Incident Response Plans

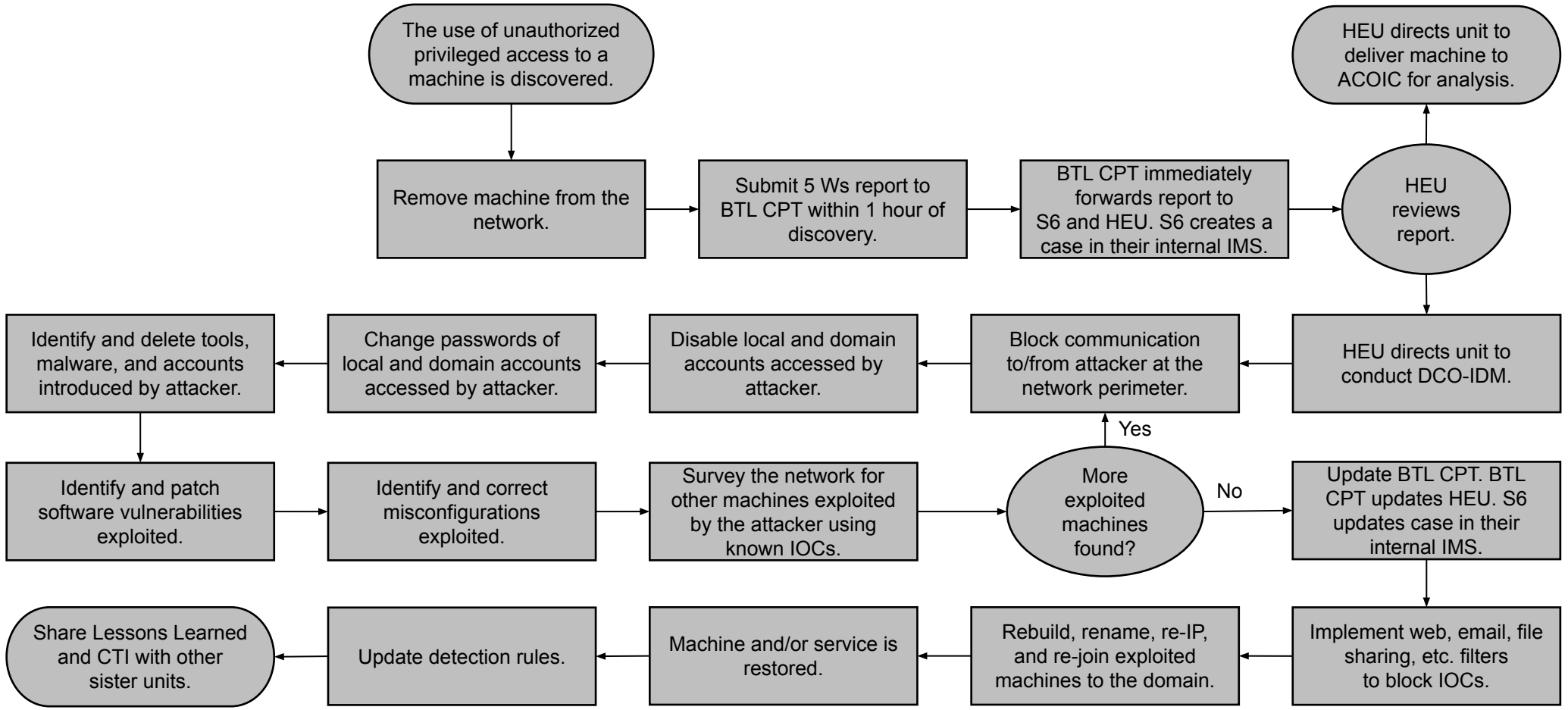
Incident Response Plans
Acronyms

Acronyms	
AUP	Acceptable Use Policy
BTL CPT	Battle Captain
CTI	Cyber Threat Intelligence
DCO-IDM	Defensive Cyberspace Operations – Internal Defensive Measures
HEU	Higher Echelon Unit
IMS	Incident Management System
IP	Internet Protocol Address
IRP	Incident Response Plan
IOCs	Indicators of Compromise
SAAR	System Access Authorization Request
PACE	Primary, Alternate, Contingency, Emergency

