Incident Response Playbook: Shadow IT

Team AnubisX

Version 1.0
September 17, 2025

Document Control

Attribute	Value
Version	1.0
Status	Final
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a structured incident response plan for handling suspicious software installations and unauthorized application usage (shadow IT). The objective is to detect unapproved or potentially malicious software early, mitigate associated risks, and restore compliance with security policies.

1.2 Scope

This playbook applies to endpoints, servers, and cloud-managed systems across the organization. It covers incidents involving installation of unauthorized or malicious software, shadow IT usage, and applications that bypass corporate security controls.

2 Overview of Shadow IT

Suspicious or unauthorized software installation (shadow IT) introduces risks such as malware infection, data leakage, compliance violations, and unmanaged attack surfaces. Such applications may be intentionally installed by users without IT approval or deployed by attackers to maintain persistence or exfiltrate data.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure readiness to detect and respond to unauthorized software installations.

- **Roles and Responsibilities:** Define roles (Incident Commander, SOC Analysts, IT Endpoint Team, Legal, Communications).
- **Tools & Resources:** Ensure availability of EDR, application allowlisting tools, software inventory systems, SIEM, and forensic tools.
- **Training:** Conduct awareness sessions on risks of shadow IT and phishing-based installs.
- **Hardening Controls:** Implement application allowlisting, centralized software deployment, strict endpoint policies, and user education.
- **Contact Lists:** Maintain IT, vendor support, and IR partner contacts.
- **Threat Intelligence:** Monitor campaigns distributing trojanized software or supply-chain risks.

3.2 Phase 2: Identification & Analysis

Goal: To confirm unauthorized software installation and assess its scope and severity.

1. **Initial Triage:** Collect endpoint alerts, installation logs, and application inventories. Open an incident ticket and enable secure communications.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:

- **Endpoint:** Unapproved software detected, registry/service changes, or unsigned executables.
- **Network:** Unusual outbound traffic after software install (C2 or cloud sync).
- **User Behavior:** End-user reports strange software or abnormal prompts.

3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the nature of the software, the scope of installation, and the sensitivity of the affected systems.

Level	Description	Example	MTTD	MTTR
Low	Single unauthorized application detected on a non-critical workstation.	A user installed a personal productivity app without IT approval.	6-12 hours	24-48 hours
Medium	Suspicious software installed on one or a few systems with potential data access.	A user installs an unauthorized file-sharing app exposing limited corporate files.	12-24 hours	2-4 days
High	Unauthorized or malicious software deployed across multiple endpoints or critical systems.	A trojanized application is deployed across finance team laptops, showing outbound C2 connections.	24-48 hours	4-7 days
Critical	Widespread unauthorized/malicious software installation causing disruption or compromise.	Malicious software is installed on servers and endpoints, used as a persistence/backdoor by attackers.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious software activity with other telemetry and vendor intelligence.
   - **If True Positive (TP):** The activity is confirmed as unauthorized or malicious software. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the shadow IT playbook.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and refine allowlisting policies.
5. **Incident Declaration:** If confirmed, formally declare a shadow IT/malware incident and escalate to leadership, legal, and relevant IT teams.

3.3 Phase 3: Containment

Goal: To prevent the spread or impact of the unauthorized software.

- **Short-Term Containment (Immediate Actions):**
  - Isolate affected systems from the network.
  - Block the application's executable via EDR/allowlisting.
  - Restrict user accounts responsible for the installations.

- **Evidence Preservation:** Quarantine suspicious files and preserve forensic images of affected systems **before** remediation.
- **Long-Term Containment Strategy:** Enhance network egress filtering to block traffic from unauthorized applications.

3.4 Phase 4: Eradication

Goal: To completely remove the unauthorized software and any related artifacts.

- **Root Cause Analysis:** Determine how the software was installed (e.g., user action, vulnerability).
- **Software Removal:** Remove the unauthorized or malicious software from all affected endpoints.
- **System Remediation:** Patch vulnerabilities exploited by installers and rotate any potentially compromised credentials.
- **Policy Update:** Update allowlisting/blacklisting policies to prevent re-installation.

3.5 Phase 5: Recovery

Goal: To safely restore systems to a compliant and secure state.

- **System Restoration:** Reintroduce cleaned systems into the production environment.
- **Validation:** Validate that all systems are compliant with security policies and the unauthorized software is gone.
- **Enhanced Monitoring:** Closely monitor endpoints for any signs of recurrence.
- **Business Continuity:** Restore any required business functionality via official, approved channels only.

3.6 Phase 6: Post-Incident Activities (Lessons Learned)

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem with IT, SOC, and compliance teams.
- **Final Incident Report:** Document the incident scope, timeline, and lessons learned.
- **Action Plan:** Train staff on the risks of shadow IT, enforce acceptable use policies, and strengthen endpoint controls and detection capabilities.

4 MITRE ATT&CK Framework Mapping

Shadow IT / Suspicious Software Installation ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1566 – Phishing*
  - *T1195 – Supply Chain Compromise*
  - *T1078 – Valid Accounts*
- **Tactic: Execution**
  - *T1204 – User Execution*
  - *T1059 – Command and Scripting Interpreter*
- **Tactic: Persistence**
  - *T1547 – Boot or Logon Autostart Execution*
  - *T1505 – Server Software Component*
- **Tactic: Defense Evasion**
  - *T1027 – Obfuscated Files or Information*
  - *T1562 – Impair Defenses*
- **Tactic: Impact**
  - *T1499 – Endpoint Denial of Service*
  - *T1486 – Data Encrypted for Impact*