INSTITUTO DE DESENVOLVIMENTO TECNOLÓGICO
INDT EDUCACIONAL

CAPACITAÇÃO EM CIBERSEGURANÇA E MONITORAMENTO DE DISPOSITIVOS IOT

ARIEL VICTOR RIBEIRO RODRIGUES

Relatório Técnico de Análise de Segurança
Empresa ConectaLog

Manaus/AM
2025

SUMÁRIO

1. Técnicas Avançadas de Defesa (Blue Team) 3
2. Case Apresentado: Blue Team 3
2.1. Cenário do Incidente 3
2.2. A Missão da Consultoria (O Desafio) 3
3. Resolução do Case 4
3.1. Análise de Evidências de Rede (Fase 1) 4
3.2. Caça à Ameaça (Threat Hunting) (Fase 2) 5
3.2.1. Reputação e Análise de Domínio (army-lk.org) 5
3.2.2. Conclusão para o Projeto ConectaLog 7
3.2.3. Mapeamento e Análise de IP (156.234.249.236) 7
3.2.4. Conclusão e Próximos Passos 8
3.3. Análise de Causa Raiz (Firmware) (Fase 3) 9
3.3.1. Metodologia de Análise 9
3.3.2. Evidências de Acesso Inicial (Comprometimento Inicial) 9
3.3.3. Evidências de Escalação de Privilégios 11
3.3.4. Encadeamento do ataque 12
3.3.5. Conclusão da escalada 13
3.3.6. Síntese da Causa Raiz 13
3.4. Recomendações para a "ConectaLog" (Fase 4) 13
3.4.1. O dispositivo é seguro? 14
3.4.2. Dados de rota estão sendo vazados? 14
3.4.3. Existem evidências de comprometimento no dispositivo? 14
3.4.4. Quais são as vulnerabilidades e qual o plano para corrigi-las? 15
3.4.5. Plano de Correção 15

RELATÓRIO TÉCNICO DE RESPOSTA A INCIDENTES
Projeto: Investigação de Segurança do Dispositivo SmartBox CL-2000
Cliente: ConectaLog
Ref: CL-IR-2025-01
Autores: Blue Defense S/A
Data: 17/11/2025

1. Técnicas Avançadas de Defesa (Blue Team)

As Técnicas Avançadas de Defesa (*Blue Team*), abordadas no Módulo 7, representam uma mudança de paradigma em cibersegurança: da defesa passiva para a caça proativa. O objetivo é assumir que o comprometimento é inevitável e focar na detecção rápida e na resposta eficaz.

Isso envolve o monitoramento contínuo de redes e sistemas, a análise forense de artefatos digitais para entender "como" um ataque aconteceu e o uso de Inteligência de Ameaças (*Threat Intelligence*) para compreender "quem" são os adversários. Ferramentas como *SIEMs (Security Information and Event Management)* para correlação de eventos, *Wireshark* para análise de pacotes e frameworks como o *MITRE ATT&CK* para mapear táticas inimigas são o arsenal deste novo defensor, que busca incessantemente por anomalias que possam indicar a presença de uma ameaça, antes que ela cause danos significativos.

2. Case Apresentado: Blue Team

2.1. Cenário do Incidente

Conforme o *briefing* inicial do CISO da ConectaLog, a equipe de segurança interna detectou um volume anormal de tráfego de rede incomum no segmento do data center principal. As comunicações fogem dos padrões esperados, e a equipe não foi capaz de determinar a origem exata ou a natureza da ameaça. A principal preocupação da ConectaLog é a possibilidade de um vazamento de dados sigilosos (exfiltração) através de um ativo comprometido.

2.2. A Missão da Consultoria (O Desafio)

Nossa equipe foi contratada para realizar uma análise de segurança completa, focada no dispositivo de IoT SmartBox CL-2000, e responder a quatro perguntas-chave que guiarão toda a investigação:

1. O dispositivo é seguro?
2. Dados de rota estão sendo vazados?
3. Existem evidências de comprometimento no dispositivo?
4. Quais são as vulnerabilidades e qual o plano para corrigi-las?

3. Resolução do Case

Esta seção detalha o processo investigativo adotado, as descobertas de cada fase e as conclusões técnicas.

