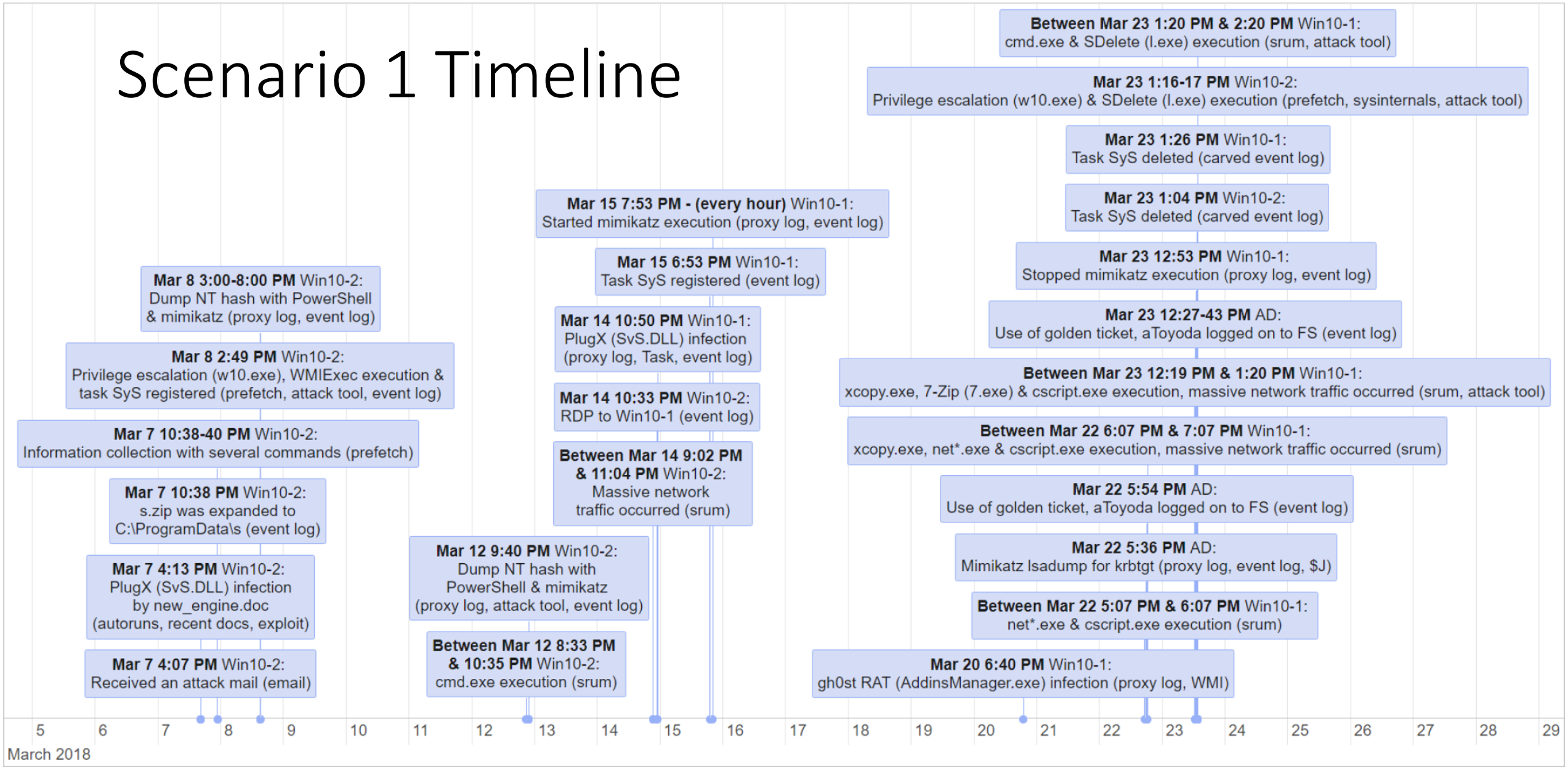
# Wrap Up

# Scenario 1 – Story

- You are an incident responder working for a certain security company.
- One day, you received a request from a customer that is located in Japan. They said, “Our confidential document has been leaked to the Internet. We’d like you to investigate the cause".
  - Time Zone : JST (+9:00)
- The document was stored in a directory on the file server that only the executive can access.
- First, you acquired the executive’s PC and investigated it. However, you could not find any suspicious evidence.
- Therefore, you decided to investigate the system administrator's PC, which may operate as the authority of all users.
- Any administrator rights (including the local administrator rights) are not given to all users except for the system administrator in the customer’s network.
- The leakage of the file on the Internet was confirmed around the end of March 2018.
- It is estimated that it was stolen in March 2018 from the file creation date.

# Scenario 1 Timeline



# The Major Attacks Used in Scenario 1

- Targeted e-mail sent to a user honda.
  - A Word file including Macro in it.
- Lateral Movements
  - RDP, wmiexec and PowerShell
  - Mimikatz (logon password hashes)
  - Golden Tickets
- Privilege escalation using CVE-2017-0213
  - Windows COM Elevation of Privilege Vulnerability
- Possible Rainbow Table password cracking
  - We did not see the evidences of it, but it might have been used.

# Were Files Stolen in Scenario 1?

- Not 100% sure, but there were indicators of attackers accessing the file servers, running 7-zip, and deleted temporarily made file using SDelete.
- The result of SRUM investigation indicate that the infected host has received 64 MB and 33 MB of data with “xcopy”.
- 7-zip was executed on the host.
  - If the purpose of executing it was to compress the acquired files, it is likely that the attackers stole the files.

# Preventing Attacks Used in Scenario 1 (1/3)

- E-mails
  - Always a difficult issue. Possible solutions include:
    - Restrict use of Macros on Microsoft Office
      - https://www.microsoft.com/security/blog/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/?source=mmpc
    - Educate users
    - Application whitelisting
    - SPAM filter?
- Use of Appropriate Logs
  - Audit on file shares/file system activities
  - Reconsider the rotation lifetime of Security logs.

# Preventing Attacks Used in Scenario 1 (2/3)

- Remote Desktop Connection (Windows 8.1+)
