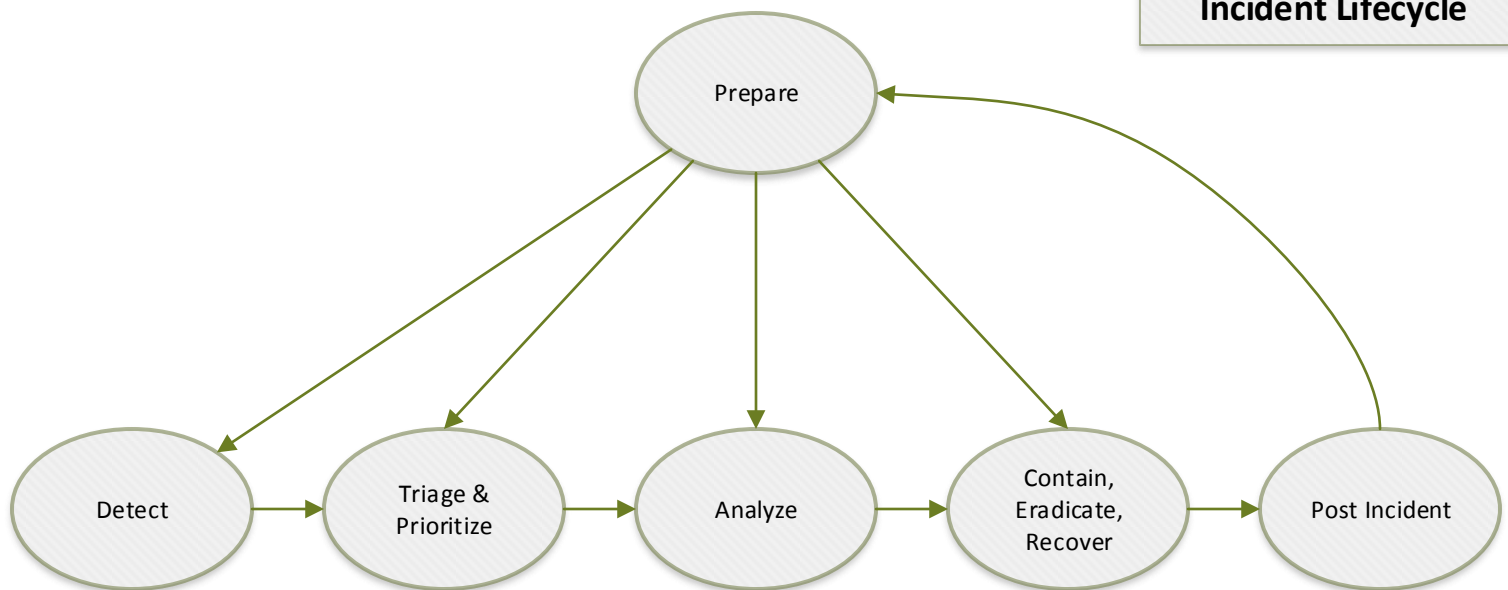


Incident Lifecycle



This work is licensed under [Creative Commons Attribution-ShareAlike 4.0](https://creativecommons.org/licenses/by-sa/4.0/)

<https://creativecommons.org/licenses/by-sa/4.0/>

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Copyright 2016 Joshua C Geno

From Post-Incident

Prepare Start

Prepare

A1 - Identify and Document Defensive Measures Against Ransomware, the Alerts They Produce, and Tools That Can Be Used for Investigation