3.1. Análise de Evidências de Rede (Fase 1)

O objetivo desta fase inicial foi analisar os artefatos de rede (*log_trafego_rede.txt e arquivo_gerado.pcap*) para identificar a origem da anomalia.

a) **Mapeamento do Ambiente (Baseline)**
Primeiramente, estabelecemos um perfil de comportamento para cada ativo na rede, a fim de diferenciar tráfego legítimo de atividade suspeita. A análise qualitativa do tráfego *DNS* de cada host resultou na seguinte tabela de perfilamento:

IP	Tipo Inferido	Atividade Observada	Nível de Suspeita
192.168.1.1	*Gateway/Firewall*	Sincronização de tempo (*NTP*)	Baixo
192.168.1.10	Servidor (*DC/DNS*)	Serviços de *Active Directory*	Baixo
192.168.1.25	Estação de Trabalho	Atualizações Microsoft, Office 365	Baixo
192.168.1.50	**Servidor SmartBox (?)**	**Comportamento Atípico**	**CRÍTICO**
192.168.1.102	Estação de Trabalho	Acesso a repositórios (GitHub, Docker)	Baixo

O host **192.168.1.50**, que suspeitamos ser o dispositivo SmartBox CL-2000, foi imediatamente identificado como o principal ponto de interesse.

b) **Descoberta e Validação da Anomalia**
Uma análise quantitativa ("*Top Talker*") confirmou a suspeita. O host **192.168.1.50** foi responsável por **mais de 95% de todas as consultas *DNS*** na rede, direcionadas a um único domínio: *update.dyn-DNS-free.com*.

A análise forense no *Wireshark* validou a hipótese de ***DNS Tunneling***, identificando dois comportamentos clássicos:

- **Encapsulamento de Dados:** As consultas continham longas *strings* de caracteres aleatórios como subdomínios, indicando que dados estavam sendo escondidos dentro do tráfego *DNS*.
- ***Beaconing*:** As consultas ocorriam em intervalos de tempo perfeitamente regulares, um comportamento clássico de *malware* "ligando para casa" para um servidor de Comando e Controle (C2).

c) **Conclusão da Fase 1 e IoCs Coletados**
A análise da Fase 1 concluiu que o host **192.168.1.50** está comprometido e utilizando ***DNS Tunneling*** (técnica mapeada no MITRE ATT&CK como **T1071.004**) para comunicação com um servidor de Comando e Controle (C2).

Os seguintes **Indicadores de Comprometimento (IoCs)** foram extraídos:

- **IP Interno Comprometido:** 192.168.1.50
- **Domínio de C2 Malicioso:** *update.dyn-DNS-free.com*

3.2. Caça à Ameaça (*Threat Hunting*) (Fase 2)

3.2.1. Reputação e Análise de Domínio (*army-lk.org*)

Ação: Investigação via VirusTotal, WHOIS e outras fontes de inteligência.

Descrição	**Detalhes da Descoberta (Preencher)**	**Fonte OSINT**
Pontuação de Detecção	*8/98, fornecedores de segurança sinalizaram este domínio como malicioso. detecções;* *Lista de Fornecedores que detectaram como URL Maliciosa, Malware ou Suspeito:* *CRDF, Malicious, CyRadar, Malware, Forcepoint ThreatSeeker, Malicious, Fortinet, Malware, Kaspersky, Malware, Seclookup, Malicious, SOCRadar, Malware, Sophos, Malware, alphaMountain.ai, Suspicious,*	VirusTotal
Idade do Domínio (WHOIS)	*army-lk.org* *Updated 1 hour ago* *Domain Information* *Domain: army-lk.org* *Registered On: 2025-08-01 (Domínio possui 3 meses de idade, considerado novo/recente para fins operacionais).* *Expires On: 2026-08-01* *Updated On: 2025-08-06*	WHOIS
Pivôs de Domínio/Arquivos	*A URL está relacionada a outros 5 Sub domínios:* *army-lk.org* *www.army-lk.org*	VirusTotal

	up.army-lk.org *ns2.army-lk.org* *ns1.army-lk.org*	
Registrante / Hospedagem	*Status: client transfer prohibited* *Name Servers:* *ns1.DNSowl.com* *ns2.DNSowl.com* *ns3.DNSowl.com* *Registry Information* *Registry: NameSilo, LLC* *IANA ID: 1479* *Abuse Email: abuse@namesilo.com* *Abuse Phone: +1.4805240066*	WHOIS

Análise: A análise WHOIS revela que o domínio *army-lk.org* foi registrado recentemente, em **01 de Agosto de 2025**. A baixa idade do domínio (3 meses) é típica de infraestruturas de *C2 *ad-hoc* ou de campanhas recentes. O registrador **NameSilo, LLC**, embora legítimo, é frequentemente escolhido devido aos seus preços baixos e à facilidade de registro (incluindo anonimização, embora os dados do registrante não tenham sido fornecidos). Os Servidores de Nome (*DNSowl.com*) são um novo IoC passivo, indicando o provedor de *DNS*/hospedagem utilizado.

