Play with Kansa on your end. <https://github.com/davehull/Kansa>

Training <https://trustedsignal.blogspot.com/search/label/Kansa>

Additional reading here!

<https://www.powershellmagazine.com/2014/07/18/kansa-a-powershell-based-incident-response-framework/>

Use winrmquickconfig which needs to be enabled.

**🧪 Kansa Challenge Lab & Applied Incident Response Management**

(Real-world IR with insider threats, web misuse, and deception campaigns)

**🔍 What is the Kansa Challenge Lab?**

**Kansa** is a **PowerShell-based incident response framework**.

It collects logs and data from Windows machines for analysis.

**💡 Why Use It?**

* Fast and scalable
* Lightweight (runs with just PowerShell)
* Used in **real-world investigations** (insider threats, malware, unauthorized use)

**🚨 Applied Incident Response Management Scenarios**

Here’s a breakdown of the **types of incidents** you might face, and how to handle them:

**1. 🕵️‍♂️ Espionage**

**Goal:** Stealing sensitive/confidential data (gov, corporate, IP theft)

**Clues:**

* Unusual large file transfers
* Off-hour activity
* Encrypted data going out

**Response:**

* Identify compromised accounts/devices
* Isolate machines
* Analyze logs and exfiltration path
* Involve legal and exec team

**2. 🎭 Active Deception Campaign**

**Goal:** Confuse defenders, plant false flags, or trigger false alerts

**Clues:**

* Random logs or traffic that seem fake
* Fake malware or usernames
* Overwhelming noisy alerts (to hide real attacks)

**Response:**

* Use behavioral analytics (e.g., **Darktrace**)
* Correlate with trusted threat intel
* Identify true anomalies from decoys

**3. 🔓 Unauthorized Use**

**Goal:** Employee using corporate systems for personal or restricted actions

**Examples:**

* Using company device for crypto mining
* Running unauthorized programs/scripts
* Excessive browsing or downloads

**Detection:**

* Use **web proxy logs**, **endpoint monitoring**
* Monitor with tools like **ObserveIT** (screenshots, keystrokes)

**Response:**

* Talk to HR/legal if policy violation
* Alert and educate user
* Lock or restrict access if repeated

**4. 🚫 Inappropriate Web Access**

(e.g., Sexually explicit content)

**Goal:** Employees accessing NSFW content during work

**Clues:**

* Web proxy logs showing repeated NSFW sites
* High data consumption to video sites
* DNS lookups to blocked content

**Response:**

* Filter such sites via **web proxy/firewall**
* Alert HR
* Track repeat offenders (ObserveIT, proxy logs)

**5. 🌐 Web Proxies**

**Purpose:**

* Provide logs for all HTTP/HTTPS traffic
* Used for blocking/filtering/monitoring

**What to Look For:**

* Access to known malware domains
* Unusual spike in traffic
* Circumvention via VPN/proxy sites

**6. 👤 Insider Threats**

**Most dangerous threat — comes from employees or contractors**

**Clues:**

* Data copied to USB
* Sending company files to Gmail/Dropbox
* Unusual printing/email behavior

**Detection Tools:**

* **ObserveIT**: Tracks screen, keystrokes, file transfer
* **Darktrace**: AI-based detection of abnormal behavior
* DLP (Data Loss Prevention): Prevents data from leaving systems

**🔁 Applied Incident Handling Process (in these cases)**

| **Step** | **What to Do** |
| --- | --- |
| 1️⃣ **Detection** | Alert via proxy logs, DLP, ObserveIT, EDR |
| 2️⃣ **Triage** | Confirm it’s real (not false positive), assess risk |
| 3️⃣ **Containment** | Block user/device/network access if harmful |
| 4️⃣ **Investigation** | Gather logs, screenshots, timelines (Kansa, ObserveIT, SCCM) |
| 5️⃣ **Eradication** | Remove malware, change passwords, apply patches |
| 6️⃣ **Recovery** | Restore services, monitor closely |
| 7️⃣ **Lessons Learned** | Improve rules, awareness, controls |
| 8️⃣ **Documentation** | Save logs, actions, timeline for legal/reporting |

**🧰 Tools Mentioned**

| **Tool** | **Purpose** |
| --- | --- |
| **Kansa** | PowerShell-based data collection for IR |
| **ObserveIT** | Insider threat tracking (screens, keystrokes, apps) |
| **Darktrace** | AI-based anomaly detection for networks/users |
| **Web Proxy Logs** | Monitor websites visited, flag misuse |
| **DNS Logs** | Reveal suspicious domains |
| **SCCM** | Manage and monitor Windows systems |
| **WMIC** | Command line tool to pull system data |

**🧠 Key Takeaways**

* Even **non-technical misuse** (e.g. adult content) can be a **security risk**.
* **Insider threats** are **hard to detect** and **easy to overlook**.
* Behavioral detection tools (like ObserveIT & Darktrace) are becoming essential.
* Every incident is an opportunity to learn, improve controls, and update policies.