  - Use of restricted admin mode to avoid re-use authentication token of RDP clients
    - Prevents pass-the-hash attacks.
  - https://blogs.technet.microsoft.com/kfalde/2013/08/14/restricted-admin-mode-for-rdp-in-windows-8-1-2012-r2/
- Additional LSA (Local Security Authority) Protection (Windows 8.1+)
  - Protects LSA from its memory space being read or codes being injected by non-protected processes.
  - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn408187(v=ws.11)

# Preventing Attacks Used in Scenario 1 (3/3)

- Protected Users Security Group (Windows Server 2012+)
  - Members of this domain group are protected automatically.
    - Prohibits authentication with NTLM, Digest Authentication and CredSSP.
    - Prohibits Kerberos authentication with weaker encryption.
    - Prohibits delegation of user accounts with Kerberos constrained/unconstrained delegation.
    - TGT lifetime (four hours by default) will be configurable.
  - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn466518(v=ws.11)
- Windows Defender Credential Guard (Windows 10+)
  - Adds hardware security and virtualization-based security features.
  - Virtualizes domain authentication and prevents credential attacks.
  - https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard

# Possible Actions

- Prepare logs
  - Audit settings
  - Retention period
  - Avoid logs being cleared (transfer to other log servers, and avoid joining the log server to the domain)
  - Periodic analysis of logs
- Securing hosts
  - As always, apply patch, use antiviruses and personal firewalls, etc…
  - Protect critical accounts
    - Account delegation
    - Restricted Admin mode
  - Application whitelists
- Redesign networks.
  - Disallow clients to communicate with other clients.
  - Isolated networks for administrative machines,
- Education

# Documents on Log Collection

- Microsoft,
  **“Use Windows Event Forwarding to help with intrusion detection”**
  https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
- Microsoft, **“Security auditing”**
  https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview
- Microsoft, **“Recommended settings for event log sizes in Windows”**
  https://support.microsoft.com/en-us/help/957662/recommended-settings-for-event-log-sizes-in-windows

# Implementation

- Discuss and design the policy before an actual incident occurs.
  - Should we construct a SOC inside or outside the company?
  - What can we do to construct a CSIRT?
  - Should we use EDR or audit tools?