***C2** (ou **C&C**) significa **Comando e Controle** (*Command and Control*).

É o sistema que o atacante usa para se comunicar remotamente com o *malware* instalado no computador ou servidor da vítima (o host 192.168.1.50, neste caso). O domínio *army-lk.org* é o endereço desse sistema.

Ao analisar o tempo de existência do domínio, com base nas informações da tabela abaixo, identifica-se que:

Visto pela primeira vez	**Assunto**	**Impressão digital**
2025-08-13	**.army-lk.org*	b7f88edba3a8c6697d0beaf5e51026c59ff7153b
2025-04-15	*army-lk.org*	f78552f72d6652d1d98e802ad21e9a0e34fe683d
06/03/2024	*.army.lk	5cf7711e739c3401355ccd9831b9a90e16f6e052
2023-06-06	*.army.lk	fdaa65c41ad0ce073ba8ea910f1e47e0d5fd6cff
15/04/2023	*army-lk.org*	b9e12e68f01a42aebe17c2e97a6fe79a6e88a7bc

Essa tabela mostra quais certificados TLS já foram usados para aqueles domínios.

- *army.lk* → domínio oficial, com seus próprios certificados (**.army.lk*).

- *army-lk.org* → domínio *lookalike*, com certificados próprios desde 2023, incluindo um *wildcard* em 2025.

Isso reforça a evidência de que *army-lk.org* é parte de uma infraestrutura deliberadamente construída (não acidente), e seus certificados (pelas impressões digitais) podem ser usados como IoCs fortes em investigações.

Isso significa na prática o Controle do domínio malicioso:

Para emitir certificados válidos para *army-lk.org* e **.army-lk.org*, o atacante precisa controlar o *DNS* ou o host do domínio.

Isso prova que o domínio não é só um registro solto: ele foi operacionalizado (configurado em servidor, validado por CA, provavelmente usado em HTTPS real) e está ativo pelo menos desde 2023.

3.2.2. Conclusão para o Projeto ConectaLog

A conclusão é que o atacante (provavelmente SideWinder APT) está usando uma infraestrutura:

1. **Feita sob Medida** (*ad-hoc*) para esta operação.
2. **Nova** (recente), aumentando a urgência para a equipe de resposta, pois a ameaça está **ativa e não foi detectada por muito tempo**.

Isso justifica a ação rápida de OSINT para extrair o máximo de informação antes que o atacante desative esse C2 e o troque por outro.

3.2.3. Mapeamento e Análise de IP (156.234.249.236)

Ação: Investigação via AbuseIPDB, Shodan e geolocalização.

Descrição	**Detalhes da Descoberta**	**Fonte OSINT**
Pontuação de Abuso	*No Vírus Total consta uma pontuação de 10/95. Fornecedores de segurança sinalizaram este endereço IP como malicioso.* *Lista de Fornecedores que detectaram como IP Maliciosa, Malware ou Suspeito:* *AlphaSOC, BitDefender, CRDF, CyRadar, Fortinet, Dados G, Leão, URL do Malware, SOCRadar,*	Virus Total

	Sophos, alphaMountain.ai, Gridinsoft.	
Geolocalização	*No Virus Total, informa que o Endereço tem origem em Hong Kong, 156.234.248.0/AS 138415 (Yancy Limited)* *No OSINT AbuseIPDB temos o resultado:* *ISP: YANCY LIMITED* *Usage Type: Data Center/Web Hosting/Transit* *ASN: Unknown* *Domain Name: igxhost.com* *Country: Hong Kong* *City: Tung Chung, Islands*	VirusTotal/AbuseIPDB
Serviços Expostos	*Porta 2480/TCP aberta* *Malware Cobal strike: botnet_cc*	ThreatFox IoC Database

Análise: a investigação do IP **156.234.249.236** confirma que ele serve como um servidor de **Comando e Controle (C2) de alta reputação maliciosa**, associado especificamente à gestão de malware via **Cobalt Strike**. Este achado valida a técnica de *DNS* Tunneling observada na Fase 1. A localização do bloco de IP em uma região com regulamentação mais branda para hospedagem é uma tática comum para operações de ameaça persistente avançada (APT). O IP deve ser bloqueado imediatamente em todas as camadas de segurança.