Incident Response Plans
Execution Criteria

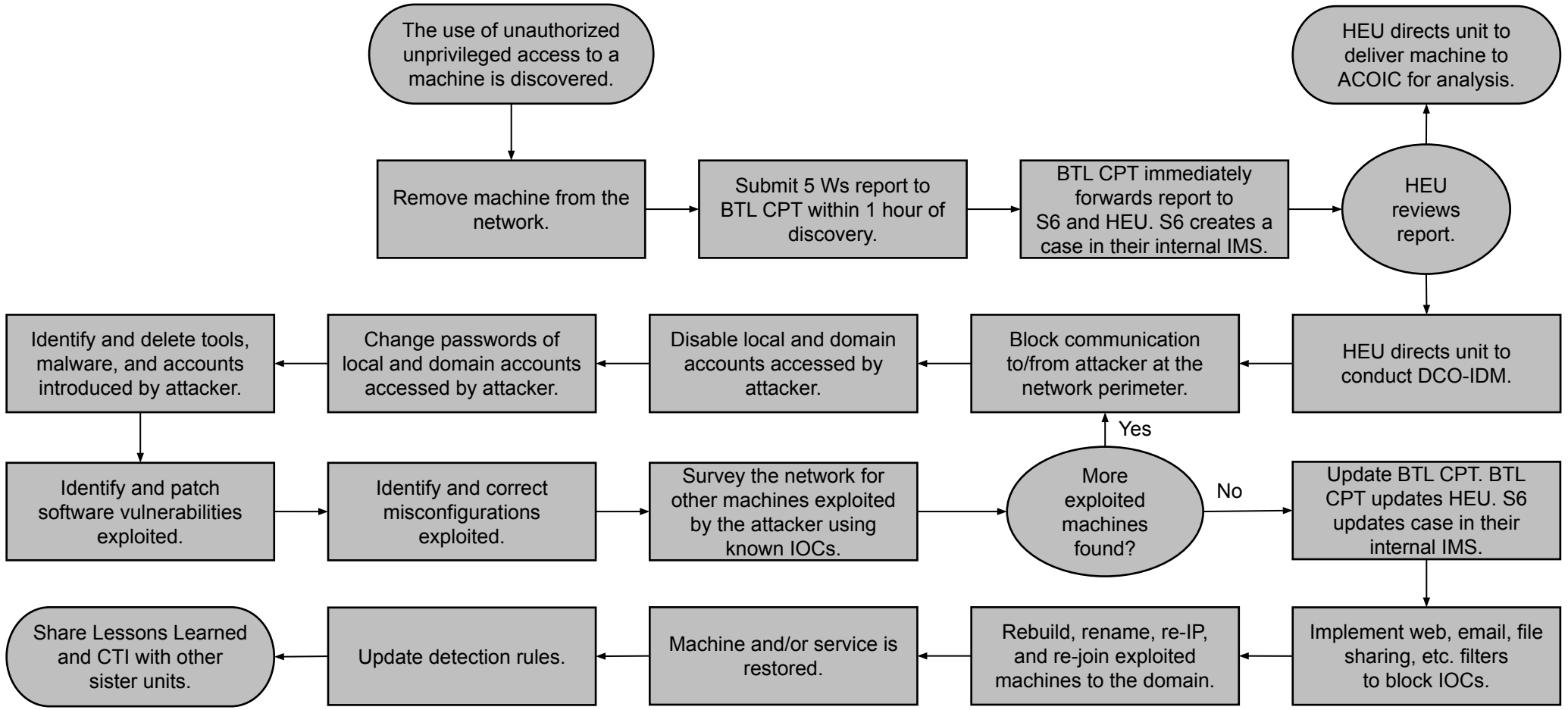
IRP Number	Incident Description	Incident Category	Execution Criteria
#01	Root Level Intrusion	Category 1	Execute this IRP when the use of unauthorized privileged access to a machine has been discovered.
#02	User Level Intrusion	Category 2	Execute this IRP when the use of unauthorized un-privileged access to a machine has been discovered.
#03	Unsuccessfully Activity Attempt	Category 3	Execute this IRP when deliberate, but unsuccessful attempts to gain unauthorized access to a machine have been discovered.
#04	Denial of Service	Category 4	Execute this IRP when activity that denies, degrades, or disrupts the functionality of a machine or network has been discovered.
#05	Non-Compliance Activity	Category 5	Execute this IRP when activity that violates the Cybersecurity or Acceptable Use Policy has been discovered (e.g., unauthorized disclosure, cross-domain violation).
#06	Reconnaissance	Category 6	Execute this IRP when activity that seeks to gather information about a machine or network without authorization has been discovered.
#07	Malware	Category 7	Execute this IRP when the installation of software intended for gaining unauthorized access to a machine or network has been discovered. If the software in question provides remote access, execute Battle Drill #1 or #2. Examples of malware that does not provide remote access, but aims to gain unauthorized access includes keyloggers, password crackers, and enumeration tools.