A2 - Identify and Document Ransomware Adversarial Playbook/ TTPs/IOCs

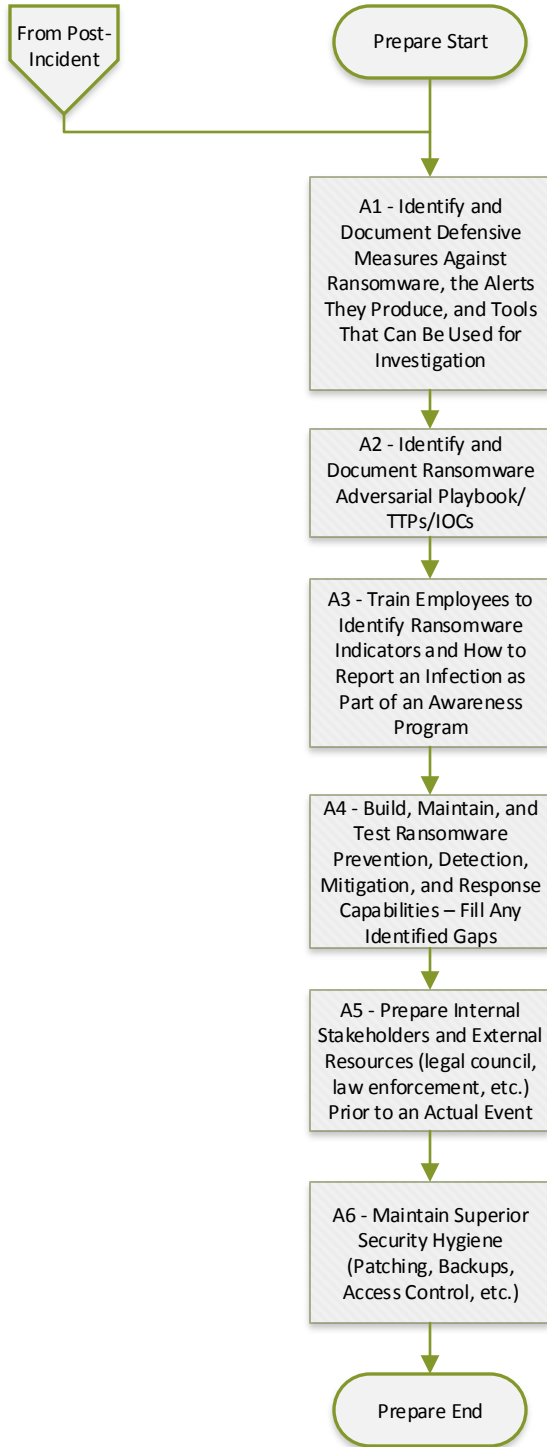
A3 - Train Employees to Identify Ransomware Indicators and How to Report an Infection as Part of an Awareness Program

A4 - Build, Maintain, and Test Ransomware Prevention, Detection, Mitigation, and Response Capabilities – Fill Any Identified Gaps

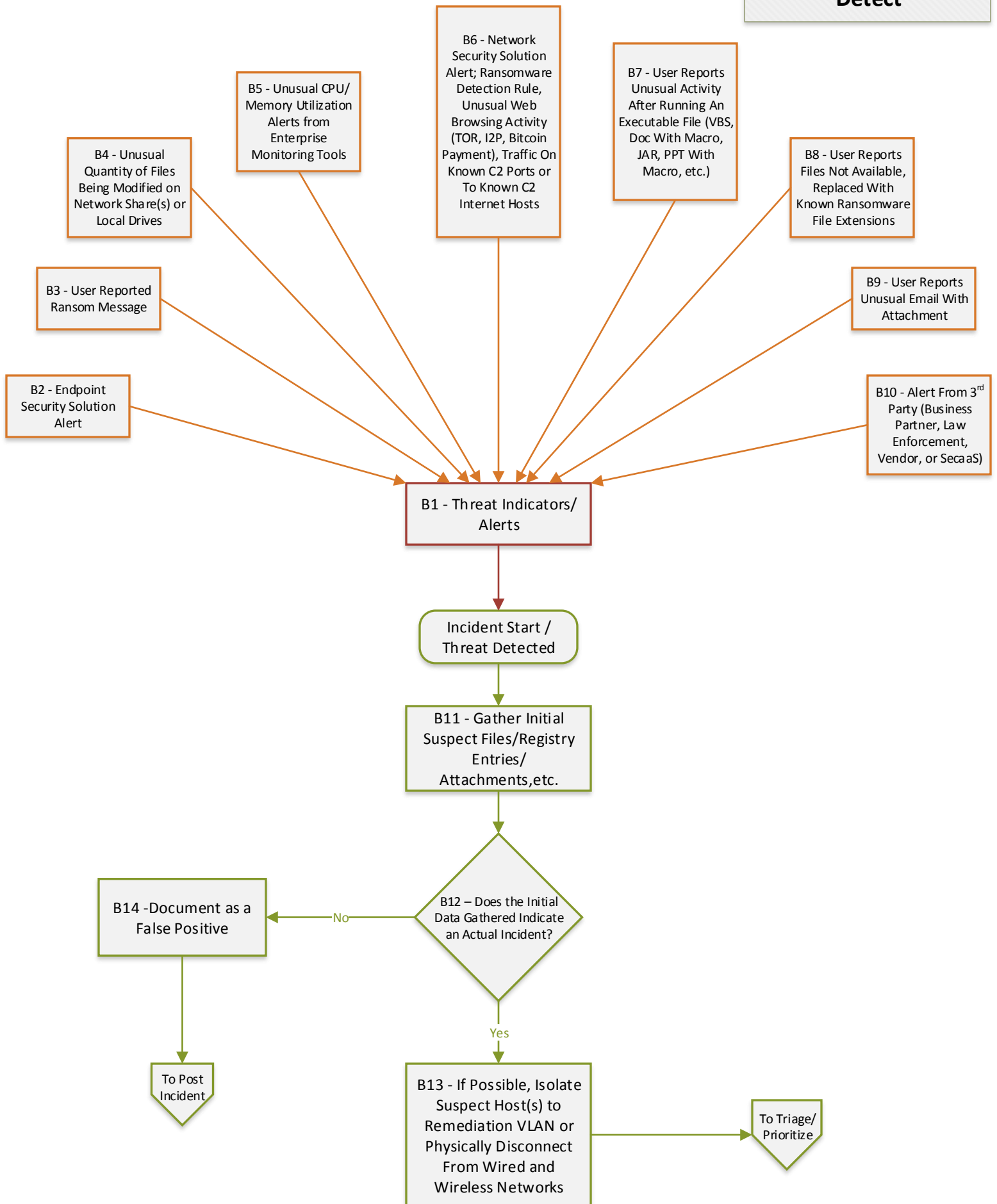
A5 - Prepare Internal Stakeholders and External Resources (legal council, law enforcement, etc.) Prior to an Actual Event

