PLATAFORMA CTEM · CYBERSECURITY POSTURE MANAGEMENT

CYBERATLAS

Datasheet Técnico

Attack Surface Management · Threat Intelligence · Maturidade & Compliance

Produto CyberAtlas — Plataforma CTEM

Documento Datasheet Técnico

Especificação funcional das capacidades em produção. Documento de referência para avaliação técnica.

Produto	CyberAtlas — Plataforma de Gestão de Postura de Cibersegurança (CTEM)
Categoria	Attack Surface Management · Threat Intelligence · Cyber Maturity & Compliance
Modelo de entrega	SaaS multi-tenant (B2B), sem instalação de agentes no ambiente do cliente
Interface	Web app responsivo, dark-first, trilíngue (pt-BR · en · es)
Status	Em produção

1. Sumário

CyberAtlas unifica, num único painel, as três frentes que uma organização precisa cobrir para gerir risco cibernético de forma contínua (CTEM — *Continuous Threat Exposure Management*):

1. **Superfície de ataque externa (ASM)** — descoberta e monitoramento contínuo de tudo o que a organização expõe na internet: domínios, subdomínios, serviços, portas, tecnologias e vulnerabilidades.
2. **Inteligência de ameaças & proteção de marca (Threat Intel)** — vazamento de credenciais e dados, monitoramento de deep/dark/surface web, domínios similares (typosquatting), perfis falsos, exposição em fóruns e canais de Telegram, monitoramento de reputação e fluxo de takedown.
3. **Maturidade & conformidade** — avaliações contra os principais frameworks (NIST CSF 2.0, CIS Controls v8, ISO 27001:2022, SOC-CMM v4), com validação de evidências assistida por IA e planos de ação gerados automaticamente.

Tudo é consolidado num fluxo único que transforma sinais em achados, riscos e tarefas priorizadas — alimentando planos de ação, roadmap de remediação, dashboards executivos e integrações com ferramentas de trabalho (Jira/Linear).

2. Características da plataforma

Característica	Descrição
Modelo	SaaS multi-tenant, com isolamento lógico total entre organizações
Coleta	100% *outside-in* — não requer agentes, appliances ou instalação no ambiente do cliente
Interface	A interface web é uma aplicação responsiva e trilíngue, acessada exclusivamente via HTTPS (TLS 1.2+), com todo o tráfego criptografado.
Operação	Monitoramento contínuo automatizado, com alertas em tempo real
Priorização	Riscos ordenados por criticidade real (exposição, explorabilidade e impacto ao negócio)
Exportação	Relatórios executivos em PDF *board-ready* e planilhas (Excel)
Integrações	Jira e Linear (exportação de itens de remediação), notificações por e-mail e push
Segurança de acesso	Autenticação multifator (MFA/TOTP), controle de acesso por papel, trilha de auditoria

Conformidade	Aderente à LGPD; suporte a NIST CSF, CIS, ISO 27001, SOC-CMM e mapeamento PCI DSS

3. Catálogo de módulos

O produto é modularizado. Cada plano habilita um subconjunto de módulos, permitindo contratar exatamente a cobertura necessária.

Grupo	Módulo	O que faz
Core	Painel principal	Visão geral do tenant: ativos, riscos e tendências
	Findings	Lista unificada de descobertas com ciclo de vida (novo → resolvido)
	Notificações	Alertas in-app, e-mail e push para mudanças críticas
ASM	ASM Discovery	Descoberta de domínios, subdomínios e ativos expostos
	DeepScan	Varredura profunda de vulnerabilidades e exposições
	Monitoramento contínuo	Re-varreduras agendadas + detecção de mudança + alerta automático
	Attack Paths	Visualização de caminhos de ataque (mapeamento MITRE ATT&CK)
Maturidade	NIST CSF	Framework NIST Cybersecurity (Govern/Identify/Protect/Detect/Respond/Recover)
	CIS Controls	CIS v8 — 18 controles + Implementation Groups (IG1/IG2/IG3)
	ISO 27001	Anexo A — 93 controles ISO 27001:2022
	SOC-CMM	Maturidade de SOC em 5 dimensões
	IA: Plano de ação	Recomendações de remediação geradas a partir dos gaps
	Validação de evidências	Upload de evidências + validação automática assistida por IA
Workflow	Plano de Ação	Kanban de remediação (maturidade + ASM)
	Roadmap	Priorização de riscos e iniciativas
	Integração Jira	Exportação de itens de ação como issues
	Integração Linear	Exportação de itens de ação
Executivo	Dashboard Executivo	Visão C-suite: radar de postura e KPIs consolidados
	Benchmark setorial	Comparação da maturidade contra a média do setor
	Export PDF	Scorecard executivo *board-ready*
Administração	Audit log	Histórico de ações dos membros da organização
	API keys	Geração e gestão de chaves de integração da organização
Threat Intel	Threat Intel	Credenciais, deep/dark web, marca, domínios similares, perfis falsos, VIPs, monitoramento e

		takedowns
Pentest	Pentest Marketplace	Pentest sob demanda (Web, BlackBox, GreyBox, Active Directory) por créditos

4. Attack Surface Management (ASM)

Descoberta e monitoramento contínuo da superfície de ataque externa da organização, sem necessidade de agentes ou instalação.

