Security Investigation Workflow

1. Create Magic Ticket
2. Security Investigation Reported
   (See Incident Reporting Process Workflow)
3. Identify System Location and Owner/Administrator
4. Gather Information about Computer’s Sensitivity and Function
5. Run Security Tool on System
6. Run Sensitivity Scan
7. Suspect the Machine has been Compromised and:
   - Sensitive Data Found?
   - Attacking other computers?
   - Yes
   - No
8. Escalate to CSIRT Status
9. Close Ticket

CSIRT Incident Workflow

Suspect the Machine has been Compromised and:
- Sensitive Data Found?
- Attacking other computers?
- Yes
- No

Identify Problem
Identify Solution
Implement Solution
Work with Client to Ensure Successful Remediation
Escalate to CSIRT Status
CSIRT Incident Workflow

1. CSIRT Incident Reported
2. Run Security Tool
3. Has Volatile Memory been Captured?
   - No
   - Yes
4. Unplug Power Cord and Confiscate Machine
5. Make Copies and Images of Hard-Drive(s)
6. Analyze Image and/or Throwaway Copy of Hard-Drive
7. Sensitive Data Found?
   - No
   - Yes
8. Police Involvement Necessary?
   - No
   - Yes
9. Clear and Reformat Hard-Drives
10. Return Machine to User
11. Create or Escalate Incident Ticket
12. Contact Exec. Dir., Exec Dept. CIO, CIO
13. Present Final Report
14. Escalate Incident to Police Department
15. Report Sensitive Data Findings to Appropriate Person(s)
16. Is there a Reason to keep Forensic Copy of Hard-Drive?
   - No
   - Yes
17. Clear Forensic Copy of Hard-Drive
18. Keep Forensic Copy of Hard-Drive in Safe
19. Close Ticket