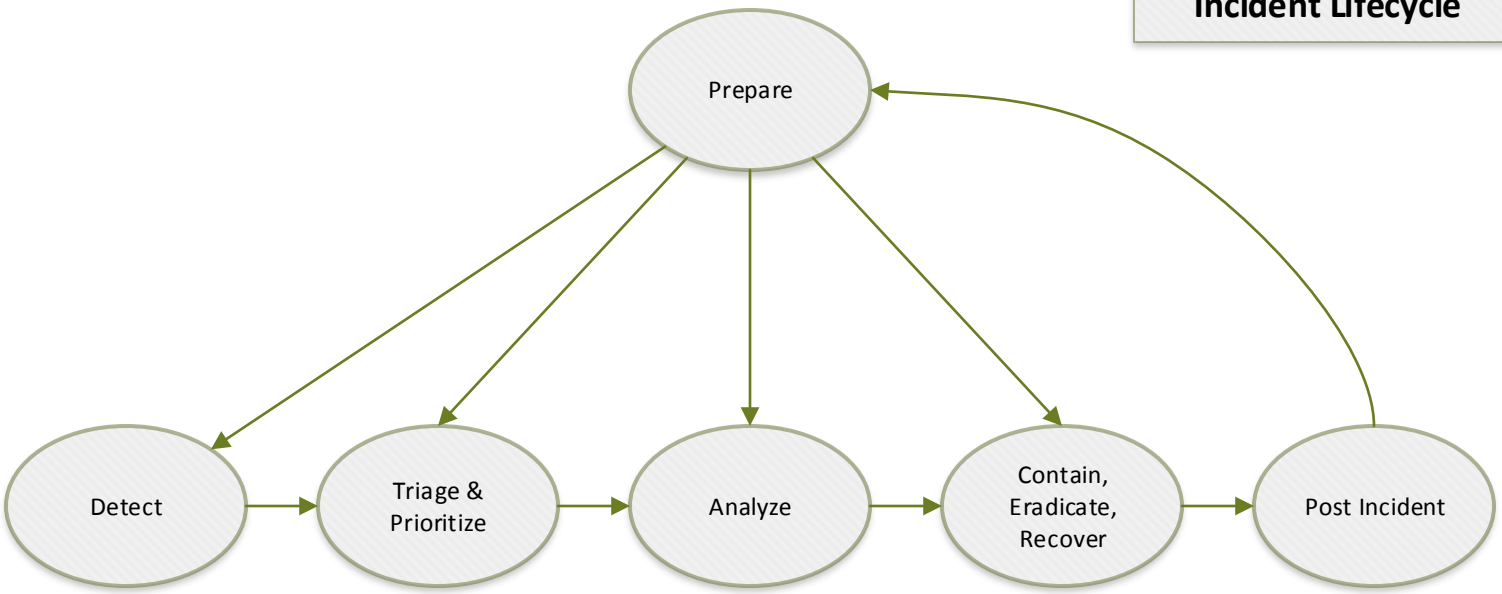
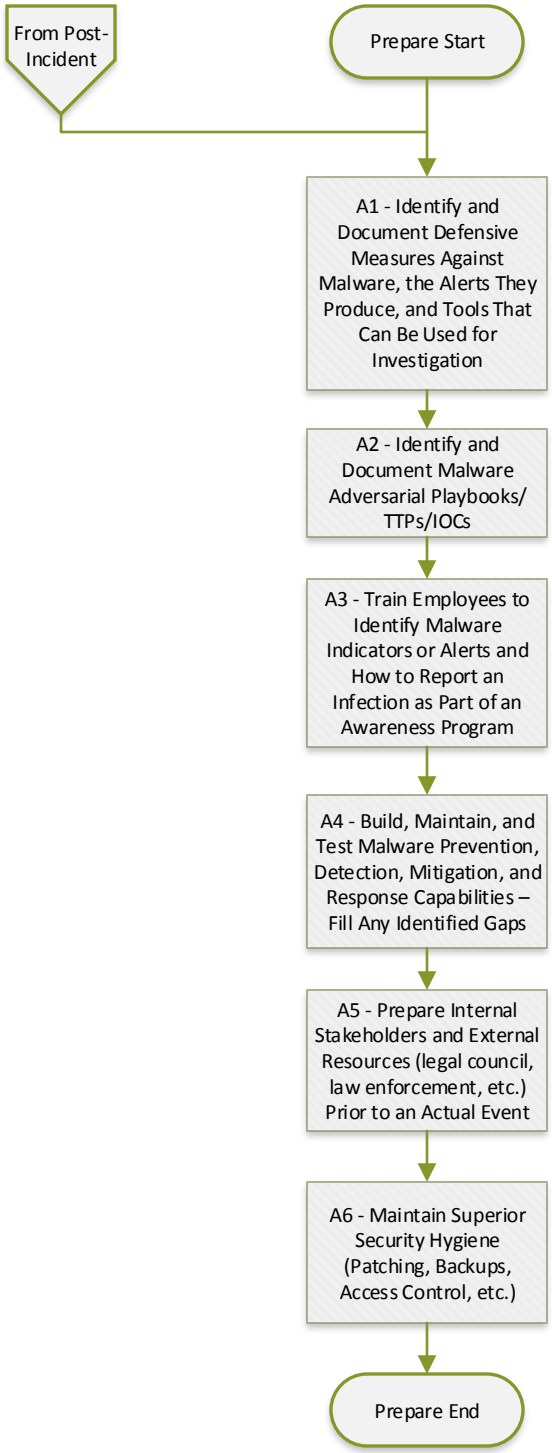
