Purpose

To detect, investigate, and respond to potential unauthorized access or abuse of IP-based KVM (Keyboard, Video, Mouse over IP) devices, which may be exploited for remote access to critical systems outside standard monitoring paths.

Runbook Overview

IP KVMs provide out-of-band access to servers and infrastructure, often bypassing operating system-level controls and logging. This runbook outlines the detection triggers, investigation steps, and containment guidance for suspicious or unauthorized access to IP KVM devices.

Triggers

|  |  |  |
| --- | --- | --- |
| Trigger Name | Trigger Condition | Source |
| Unusual IP KVM Login Attempt | IP KVM access attempted from unexpected IP, geolocation, or outside business hours | Firewall/NetFlow  SIEM Logs  Syslog, IDS/IPS |
| Multiple Failed Login Attempts | Repeated login failures indicating possible brute force attempts | Firewall/NetFlow  SIEM Logs  Syslog, IDS/IPS |
| Login Without Change or System Activity | Login recorded but no expected device or server interaction followed | Firewall/NetFlow  SIEM Logs  Syslog, IDS/IPS |
| Device Beaconing or Outbound Connections | IP KVM device initiating unusual outbound traffic | Firewall/NetFlow  SIEM Logs  Syslog, IDS/IPS |

Prerequisites

| Tools | Access and Permissions | Relevant Knowledge |
| --- | --- | --- |
| **SIEM & Cloud Monitoring**: Google SecOps (Chronicle SIEM) | Access to Telemetry data |  |
| **EDR**: CrowdStrike Falcon | RTR Access to Endpoint host |  |
| Firewall logs or packet capture (PCAP) | Read access to network logs |  |
| **Forensic and Log Collection**: KAPE (Kroll Artifact Parser and Extractor), Axiom Cyber (Magnet Forensics) | Read access to Syslog/Netflow collector |  |

Escalation Point

|  |  |  |
| --- | --- | --- |
| Escalated From | Escalation Point | Escalation Condition |
| Contractor | CSIRT | When confirmed unauthorized KVM access or configuration tampering is detected |
| CSIRT | CSIM | If multiple IP KVMs or related infrastructure are compromised or exposed externally |

Investigation Steps

**Validate Trigger**

* Confirm alert fidelity and timestamp accuracy.
* Correlate login or access logs with known authorized access patterns.

**Identify Affected Device and Scope**

* Determine the specific IP KVM, hostname, and serial number.
* Correlate associated downstream systems or servers connected to the KVM.

**Review Access Logs**

* Pull 24–48 hours of access history from the KVM.
* Identify anomalous users, IPs, or connection timestamps.

**Assess Device Exposure**

* Check if KVM device has public IP or is reachable over VPN/remote networks.
* Validate firewall rules and segmentation policies.

**Containment Decision**

* If active unauthorized session exists, disconnect or disable the interface.
* If suspected compromise without active use, proceed to credential rotation.

**Execute Containment**

* Lock out suspicious accounts or reset KVM passwords.
* Disable unused interfaces (e.g., SSH, web console).
* Block access from suspicious IPs at firewall level.

**Eradication and Recovery**

* Reimage or reset IP KVM firmware to trusted baseline.
* Audit and update firmware versions across all IP KVMs.
* Enforce MFA or jump server-only access where applicable.

**Post-Incident Actions**

* Review asset inventory to identify similar vulnerable devices.
* Implement additional logging (e.g., syslog export from KVM).
* Write detections in SIEM for unusual IP KVM login patterns.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Description of Change** |
| 07-22-25 | 1.0 | Ray Ferrufino | Initial Version |