Incident Response Plan #01
Root Level Intrusion (Incident Category 1)



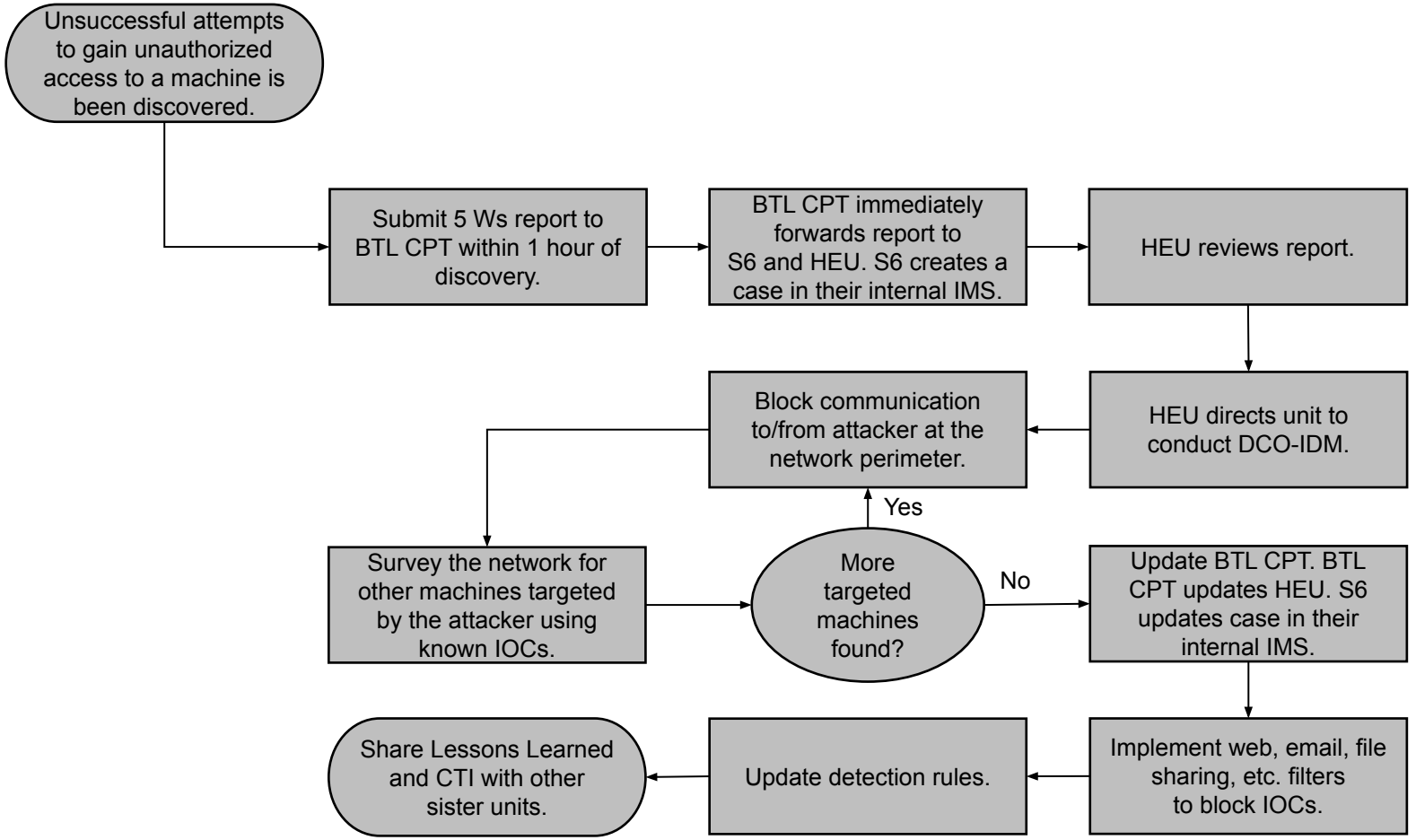
Victor Fernandez III

Incident Response Plan #02
User Level Intrusion (Incident Category 2)