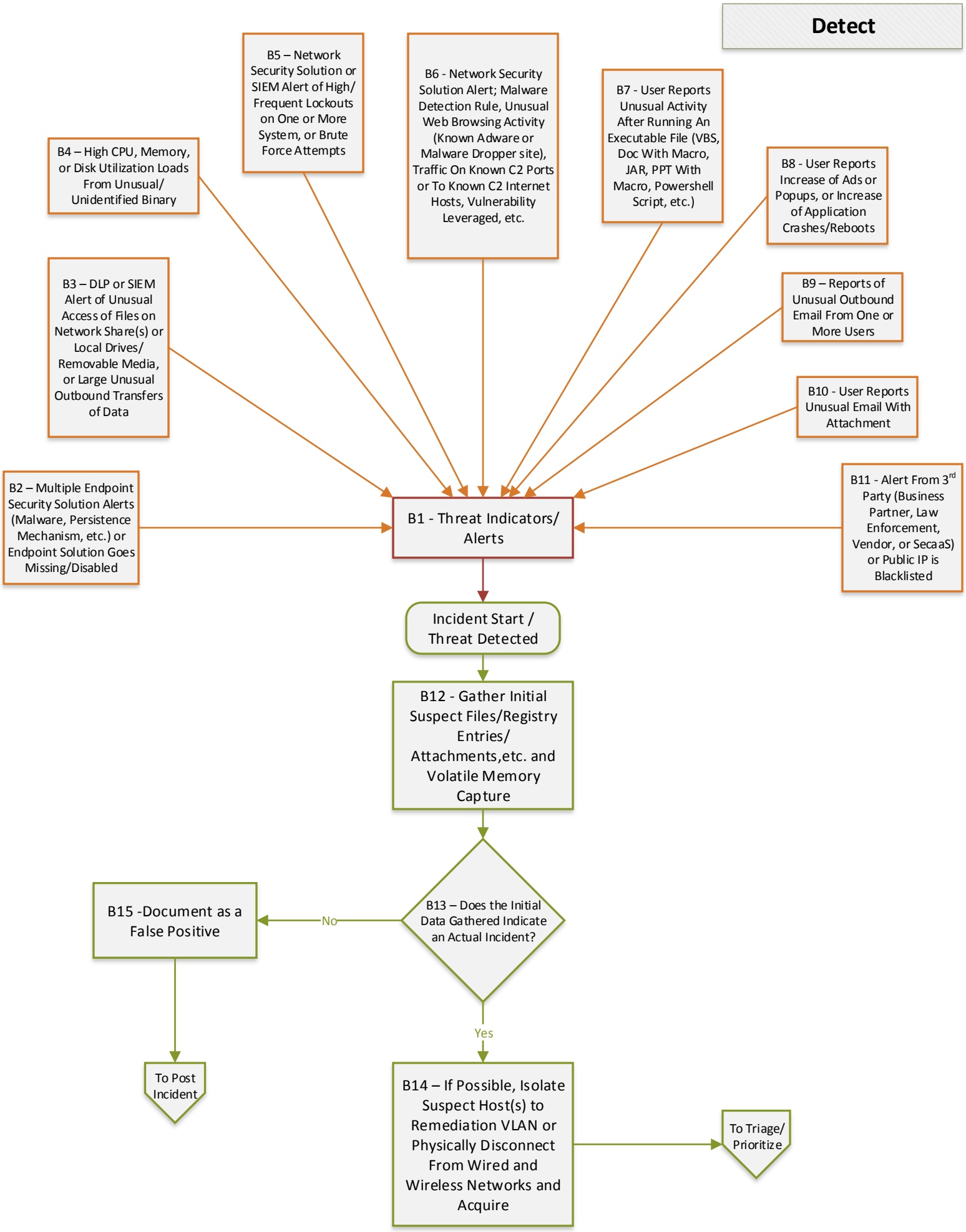
Incident Lifecycle