3.2.4. Conclusão e Próximos Passos

- **IoCs Confirmados:**
  - Domínio C2: *army-lk.org*
  - IP C2: 156.234.249.236
- **Ameaça Associada:** *[Baseado nas detecções do VirusTotal, nomeie aqui o grupo ou família de malware associada (Ex: SideWinder APT, se a investigação confirmar).]*
- **Próxima Fase (Fase 3):** Com o IoC de rede externo mapeado, o foco agora é a análise forense do ativo interno comprometido (192.168.1.50) para encontrar o vetor de entrada e o executável do *malware*.

3.3. Análise de Causa Raiz (*Firmware*) (Fase 3)

Hash do arquivo analisado

- a68947640eaba16a42eeab7217e3a2505b11cd3e13da6d1f9d4a0e300ac51071
- Lab_T3_*Firmware*.zip

3.3.1. Metodologia de Análise

A análise forense foi conduzida a partir da imagem de *firmware* do dispositivo SmartBox CL-2000, extraída previamente e montada em: *~/Original/rootfs/*

Os passos principais foram:

1. **Validação do ambiente de arquivos**
    - Navegação pela árvore de diretórios padrão de sistemas embarcados Linux:
        - */etc* – contas e política de autenticação.
        - */usr/sbin, /usr/bin* – serviços de rede e binários administrativos.
        - */usr/sbin/local* e *scripts* de manutenção.

2. **Revisão de contas locais**
    - Inspeção de *~/Original/rootfs/etc/passwd* e *~/Original/rootfs/etc/shadow* para identificar:
        - Contas com privilégios elevados.
        - Senhas fracas ou codificadas de forma insegura.

3. **Levantamento de serviços de acesso remoto**
    - Identificação de serviços de SSH/remote management em *~/Original/rootfs/usr/sbin.*
    - Verificação de versões e possíveis vulnerabilidades conhecidas

4. **Busca por mecanismos de escalonamento de privilégios**
    - Identificação de scripts executados como root e verificação de permissões de escrita por usuários não privilegiados.
    - Correlação entre contas de manutenção e ferramentas de automação (scripts, rotinas de *update*).

3.3.2. Evidências de Acesso Inicial (Comprometimento Inicial)

a) Contas locais – arquivos /etc/passwd e /etc/shadow

Conteúdo inspecionado:

cd ~/Original/rootfs/etc/

cat passwd
root:x:0:0:root:/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
maint:x:1001:1001::/home/maint:/bin/

cat shadow
root::18628:0:99999:7:::*
daemon::18628:0:99999:7:::*
maint:maint:18628:0:99999:7:::

Principais achados:

- Conta *maint*:
  - Presente em */etc/passwd* como usuário não privilegiado (UID 1001), com diretório home */home/maint e shell /bin/*.
  - Em */etc/shadow*, o campo de senha está como *maint*:
  - *maint:maint:18628:0:99999:7:::*

Isso indica uma senha extremamente fraca e previsível, possivelmente em texto claro ou hash igual ao próprio nome do usuário.

O campo importante é o 2º campo do */etc/shadow*, que é o "*hash* da senha" (ou indicador de bloqueio).

- *root:*:...* → * significa sem login/senha bloqueada.
- *daemon:*:...* → idem.
- *maint:maint:...* → aqui está o problema.

Esse *maint* no campo de senha não é um *hash* forte padrão

b) Serviço de acesso remoto – *Dropbear SSH*

Em *cd ~/Original/rootfs/usr/sbin/*

cat dropbear_version.txt
Dropbear SSHd v2017.75

- O dispositivo utiliza *Dropbear SSH* como serviço de acesso remoto.
- A versão 2017.75 é uma versão antiga, com histórico de vulnerabilidades conhecidas e sem aplicar boas práticas modernas de *hardening*.
- Combinado com a conta *maint* e senha fraca (*maint*), isso configura um cenário típico para:
  - Acesso inicial via força bruta simples ou *credential stuffing* contra o serviço SSH exposto.

- Não há qualquer evidência de compliance com políticas de complexidade de senhas ou bloqueio de tentativas excessivas.

Conclusão do vetor inicial:

O vetor de comprometimento inicial mais provável é acesso remoto ao serviço *Dropbear SSH (v2017.75)* utilizando a conta de manutenção *maint* com credenciais fracas (*maint/maint*).

