DOCUMENTO DE EXEMPLO · DADOS FICTÍCIOS

Relatório de teste de intrusão contínuo.

O formato de um relatório DIANA — achados validados por exploração, cadeias de ataque, priorização por explorabilidade real e um sumário executivo pronto para a administração.

CLIENTE
ACME Serviços, S.A. (fictício)

PERÍODO
01–30 jun 2026

ÂMBITO
Externo + interno autorizado

SUMÁRIO EXECUTIVO

Para a administração.

Durante junho de 2026, a DIANA avaliou em contínuo a superfície de ataque autorizada da ACME Serviços, S.A. Foram descobertos **1.847 ativos** e validados por exploração controlada **quatro caminhos de ataque** com impacto material — cada um confirmado com evidência e sujeito a aprovação humana antes de qualquer ação sensível.

2	1	1	< 24h
achados críticos	achado elevado	achado médio	descoberta → evidência

Mensagem-chave

Dos milhares de alertas teóricos que um scanner produziria, apenas quatro representam risco *provado* e explorável neste ambiente. A remediação deve começar pelos dois achados críticos — ambos permitem, em cadeia, o acesso a dados de clientes.

> **COMO LER ESTE RELATÓRIO**
>
> Cada achado inclui a cadeia de ataque validada, a evidência técnica, o impacto de negócio, a priorização por explorabilidade e a recomendação de correção. O anexo de aprovações documenta cada ação sensível autorizada por um responsável do cliente.

QUADRO DE ACHADOS

Priorização por explorabilidade.

Ordenado pelo risco real validado no ambiente, não apenas pelo CVSS teórico.

#	ACHADO	SEVERIDADE	IMPACTO VALIDADO
F-01	Credenciais expostas em endpoint de gestão sem MFA	CRÍTICO	Acesso administrativo à aplicação de faturação
F-02	Bucket de armazenamento com listagem pública	CRÍTICO	Exposição de 12.400 registos de clientes (exfiltração provada em âmbito)
F-03	Serviço interno vulnerável a movimento lateral	ELEVADO	Pivô de DMZ para segmento de dados
F-04	Componente desatualizado com CVE conhecido	MÉDIO	Execução remota — não explorável isoladamente neste ambiente

Porque F-04 é «médio» e não «crítico»

O CVE associado a F-04 tem CVSS 9.8. Porém, a validação por exploração mostrou que o componente não está acessível a partir de nenhum caminho autorizado testado e depende de um pré-requisito que não se verifica neste ambiente. O risco *real* é médio — um exemplo de como a explorabilidade corrige a priorização puramente teórica.

F-01 · Credenciais sem MFA CRÍTICO

Cadeia de ataque validada

```
# 1 · Descoberta — endpoint de gestão exposto
mgmt.acme-servicos.example  →  porta 443 (painel de administração)

# 2 · Credenciais reutilizadas encontradas em fuga pública
utilizador: ops-admin   estado MFA: não configurado

# 3 · Autenticação bem-sucedida (aprovação humana solicitada e concedida)
POST /api/session  →  200 OK  sessão administrativa obtida

# 4 · Alcance confirmado — sem alterar dados (ação read-only)
acesso: gestão de faturação, exportação de faturas, dados de clientes
```

Evidência

Sessão administrativa estabelecida às 14:32 de 08 jun 2026. A DIANA parou na confirmação de acesso, sem modificar dados nem escalar privilégios — a ação foi **read-only** e aprovada previamente pelo responsável de segurança da ACME (ver anexo de aprovações, A-07).

Impacto de negócio

Um atacante com estas credenciais obteria controlo da aplicação de faturação e acesso a dados de clientes — com implicações de RGPD e de continuidade do serviço de cobrança.

> **RECOMENDAÇÃO**
>
> Impor MFA em todos os endpoints de gestão (prioridade imediata) · rodar as credenciais expostas · restringir o painel a origens de confiança / VPN · monitorizar autenticações anómalas no SOC.
>
> **REVALIDAÇÃO AGENDADA APÓS CORREÇÃO.**

F-02 · Dados de clientes expostos CRÍTICO

Cadeia de ataque validada

```
# 1 · Descoberta — bucket referenciado no código do site
assets-acme.storage.example  →  listagem pública ativada

# 2 · Enumeração (read-only, dentro do âmbito)
/exports/clientes-2026-05.csv  →  acessível sem autenticação

# 3 · Confirmação de sensibilidade (amostra mínima, não exfiltrada)
cabeçalho: nome, email, NIF, morada  →  ~12.400 registos
```

RECOMENDAÇÃO

Desativar a listagem pública · aplicar política de acesso mínimo · revisão de todos os buckets do inventário · avaliar dever de notificação ao abrigo do RGPD.

F-03 · Movimento lateral ELEVADO

A partir de um serviço na DMZ, a DIANA validou um caminho de pivô para o segmento de dados, contornando a segmentação pretendida. Ação executada com aprovação humana; sem impacto em produção. **Recomendação:** rever regras de segmentação e aplicar o princípio do menor privilégio entre segmentos; reteste após correção.

GOVERNAÇÃO

Trilho de aprovações.

Extrato — cada ação sensível é autorizada por um responsável do cliente antes de executar.

REF.	DATA / HORA	AÇÃO SOLICITADA	DECISÃO	AUTORIZADO POR
A-07	08 jun · 14:30	Autenticar com credenciais expostas (F-01)	APROVADO	CISO ACME
A-08	08 jun · 14:41	Enumerar bucket público (F-02)	APROVADO	CISO ACME
A-09	11 jun · 10:15	Validar pivô entre segmentos (F-03)	APROVADO	Resp. Infra
A-10	11 jun · 10:52	Escalar privilégios em servidor de dados	RECUSADO	Resp. Infra

A-10 ilustra o controlo humano em ação: a ação foi recusada e a DIANA **parou**, registando a decisão. A autonomia da IA opera sempre dentro do que a organização autoriza.

METODOLOGIA

Duas fases: descobrir e provar

Descoberta: mapeamento contínuo da superfície de ataque autorizada (ativos externos e internos). **Exploração:** validação controlada de que uma exposição é *realmente* explorável, com evidência e sob aprovação humana nas ações sensíveis. A priorização usa a explorabilidade observada no ambiente, complementada por modelos públicos de probabilidade de exploração (p. ex. EPSS).

Fundamento: Manadhata & Wing, «An Attack Surface Metric», IEEE TSE 2011 · Jacobs et al., «Exploit Prediction Scoring System (EPSS)», 2019 (arXiv:1908.04856).

O SEU RELATÓRIO, COM OS SEUS DADOS

Este é o formato.
Os achados serão os seus.

Numa demonstração de 30 minutos, mostramos a DIANA a operar num âmbito de exemplo: da descoberta à exploração validada, com aprovação humana e o relatório de evidências gerado na sessão. Empresa portuguesa, dados em Portugal e na UE, alinhada com NIS2 e ISO 27001.

AGENDE A SUA DEMONSTRAÇÃO

diana.red/contactos
hello@cybersec.pt · +351 21 594 4726
Passeio das Ilhas, nº 3, Loja B · 2670-322 Loures