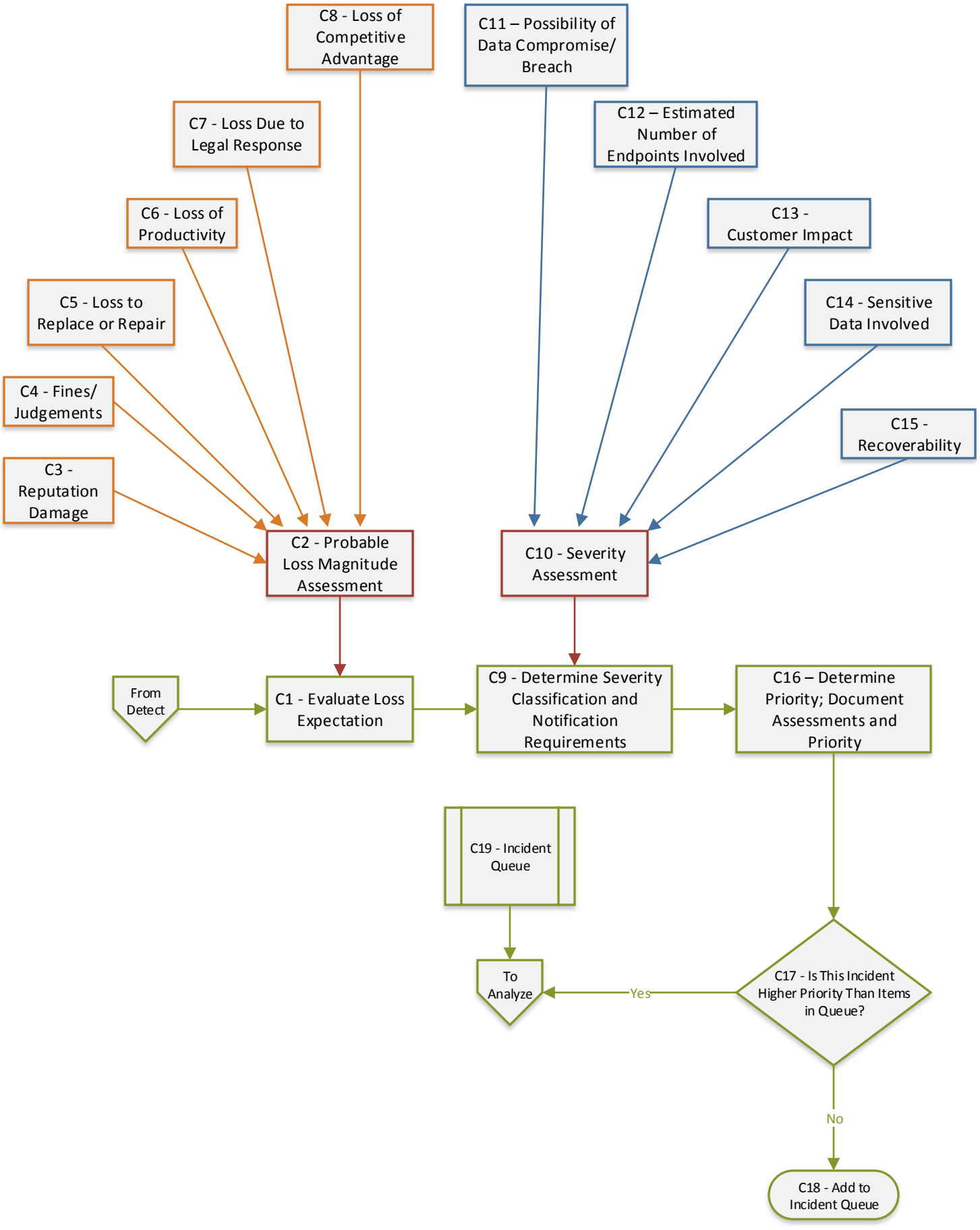


Prepare

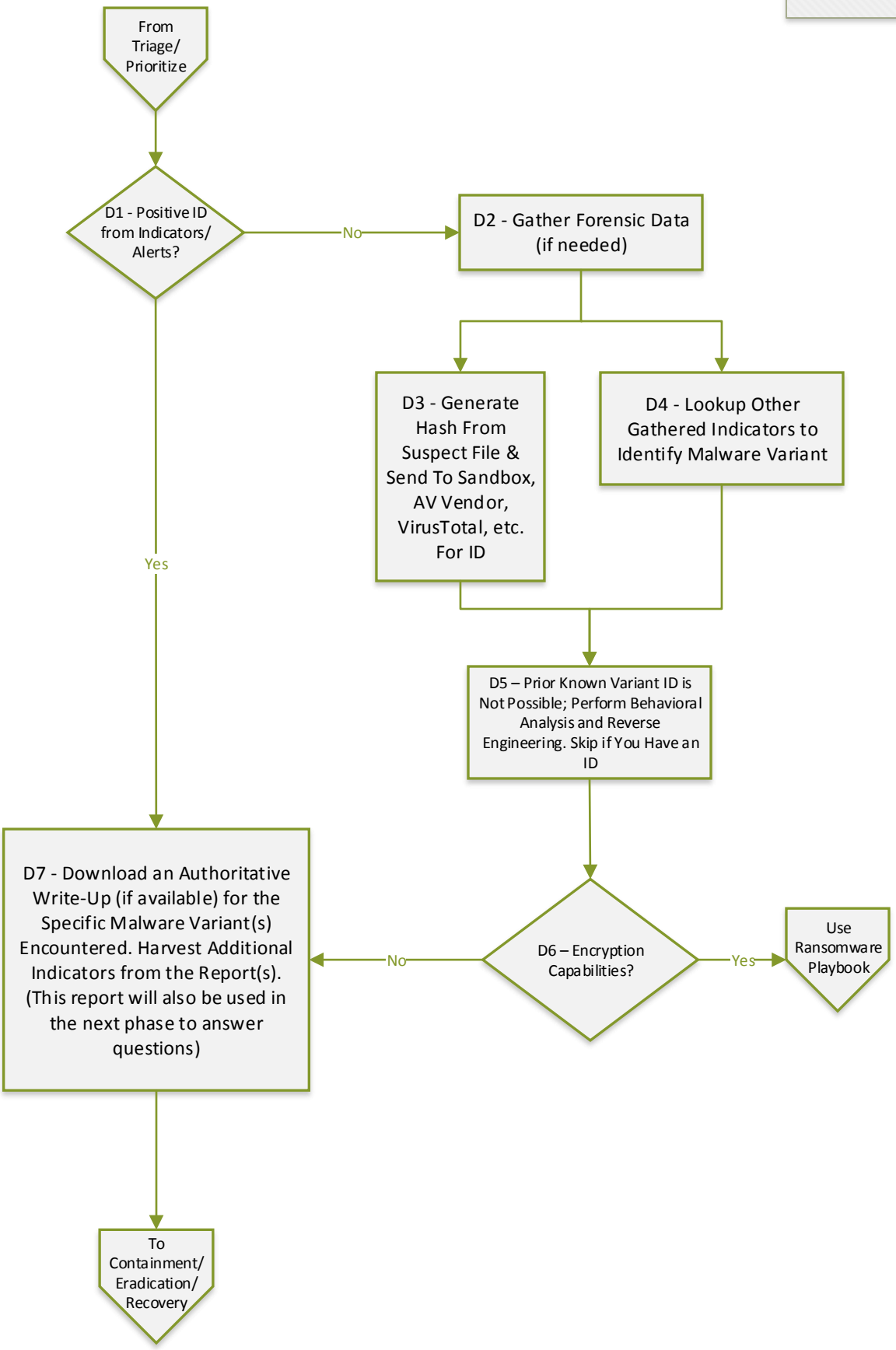

From Post-Incident
Prepare Start
A1 - Identify and Document Defensive Measures Against Malware, the Alerts They Produce, and Tools That Can Be Used for Investigation
A2 - Identify and Document Malware Adversarial Playbooks/ TTPs/IOCs
A3 - Train Employees to Identify Malware Indicators or Alerts and How to Report an Infection as Part of an Awareness Program
A4 - Build, Maintain, and Test Malware Prevention, Detection, Mitigation, and Response Capabilities – Fill Any Identified Gaps
A5 - Prepare Internal Stakeholders and External Resources (legal council, law enforcement, etc.) Prior to an Actual Event
A6 - Maintain Superior Security Hygiene (Patching, Backups, Access Control, etc.)
Prepare End