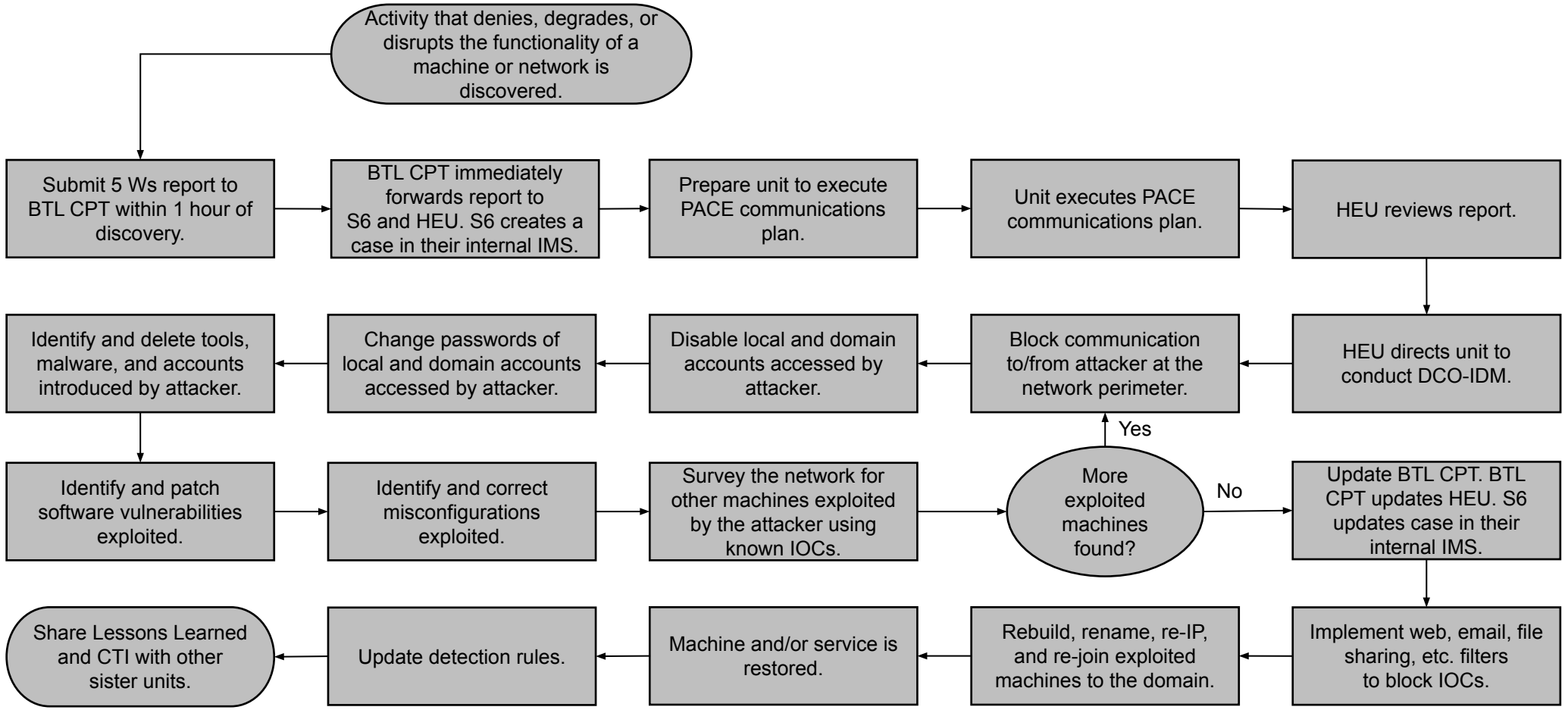


Victor Fernandez III

Incident Response Plan #03
Unsuccessful Activity Attempt (Incident Category 3)