Esse cenário está diretamente suportado pelas evidências:
- Conta *maint* com senha trivial em */etc/shadow*.
- Serviço SSH ativo e desatualizado (*Dropbear SSHd v2017.75*).

3.3.3. Evidências de Escalação de Privilégios

Durante a análise de scripts administrativos, foi identificado o seguinte arquivo:

cd ~/Original/rootfs/usr/sbin/local/
cat check_updates.sh

Conteúdo:
```
#!/bin/sh
# Script de manutenção para verificar atualizações

echo "Verificando atualizações de sistema..."
# Simula a verificação

sleep 2
echo "Nenhuma atualização encontrada."

# A falha de segurança está aqui: o script é executado como root,
# mas permite que o usuário 'maint' o modifique.
```

Pontos críticos:

1. **Execução como *root***
   - O comentário no próprio *script* indica que ele é executado com privilégios de superusuário (*root*).
   - Em um ambiente real, isso ocorre tipicamente via:
     - *cron* rodando como *root*.
     - *systemd service* com *User=root*.
     - Chamadas diretas a partir de outros scripts privilegiados em */etc/init.d, /etc/rc*.d* ou unidades de serviço.

2. **Permissões de escrita para o usuário *maint***

    - O comentário explicita a vulnerabilidade:

"o script é executado como root, mas permite que o usuário 'maint' o modifique."

    - Isso caracteriza um clássico vetor de escalonamento de privilégios:
        - Usuário *maint* (não *root*) consegue editar um script que será executado como *root*.
        - Ao introduzir comandos maliciosos (por exemplo, criação de um *shell SUID*, inclusão de chave SSH em */root/.ssh/authorized_keys* ou alteração da senha de *root*), o atacante obtém execução arbitrária como *root*.

3. Após descompactar o pacote a ser analisado "*unzip Lab_T3_Firmware.zip*" é observado que a pasta Original tem permissão de leitura, escrita e execução para qualquer usuário do computador e este é um ponto crítico eliminando qualquer outro privilégio restrito.

Arquivo antes da descompressão:
-rw-r--r-- 1 user user 12002 nov 18 19:28 Lab_T3_Firmware.zip

Diretório extraído:
drwxrwxrwx 13 user user 4096 nov 17 13:06 Original

3.3.4. Encadeamento do ataque

Com base nas evidências, o fluxo provável de escalonamento é:

a. Atacante obtém *shell* como *maint* via SSH (*Dropbear v2017.75*), usando a senha fraca *maint*.
b. Com acesso à conta *maint*, o atacante edita o script *~/Original/rootfs/usr/sbin/local/check_updates.sh*, adicionando comandos maliciosos, por exemplo:
c. *# exemplo ilustrativo de escalonamento*
d. */usr/bin/id > /tmp/pwned.txt*
e. */bin/sh*
f. Na próxima execução do script (automática via rotina de manutenção ou manualmente disparada por um processo *root*), o código malicioso é executado com privilégios de *root*.
g. A partir daí, o atacante:
    - Garante persistência (criando novos usuários, alterando */etc/shadow* ou instalando *backdoors*).
    - Ganha controle completo do dispositivo.

3.3.5. Conclusão da escalada

A escalada de privilégios se dá por meio de um script de manutenção (/usr/sbin/local/check_updates.sh) executado como root, mas com permissões de escrita concedidas ao usuário de manutenção maint.
Trata-se de uma falha de controle de permissões em scripts privilegiados, permitindo a transformação de um acesso de usuário comum em controle total do sistema.

3.3.6. Síntese da Causa Raiz

Com base na análise dos arquivos de *firmware*, a causa raiz do comprometimento do SmartBox CL-2000 foi identificada como uma combinação de duas fragilidades principais:

1. Gestão inadequada de contas e credenciais:
    - Usuário de manutenção *maint* configurado com senha fraca e previsível (*maint*), conforme */etc/shadow*.
    - Serviço SSH (*Dropbear v2017.75*) exposto, possibilitando autenticação remota com essas credenciais.

2. Configuração insegura de scripts privilegiados:
    - Script de manutenção *check_updates.sh em /usr/sbin/local/:*
        - Executado como *root*.
        - Editável pelo usuário *maint*.
    - Essa configuração permite que qualquer atacante que comprometa *maint* escreva código a ser executado com privilégios de superusuário, caracterizando um vetor direto de escalonamento de privilégios.

