, Eradication & Recovery still needed
- *Eradication*: identify, remove and repair the vulnerability, implement additional security controls . . .
- *Recovery*: resuming operations to fully operation status

Technical vs. Managerial vs. Legal

Evidence Gathering and Handling

Containment
Eradication
& Recovery

- Primary reason — resolve the incident
- Sometimes it may be needed for legal proceedings
  - In such case it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court.
- Forensic techniques may be used

Incident Response vs. Computer Forensics

Incident Response

- Management and quick containment of the security incident
- Integration into the business processes
- Return back to operations

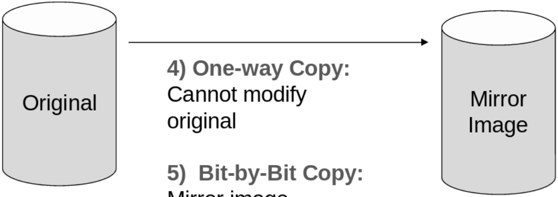
Computer Forensics

- Identifying preserving, analyzing and presenting digital evidence for a legal proceeding
- Detailed and careful handling of digital evidence and analysis

Creating a Forensic Copy

Susan J. Lincke: Incident Response

2) Accuracy Feature:
Tool is accepted as accurate by the scientific community:



Original

4) One-way Copy:
Cannot modify original

5) Bit-by-Bit Copy:
Mirror image

Mirror Image

1) & 6) Calculate Message Digest:
Before and after copy

3) Forensically Sterile:
Wipes existing data;
Records sterility

7) Calculate Message Digest
Validate correctness of copy

Chain of Custody

Containment
Eradication
& Recovery

- Chain of evidence:
  - whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence, including the following:
    - Identifying information: location, serial number, model number, hostname, . . .
    - Name, title, phone, . . . of each individual who collected or handled the evidence
    - Time and date of each occurrence of evidence handling
    - Locations where the evidence was stored

Data Collection

Containment
Eradication
& Recovery

- Offline data collection — machine disconnected, creating exact (bit) copy of hard drive (using write blockers)
- Live data collection — preserves volatile evidence
  - Risks: changes on the system due to collection process (destroying evidence)
- Best practice:
  - Document
  - Use tools with minimum impact on running system
  - Use cryptographic checksums for collected evidence
  - Prefer automation, instead of human interaction with machine
  - Treat all collected data as evidence
  - Consider any data on media connected to the suspect machine as lost, any used credentials as compromised
  - Do not use suspect machine to perform analysis

Malware Handling

Containment
Eradication
& Recovery

- Safety:
  - Use a virtual environment for triage with isolated network connection
  - Update!
  - Disable convenient features such as drag&drop, clipboard, preview, autoruns
  - Label media containing malware
  - .exe_, disable execution on the folder
  - Password protected archives (password:infected)
  - Once analysis ready, revert
- *Static analysis* (without execution, disassembling) vs. *Dynamic analysis* (run in sandbox & observe the executable's behavior)

Live Response Collection

Containment
Eradication
& Recovery

- OS and general info (memory, HDD, mounted file systems)
- Running processes
- List of services and programs — autoruns, scheduled tasks
- Local user accounts and group membership; user login history
- Network interface details, routing table, ARP table, DNS cache
- Network connections, including associated processes
- Loaded drivers and modules
- Installed software
- Standard system logs — eventlog; application logs
- MFT (NTFS), inode table, etc.
- Files and other open handles

Network Evidence

Containment
Eradication
& Recovery

- Event-based alerts
- Header logging
- Full packet logging
- Statistical modeling

Recovery

Containment
Eradication
& Recovery

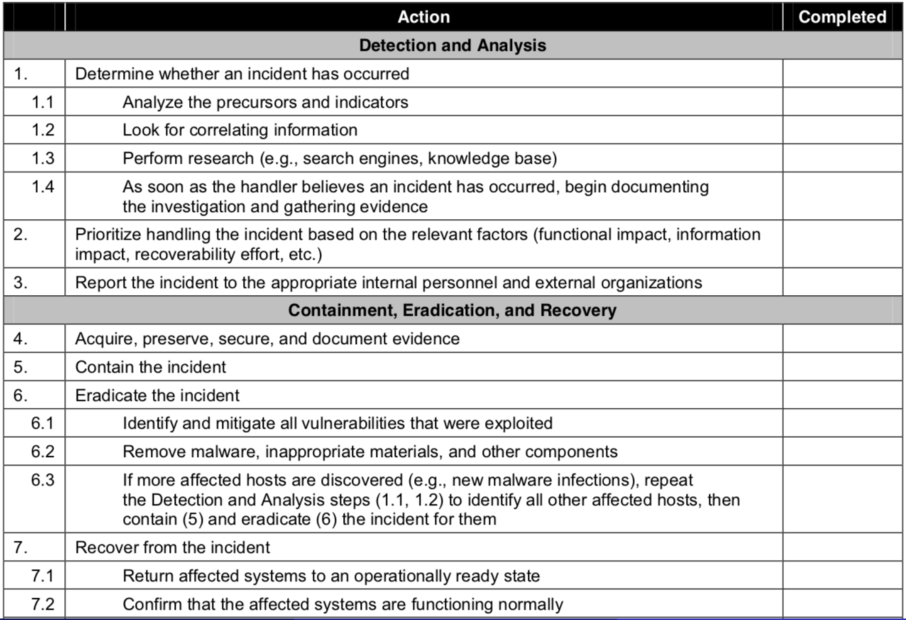
- Back to normal operations
- Minimize business processes disruption
- — all remediation steps done