A6 - Maintain Superior Security Hygiene (Patching, Backups, Access Control, etc.)

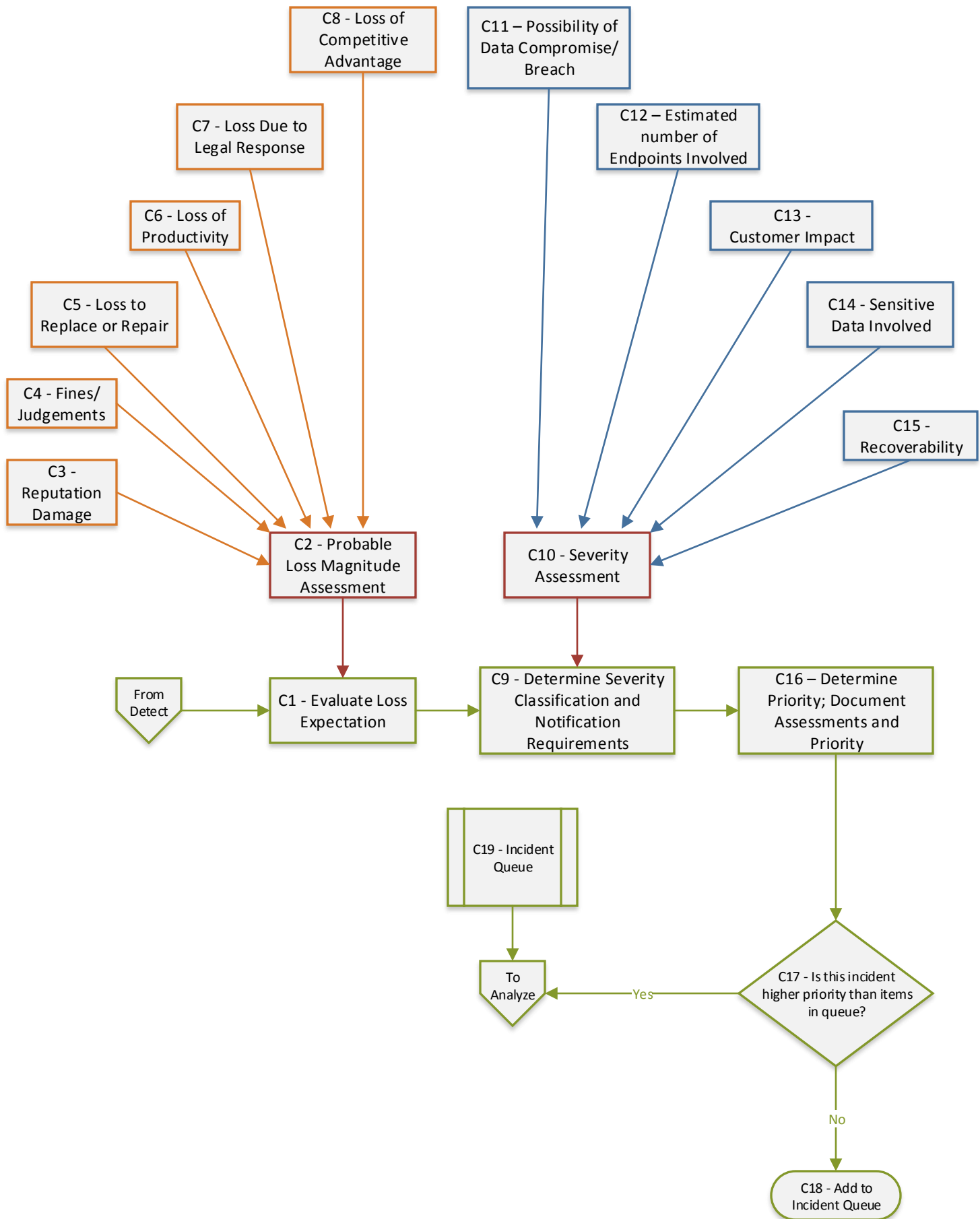
Prepare End

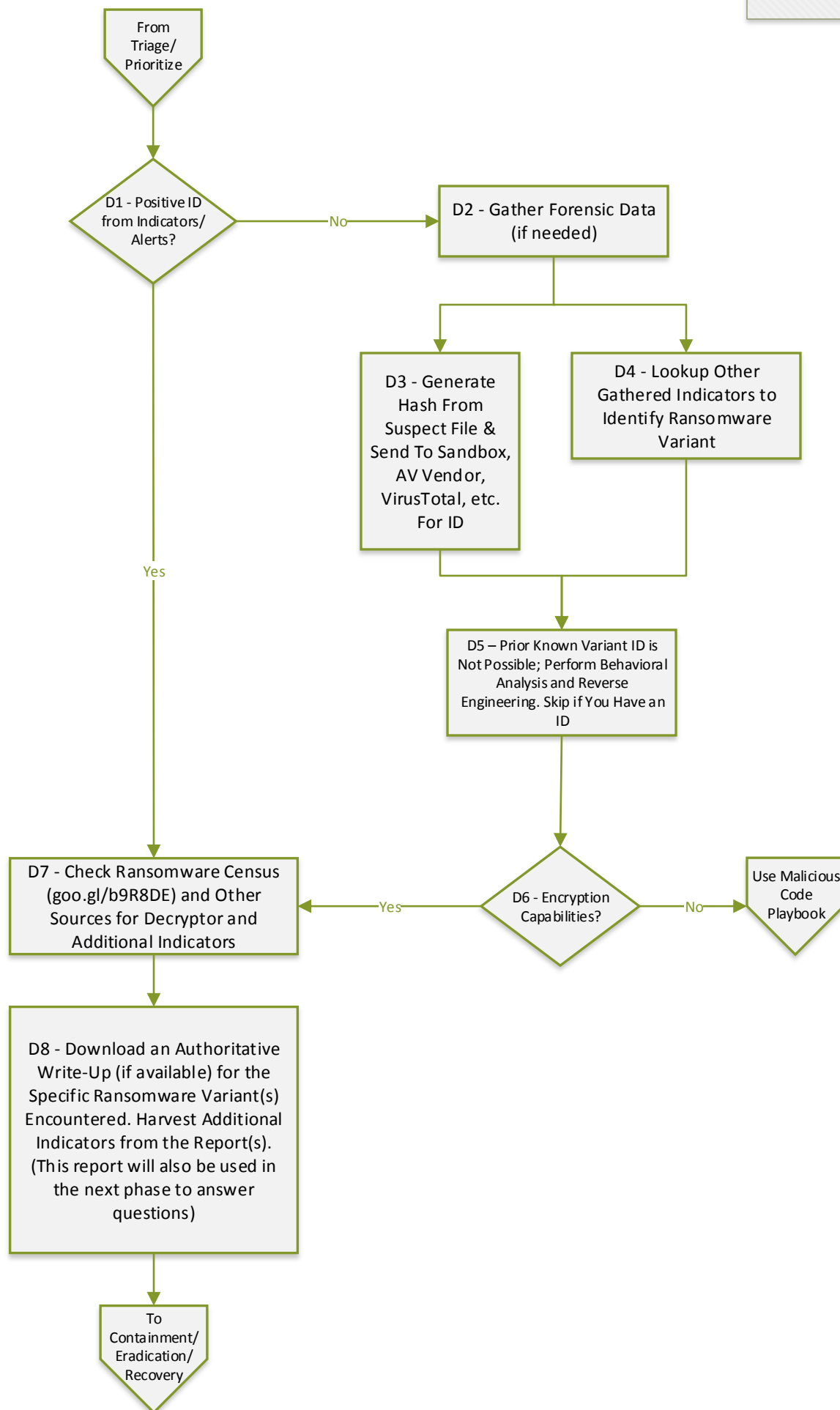


