SOC Playbook — Laboratório Pessoal

Runbooks para detecção, reação e auditoria

Focado em Splunk, Linux, UFW, Threat Intel e automação.

1. Brute Force SSH → Deteção & Auto-ban

Objetivo: bloquear rapidamente IPs que insistem em autenticação SSH falhada.

Passos

1. Ingestão dos logs `auth.log/linux_secure` no Splunk.
2. Deteção de falhas SSH com regex para extrair o `src_ip`.
3. Uso de `streamstats` para contar falhas num intervalo de 1 minuto.
4. Envio dos IPs suspeitos para o lookup `ips_a_banir.csv` via `outputlookup`.
5. Execução periódica do script `ban_ip.sh` para aplicar regras de UFW.

Resultado: IPs agressivos são automaticamente banidos na firewall, com histórico registado em `banned_history.csv` e event logging via `logger -t BAN_SCRIPT`.

2. Threat Intel Match → Investigação Rápida

Objetivo: priorizar investigação quando um IP banido também figura em feeds de ameaça.

Procedimento

1. Atualizar periodicamente o lookup `threatintel_by_ip.csv` com feeds externos.
2. Correlação dos IPs banidos com esse lookup usando o painel "IPs coincidentes com Threat Intel".
3. Marcar IPs com `score >= 70` como de alta prioridade.
4. Verificar:
   - Geolocalização (pais/cidade).
   - Descrição do feed (C&C, scanner, botnet, etc.).
   - Histórico de atividades nos logs (SSH, HTTP, MySQL).
5. Documentar o incidente no Casebook e, se necessário, criar regras adicionais (e.g. bloquear range CIDR).

3. Auditoria 24h / 15d / 30d

Objetivo: garantir que o SOC caseiro continua saudável e eficaz ao longo do tempo.

Auditoria Rápida (24h)

- Verificar painel de saúde do Splunk (erros/warnings).
- Rever últimos IPs banidos e volume de falhas SSH.
- Validar se os painéis principais estão a devolver dados recentes.

Auditoria 15 dias

- Volume de erros em `splunkd` e `mysql_error_log`.
- Top sourcetypes e crescimento de dados.
- Validação dos inputs (se algum host deixou de enviar logs).

Auditoria 30 dias

- Análise de tendências (mais ataques? mais falhas SSH?).
- Revisão das regras de firewall/UFW (muitos IPs? ranges?).
- Ajustar limiares de alertas, SPLs e dashboards conforme necessário.

4. Manual Ban API & Painel de Controlo

Playbook de emergência para banir IPs manualmente através de um endpoint REST (Flask ou script HTTP) protegido, disparado a partir de um painel no Splunk ou de uma ferramenta externa. Inclui:

- Input validado de IP (regex IPv4 / IPv6).
- Confirmação antes de aplicar UFW.
- Registo no `banned_history.csv` com tipo `manual`.
- Opcional: notificação por email/Telegram/Discord.

Este Playbook complementa o Casebook (casos concretos) e o Portfolio Book (visão geral do projeto).