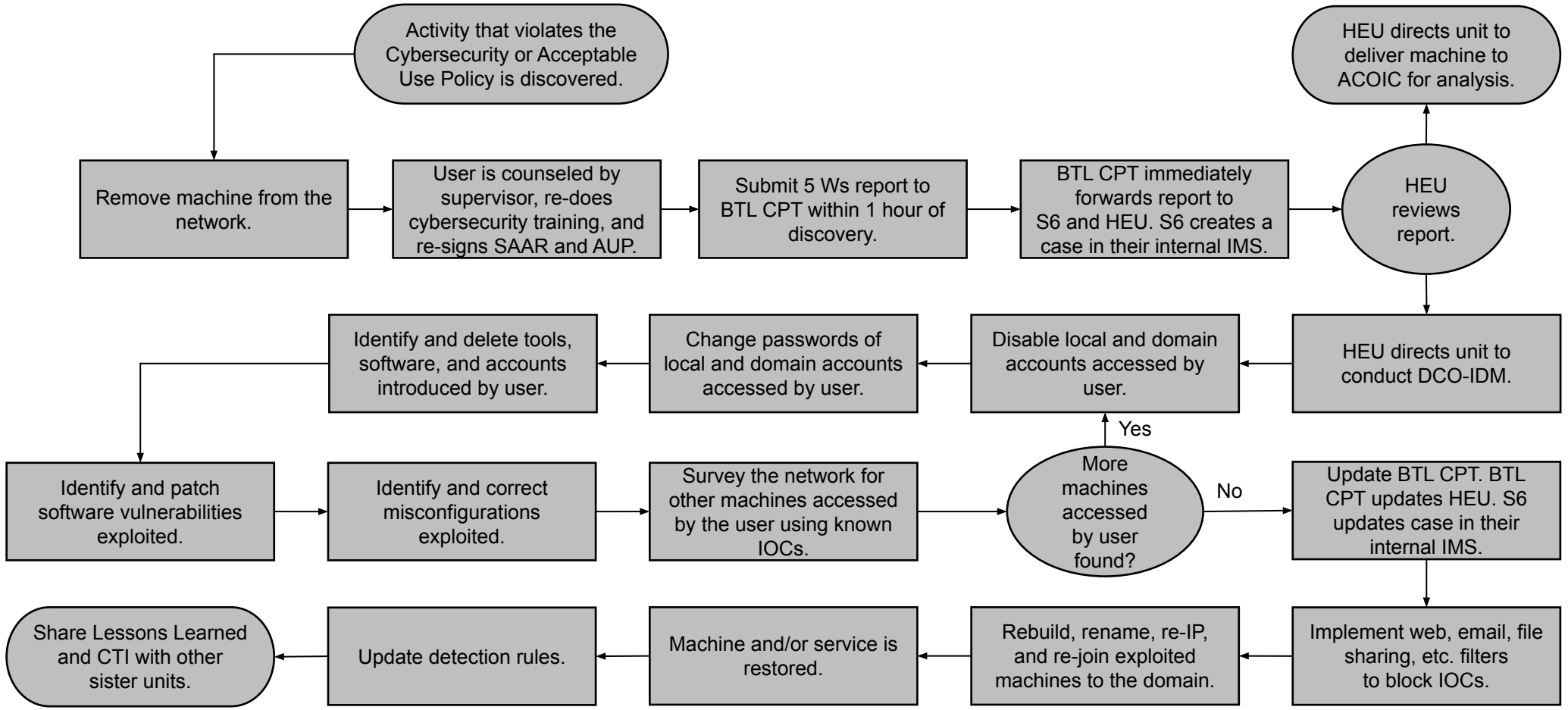


Incident Response Plan #04
Denial of Service (Incident Category 4)