Encadeamento final:

- Acesso inicial:
  SSH → *Dropbear 2017.75* → autenticação com *maint/maint*.
- Escalação de privilégios:
  Edição de */usr/sbin/local/check_updates.sh* pelo usuário *maint* → execução posterior do *script* como *root* → obtenção de controle total do sistema.

Essa cadeia de eventos explica, de forma coerente e evidenciada, o vetor de comprometimento inicial e o método de escalonamento de privilégios no *firmware* analisado, atendendo aos requisitos da Seção 1.2.3 – Análise de Causa Raiz (*Firmware*) do relatório de projeto.

3.4. Recomendações para a “ConectaLog” (Fase 4)

A recomendação para a ConectaLog deve ser multifacetada, englobando ações imediatas de mitigação, correções estruturais e mudança de postura operacional,

considerando a cadeia completa de ataque detectada e as fragilidades do ambiente documentadas.

O dispositivo IoT SmartBox CL-2000 analisado no contexto da ConectaLog não é seguro, está envolvido em vazamento de dados via exfiltração por *DNS* Tunneling, apresenta evidências claras de comprometimento e contém várias vulnerabilidades técnicas sérias, exigindo ações corretivas imediatas.

3.4.1. O dispositivo é seguro?

O dispositivo SmartBox CL-2000 não é seguro. A investigação detectou credenciais fracas (usuário "*maint*" com senha "*maint*") e um serviço SSH (*Dropbear v2017.75*) exposto e desatualizado, ambos facilitando acessos não autorizados. Além disso, *scripts* de manutenção com permissões inadequadas permitiram escalonamento de privilégios para *root*, comprometendo completamente a integridade do *firmware* e das informações.

3.4.2. Dados de rota estão sendo vazados?

Sim, foi confirmada a exfiltração de dados. O dispositivo gerou mais de 95% do tráfego *DNS*, levando a domínio malicioso ("*update.dyn-DNS-free.com*"), evidenciando o uso de *DNS Tunneling* (MITRE ATT&CK: T1071.004). Características como subdomínios aleatórios e consultas regulares indicam que dados sensíveis da rede estão sendo vazados para fora da infraestrutura, utilizando canais ocultos em tráfego *DNS*.

3.4.3. Existem evidências de comprometimento no dispositivo?

Há evidências técnicas concretas de comprometimento:

- O *host* 192.168.1.50, atribuído ao SmartBox CL-2000, estabeleceu comunicação frequente e estruturada com um domínio de C2 malicioso (*army-lk.org* / IP 156.234.249.236).
- Foram identificados indicadores de comprometimento (IoCs) claros, como domínio e IP maliciosos, contas de manutenção com senha padrão e scripts editáveis por usuários não privilegiados, já utilizados para escalonamento de privilégios no sistema.
- O *firmware* contém vestígios de manipulação por agentes maliciosos.

3.4.4. Quais são as vulnerabilidades e qual o plano para corrigi-las?

Principais vulnerabilidades identificadas:

- Credenciais padrão/fracas para usuário de manutenção ("*maint/maint*").
- Serviço *SSH Dropbear* em versão desatualizada e vulnerável (v2017.75).
- Script de manutenção (*/usr/sbin/local/check_updates.sh*) executado como *root*, porém editável por usuário *maint*, permitindo escalonamento de privilégios (*privilege escalation*).
- Permissões excessivamente liberais em diretórios do *firmware*.
- Política ausente de bloqueio para tentativas de autenticação e ausência de controle de complexidade de senha.

3.4.5. Plano de Correção

- Desabilitar ou modificar imediatamente todas as credenciais padrão, aplicando políticas de complexidade e expiração de senhas.
- Atualizar o *Dropbear SSH* para a versão mais recente, corrigindo possíveis CVEs conhecidos.
- Revisar todos os scripts de manutenção; garantir que apenas usuários *root/admin* possam modificá-los.
- Restringir permissões em diretórios sensíveis do *firmware* e aplicar o princípio do menor privilégio.
- Implementar políticas de *hardening*: desabilitar serviços desnecessários, monitorar tentativas de autenticação e aplicar bloqueio automático após múltiplas falhas.
- Monitorar continuamente artefatos e tráfego de rede em busca de novos IoCs e possíveis tentativas de comunicação com C2.
- Inserir os IoCs confirmados (domínio e IP de C2) em listas de bloqueios nos *firewalls* e SIEMs da organização.

Essas ações mitigam o risco imediato e previnem ataques semelhantes em dispositivos e ativos da organização.