SOC Playbook — Home Lab

Runbooks for detection, response and auditing

Focused on Splunk, Linux, UFW, Threat Intel and automation.

1. SSH Brute Force → Detection & Auto-ban

Goal: quickly block IPs that keep failing SSH authentication.

Steps

1. Ingest `auth.log/linux_secure` into Splunk.
2. Detect SSH failures with regex extracting `src_ip`.
3. Use `streamstats` to count failures within a 1-minute window.
4. Send suspicious IPs to `ips_a_banir.csv` via `outputlookup`.
5. Run `ban_ip.sh` periodically to enforce UFW rules.

Result: aggressive IPs are automatically blocked at the firewall, with a full history stored in `banned_history.csv` and events logged through `logger -t BAN_SCRIPT`.

2. Threat Intel Match → Prioritized Investigation

Goal: prioritize investigations when a banned IP is also present in threat feeds.

Procedure

1. Regularly refresh `threatintel_by_ip.csv` with external feeds.
2. Correlate banned IPs with this lookup via the “IPs matching Threat Intel” panel.
3. Flag IPs with `score >= 70` as high priority.
4. Check:
   - Geo (country / city).
   - Feed description (C&C, scanner, botnet, etc.).
   - Activity history across SSH / HTTP / MySQL logs.
5. Document the incident in the Casebook and, if needed, add extra rules (e.g. CIDR blocks).

3. 24h / 15d / 30d Audits

Goal: keep the home SOC healthy and effective over time.

Quick Audit (24h)

- Check Splunk health (errors/warnings panels).
- Review latest banned IPs and SSH failures volume.
- Verify that main dashboards show fresh data.

15-day Audit

- Volume of `splunkd` and `mysql_error_log` errors.
- Top sourcetypes and data growth.
- Validate inputs (any host stopped sending logs?).

30-day Audit

- Trend analysis (more attacks? more SSH failures?).
- Review firewall/UFW rules (too many IPs? ranges?).
- Adjust thresholds, SPL and dashboards as required.

4. Manual Ban API & Control Panel

Emergency playbook for manually banning IPs through a protected REST endpoint (Flask or HTTP script), triggered from a Splunk panel or an external tool. Includes:

- Validated IP input (IPv4/IPv6 regex).
- Confirmation before applying UFW rules.
- Logging into `banned_history.csv` with type `manual`.
- Optional: Email / Telegram / Discord notifications.

This Playbook complements the Casebook (concrete cases) and the Portfolio Book (overall project view).