Detect
B5 – Network Security Solution or SIEM Alert of High/ Frequent Lockouts on One or More System, or Brute Force Attempts
B6 - Network Security Solution Alert; Malware Detection Rule, Unusual Web Browsing Activity (Known Adware or Malware Dropper site), Traffic On Known C2 Ports or To Known C2 Internet Hosts, Vulnerability Leveraged, etc.
B7 - User Reports Unusual Activity After Running An Executable File (VBS, Doc With Macro, JAR, PPT With Macro, Powershell Script, etc.)
B4 – High CPU, Memory, or Disk Utilization Loads From Unusual/ Unidentified Binary
B8 - User Reports Increase of Ads or Popups, or Increase of Application Crashes/Reboots
B3 – DLP or SIEM Alert of Unusual Access of Files on Network Share(s) or Local Drives/ Removable Media, or Large Unusual Outbound Transfers of Data
B9 – Reports of Unusual Outbound Email From One or More Users
B10 - User Reports Unusual Email With Attachment
B2 – Multiple Endpoint Security Solution Alerts (Malware, Persistence Mechanism, etc.) or Endpoint Solution Goes Missing/Disabled
B1 - Threat Indicators/ Alerts
B11 - Alert From 3rd Party (Business Partner, Law Enforcement, Vendor, or SecaaS) or Public IP is Blacklisted
Incident Start / Threat Detected
B12 - Gather Initial Suspect Files/Registry Entries/ Attachments,etc. and Volatile Memory Capture
B13 – Does the Initial Data Gathered Indicate an Actual Incident?
No
B15 -Document as a False Positive
To Post Incident
Yes
B14 – If Possible, Isolate Suspect Host(s) to Remediation VLAN or Physically Disconnect From Wired and Wireless Networks and Acquire
To Triage/ Prioritize