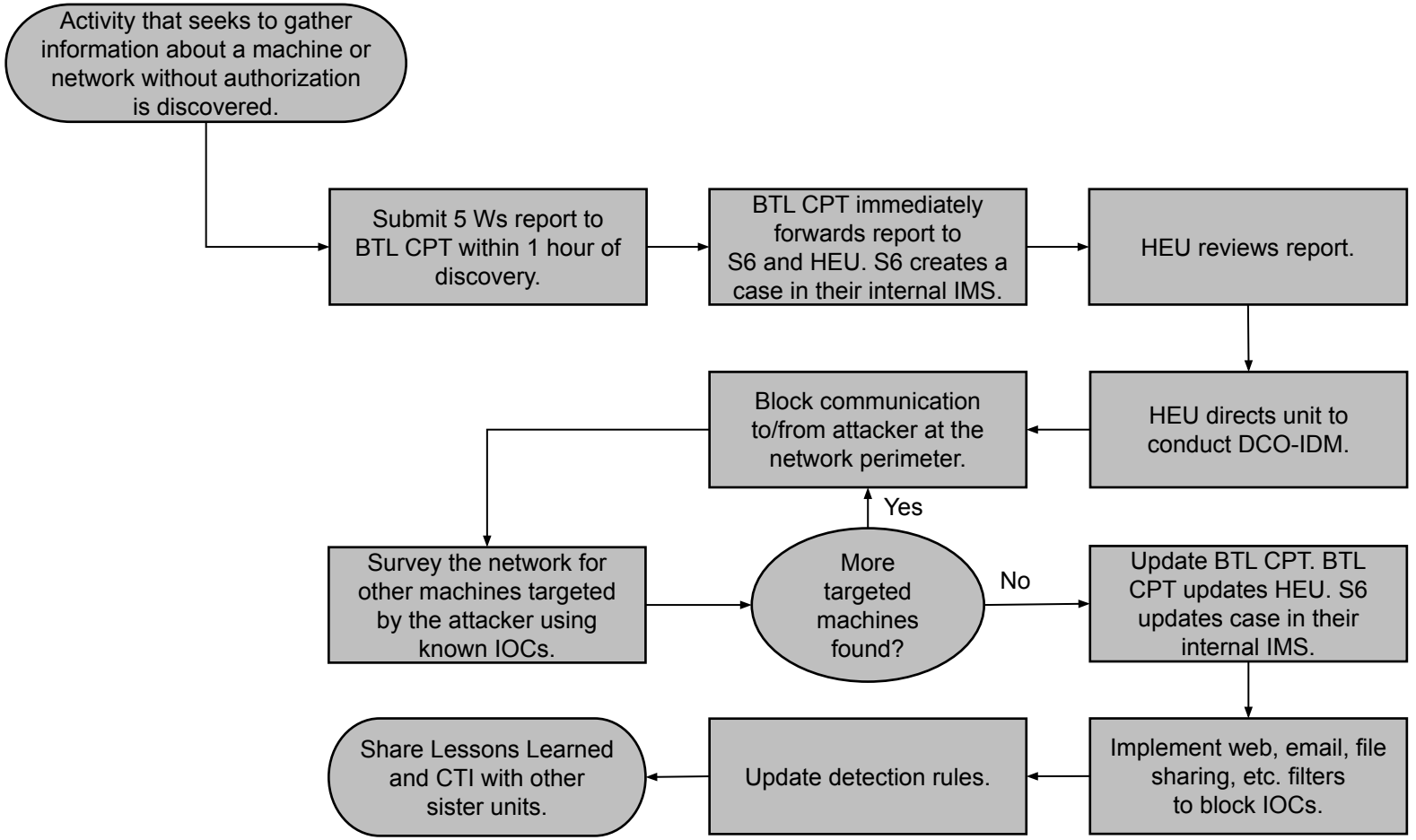
Victor Fernandez III

Incident Response Plan #05
Non-Compliance Activity (Incident Category 5)