- Policy design
- Incident response design

- Who will pay for preparation, implementation, and maintenance?
- Will there be side effects by the implementation?

# Documents on Guidelines/Practices

- Microsoft, **“Windows security guidance for enterprises”**
  https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-compliance
- Microsoft, **“Best Practices for Securing Active Directory”**
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- Australian Cyber Security Centre, **“How to mitigate cyber security incidents”**
  https://www.cyber.gov.au/advice/how-to-mitigate-cyber-security-incidents
- Mitre, **“ATT&CK Matrix for Enterprise”**
  https://attack.mitre.org/matrices/enterprise/
- Mitre, **“ATT&CK Navigator”**
  https://mitre-attack.github.io/attack-navigator/enterprise/

# Catching Up the New Trends/Technologies

- Technology is updated frequently.
  - If you are using Windows 10, it gets a major update every six months.
- Attackers develop new attack methods frequently.
  - Investigators (We) have to know these methods to investigate the incidents.

***Catching up with new trends/technologies is important.***

# Examples of News Sources

- SANS Institute, **“Digital Forensics and Incident Response Blog”**
  https://digital-forensics.sans.org/blog
- Internet Storm Center, **“InfoSec Handlers Diary Blog”**
  https://isc.sans.edu/diary.html
- FireEye, **“Threat Research”**
  https://www.fireeye.com/blog/threat-research.html
- Sean Metcalf, **“Active Directory Security”**
  https://adsecurity.org/
- Phill Moore, **“This Week In 4n6”**
  https://thisweekin4n6.com/