Triage/Prioritize



Analyze


From Triage/ Prioritize
D1 - Positive ID from Indicators/ Alerts?
No
D2 - Gather Forensic Data (if needed)
D3 - Generate Hash From Suspect File & Send To Sandbox, AV Vendor, VirusTotal, etc. For ID
D4 - Lookup Other Gathered Indicators to Identify Malware Variant
Yes
D5 – Prior Known Variant ID is Not Possible; Perform Behavioral Analysis and Reverse Engineering. Skip if You Have an ID
D6 – Encryption Capabilities?
No
Yes
Use Ransomware Playbook
D7 - Download an Authoritative Write-Up (if available) for the Specific Malware Variant(s) Encountered. Harvest Additional Indicators from the Report(s). (This report will also be used in the next phase to answer questions)
To Containment/ Eradication/ Recovery

Contain/Eradicate/ Recover

From Analyze

E1 - Able to Blacklist Executables?

Yes

E2 - Blacklist Malware and Dropper/Downloader/ Infection/Persistence Mechanism Hashes

No

E3 - Scan Endpoints to Find Additional Infections. Check System/Network Artifacts (Logs, Flows, Filenames, Hashes, Registry Entries, etc,) for Indicators of Compromise and Lateral Movement

E4 - Isolate New Suspect Host(s) to Remediation VLAN (when using remote tools) or Physically Disconnect From Wired and Wireless Networks and Acquire

E5 - If Possible, Block Known Communication (External C2C and Internal Propagation), Exfiltration, and Infection Channels (Firewall, IPS, HIPS, Email Senders, NAC, etc.)

E6 - Use Remote (if available)/ Admin Tools to Kill Malicious Processes and Remove Infected Files/Droppers/Downloaders/ Persistence Mechanisms from Infected Hosts

E7 - Apply Patches, Security Products, etc. or Other Mitigations to Prevent Re-Infection

E8 – Bootkit or UEFI Rootkit That Cannot Be Cleaned By Your Security Tools?

No

Yes

E9 – Take a Full Forensic Image, Including Volatile Data. Wipe Partition Table (Bootkit) or Re-Flash BIOS/UEFI and Rebuild

E10 – Does this Malware Variant Create a Remote Access Channel? (Botnet,RAT,Rootkit, Reverse Shell,etc)

Yes

Add System Compromise/ Breach Playbook, Continue This Playbook

No

E11 – Does this Malware Variant Collect and Exfiltrate Sensitive or Protected Data Types? (MiTM, MiTB, Keylogger, etc.)

Yes

Add Data Loss/ Theft Playbook, Continue This Playbook

No

E12 – Does this Malware Variant Collect and Exfiltrate Credentials? (MiTB, Keylogger, etc.)

Yes

E13 – Change All Affected Credentials

E14 – Check Internal and External Systems For Login Attempts From Unexpected Sources and Login Failures on Unexpected Systems

E15 - Signs of Compromise?

Yes

Add Authority/ Credential Misuse Playbook, Continue This Playbook

No

Additional Hosts Found

E16 – If Needed, Chain the Attack (Investigative Chains) Backward and Forward Until You Discover the Initial Infection Vector and Each Infected Endpoint

E17 - Rescan Endpoints for Indicators of Compromise and Lateral Movement, Include Any Additional Indicators Discovered During Containment

No Additional Hosts Found

E18 – Files May Have Been Damaged When Infected, Depending Upon the Malware's Capabilites. Check Your Anti-Virus/Malware Logs for Files That Were Deleted (as opposed to cleaned)

E19 - Backups Available of Deleted Files?

Yes

E20 - Restore Deleted Files

No

E21 - Block Any Additional Communication and Infection Channels Discovered During Containment and Eradication (Firewall, IPS, HIPS, Email Senders, NAC, etc.)

E22 – Return and Reconnect Isolated Hosts

E23 - Send Samples/Indicators to Vendors That Did Not Detect Threat (follow their defined process)

E24 - Implement New/Custom Detection Rules (IPS, Anti-Malware/Virus, Log Correlation, Analytics, etc.) To Better Detect Other/Future Infections

To Post-Incident

Post-Incident