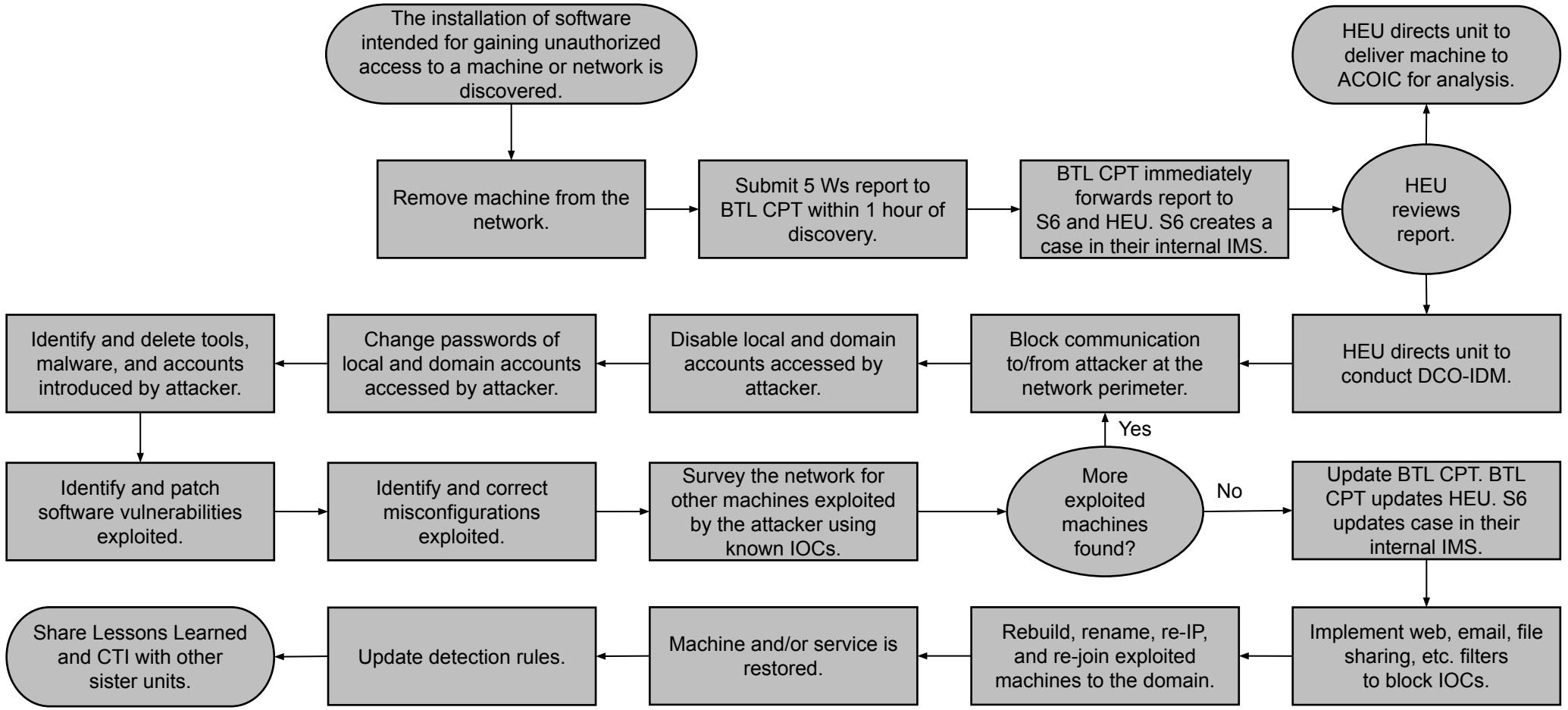


Victor Fernandez III

Incident Response Plan #06
Reconnaissance (Incident Category 6)



Incident Response Plan #07
Malware (Incident Category 7)



Victor Fernandez III