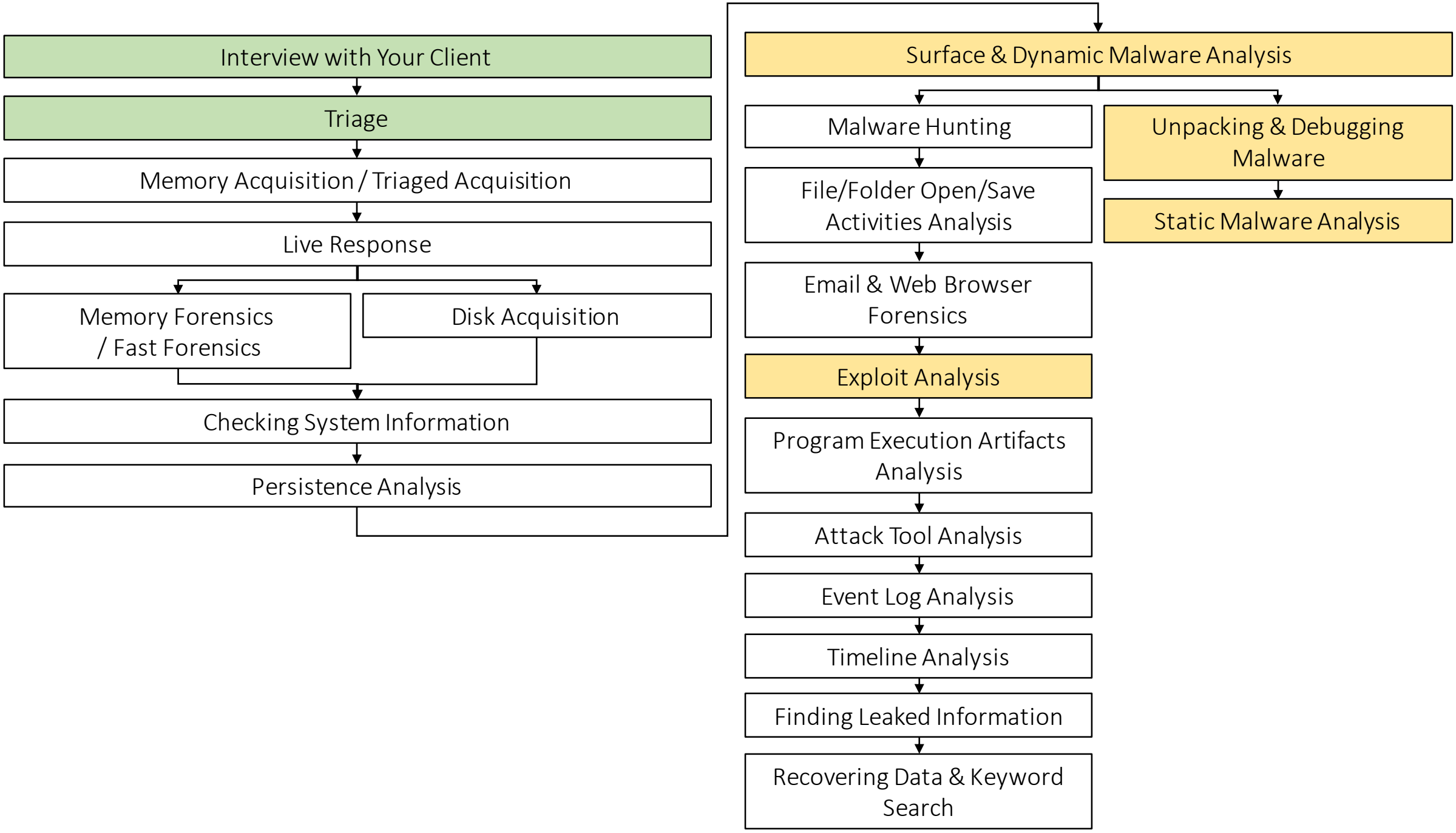
# Course Review

# Review of Overall Topics (1/2)

- Day 1
  1. Introduction
  2. Initial Response
     1. Evidence Preservation
     2. Image Mounting and Parsing
  3. Persistence Analysis
  4. Malware Analysis (Surface & Dynamic Analysis)
  5. Root Cause Analysis
     1. Malware Hunting
     2. File/Folder Open/Save Analysis
  5. Root Cause Analysis (Cont.)
     3. E-mail Forensics
     4. Web Browser Forensics
     5. Exploit Analysis
  6. Lateral Movements Investigation
     1. Program Execution Artifacts Analysis

# Review of Overall Topics (2/2)

- Day 2
  6. Lateral Movements Investigation (Cont.)
     1. Program Execution Artifacts Analysis (Cont.)
     2. Attack Tool Analysis
     3. Event Log Analysis
  7. Timeline Analysis
  8. Finding Leaked Information
  9. Recovering Data & Keyword Search
  10. Memory Forensics
  11. Wrap Up


Interview with Your Client
Triage
Memory Acquisition / Triaged Acquisition
Live Response
Memory Forensics / Fast Forensics
Disk Acquisition
Checking System Information
Persistence Analysis
Surface & Dynamic Malware Analysis
Malware Hunting
File/Folder Open/Save Activities Analysis
Email & Web Browser Forensics
Exploit Analysis
Program Execution Artifacts Analysis
Attack Tool Analysis
Event Log Analysis
Timeline Analysis
Finding Leaked Information
Recovering Data & Keyword Search
Unpacking & Debugging Malware
Static Malware Analysis

# Time to Conclude Our Course

- We have covered many topics in four days.
  - They are useful for investigating actual incidents.
- Whether you can use them appropriately or not is your responsibility.
  - We believe you can.
  - Do not forget to review, and try the extra exercises we did not cover in the class.
- If you have any question, please contact us.

*Thank you!*