Lessons Learned

Post-Incident Activity

- Do not waste potential of good incident — incidents are drivers for change and improvement
- Lessons learned report & meeting: learn and improve
- Using collected incident data, e.g., feed the risk assessment process (ultimately may lead to implementation of additional controls)
- Review procedures, processes, fix what did not work

Summary: Incident Response Checklist

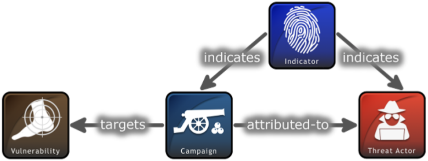


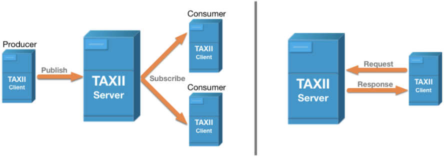
	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	

Bad guys work together, Good guys should too!

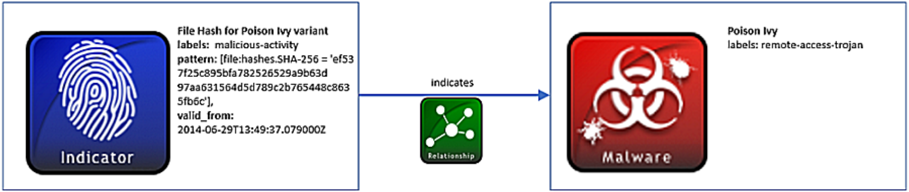
Collaboration & Information Sharing

- STIX: A structured language for cyber threat intelligence
- TAXII: A transport mechanism for sharing cyber threat intelligence





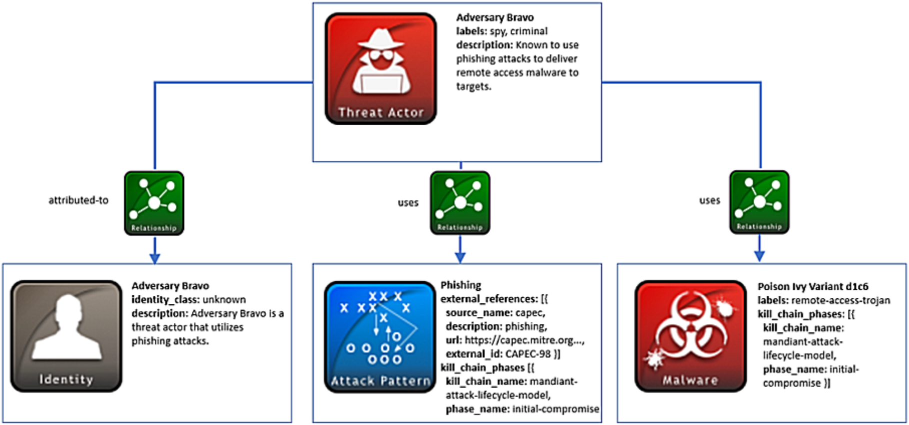
STIX example #1 - Malware Indicator for File Hash



File Hash for Poison Ivy variant
labels: malicious-activity
pattern: [file:hashes.SHA-256 = 'ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c'],
valid_from:
2014-06-29T13:49:37.079000Z

Poison Ivy
labels: remote-access-trojan

STIX example #2 - Threat Actor Leveraging Attack Patterns and Malware



Adversary Bravo
labels: spy, criminal
description: Known to use phishing attacks to deliver remote access malware to targets.

Adversary Bravo
identity_class: unknown
description: Adversary Bravo is a threat actor that utilizes phishing attacks.

Phishing
external_references: [{
source_name: capec,
description: phishing,
url: https://capec.mitre.org...,
external_id: CAPEC-98 }]
kill_chain_phases [{
kill_chain_name: mandiant-attack-lifecycle-model,
phase_name: initial-compromise

Poison Ivy Variant d1c6
labels: remote-access-trojan
kill_chain_phases: [{
kill_chain_name: mandiant-attack-lifecycle-model,
phase_name: initial-compromise }]

Exercise time: How would you handle... ?

- Data Breach (Password of your users published on Pastebin)
- Emails with links to phishing website
- Hacker Group announced that they will hacked all of YOURDOMAIN on July 1st 2014
- Attacker sent you an Email and threatened to launch DDoS attack if you don't pay money
- Receive an email from ShadowServer.ORG about hosts on your network that are running Open Recursive DNS

Resources

- Susan J. Lincke: Incident Response
- NIST Computer Security Incident Handling Guide
- J. Luttgens et al.: Incident Response and Computer Forensics
- Adli Wahid: Incident Response & Handling
- STIX & TAXII: `https://oasis-open.github.io/cti-documentation/`
- `https://idea.cesnet.cz/en/index`

Questions?