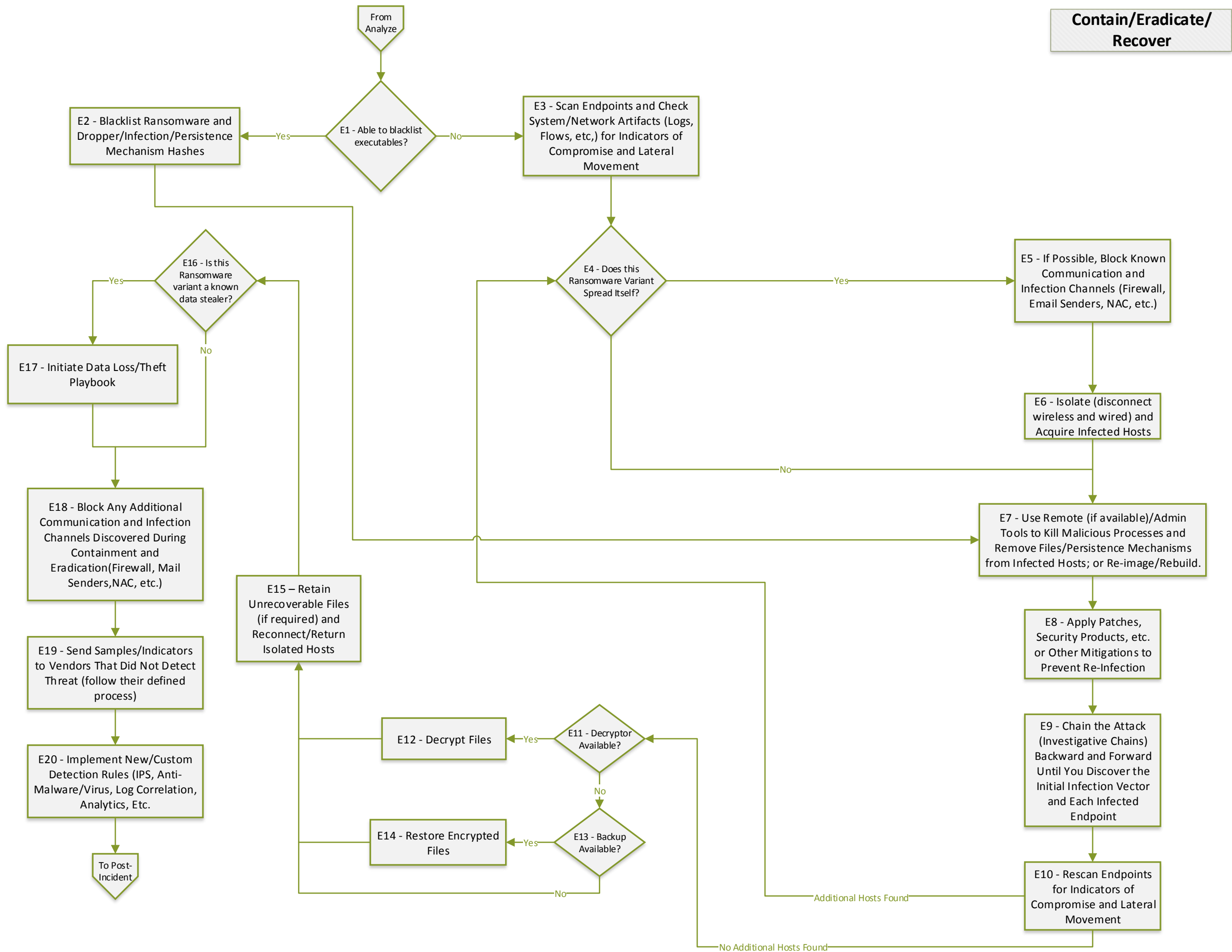
Detect



Triage/Prioritize







Post-Incident