4.1 Descoberta de ativos

Capacidade	O que entrega
Gestão de domínios	Cadastro e acompanhamento dos domínios da organização, com histórico por ativo
Descoberta de subdomínios	Enumeração automática de subdomínios (passiva e ativa)
Inteligência de certificados	Descoberta de ativos a partir de registros de certificados públicos
Descoberta orquestrada	Pipeline completo que descobre, valida, enriquece, pontua e detecta mudanças
Mapeamento de rede	Faixas de IP e blocos de rede associados à organização
Grafo de ativos	Relacionamento entre domínios, subdomínios, serviços e IPs

4.2 Sondagem e caracterização

Capacidade	O que entrega
Portas e serviços	Identificação de portas abertas e serviços expostos
Sondagem web	Status, títulos, redirecionamentos e tecnologias de cada endereço
Descoberta de conteúdo	Mapeamento de páginas, diretórios e arquivos expostos
Fingerprinting tecnológico	Identificação do stack tecnológico de cada ativo
Capturas de tela	Registro visual dos ativos expostos
Análise TLS/certificados	Validade, cadeia, protocolos e cifras dos certificados
Detecção de WAF	Identificação de firewall de aplicação web
Headers de segurança HTTP	Verificação de headers de proteção (HSTS, CSP, X-Frame-Options, etc.)

4.3 Vulnerabilidades e exposições

Capacidade	O que entrega
Detecção de vulnerabilidades	Identificação de vulnerabilidades conhecidas nos ativos expostos
Subdomain takeover	Detecção de subdomínios passíveis de sequestro

Exposição de dados	Arquivos, diretórios, backups e repositórios sensíveis expostos
Exposição em nuvem	Ativos e serviços de nuvem pública expostos
Serviços de acesso remoto	Identificação de VPN, webmail, SSO, painéis administrativos, SSH, RDP e Git expostos
Cadeia de suprimentos web	Análise de scripts de terceiros e bibliotecas desatualizadas/vulneráveis
Segredos expostos	Detecção de segredos e credenciais vazadas em repositórios públicos

4.4 Priorização inteligente

Cada vulnerabilidade é priorizada por risco real — não apenas pela severidade nominal:

Dimensão	O que agrega
Probabilidade de exploração	Estimativa de chance de exploração no curto prazo (padrão EPSS)
Exploração ativa conhecida	Sinalização de vulnerabilidades já exploradas por atacantes (catálogo CISA KEV)
Severidade técnica	Pontuação padrão CVSS, complementada quando ausente
Contexto de exposição	Grau de exposição do ativo na internet

4.5 Monitoramento contínuo

Capacidade	O que entrega
Re-varredura agendada	Reavaliação periódica e automática da superfície
Detecção de mudança	Compara com o estado anterior e sinaliza o que surgiu, mudou ou desapareceu
Histórico de superfície	Linha do tempo versionada da superfície de ataque
Priorização de mudanças	Ordenação das mudanças por criticidade
Alerta automático	Notificação em tempo real de novas exposições relevantes

4.6 ASM Score

Índice objetivo que resume a postura de superfície de ataque, decomposto por dimensão e recalculado automaticamente a cada avaliação — permitindo acompanhar a evolução ao longo do tempo.

5. Threat Intelligence & Proteção de Marca

Inteligência de ameaças externa focada em detecção de exposição, fraude e uso indevido da marca, cobrindo as camadas **Surface, Deep e Dark Web**. A seção a seguir detalha a cobertura de monitoramento de ameaças externas, vazamentos e proteção de marca.

5.1 Alertas em tempo real de domínios

Ingestão contínua de vazamentos e exposições associados aos domínios da contratante, com **geração de alertas em tempo real** assim que um novo dado é identificado. Os domínios monitorados são configuráveis, e cada evento gera notificação in-app, e-mail e push.

5.2 Busca e coleta multi-fonte

Coleta e busca em múltiplas fontes, com consultas relacionadas à contratante:

Fonte	Cobertura
Deep Web	Menções e vazamentos em fóruns e marketplaces indexados de deep web
Dark Web / Tor (onion)	Mercados, fóruns e sites de vazamento na rede onion (Tor hidden services)
Fóruns underground / restritos	Comunidades fechadas de compra e venda de dados (breach/leak forums)
Canais de Telegram (cybercrime)	Feeds de stealer logs e dados vazados distribuídos em canais de cybercrime no Telegram
Redes sociais	Perfis, páginas e menções públicas
Paste sites / sites de vazamento	Repositórios públicos de dados vazados
Credenciais expostas	Bases de credenciais vazadas correlacionadas aos domínios monitorados

Modos de busca:

Modo	O que entrega
Busca por palavra-chave	Editor de consultas com termos relacionados à contratante + coletores salvos por canal, executáveis de forma recorrente
Busca avançada (estruturada)	Filtro por domínios, e-mails, usuários, senhas, IPs, URLs, fontes, força de senha e intervalo de data — resultados com revelação controlada
Busca semântica por IA (NLP/ML)	Consulta em **linguagem natural** sobre as menções coletadas, com *embeddings* e ranqueamento por **similaridade de significado** — não apenas correspondência exata de termos

5.3 Alertas de vazamento em Deep, Dark e Surface Web

Criação e geração de alertas sobre possíveis vazamentos de dados da contratante nas três camadas da web, incluindo:

- **Credenciais corporativas vazadas** — login/senha expostos, com inferência do papel da conta (administrativa, colaborador, cliente) e revelação controlada com registro de acesso.
- **Dados à venda** — exposição em mídias sociais, sites de compra e venda de dados vazados e fóruns criminosos.
- **Menções em grupos de Telegram** — dados e acessos circulando em canais de cybercrime.

- **Correlação de maior valor** — cruzamento entre credencial corporativa vazada e serviço de acesso remoto exposto, sinalizando o risco de invasão mais provável.
- **Verificação contra bases de vazamento conhecidas** — confirmação de comprometimento de contas e domínios.

5.4 Exploits e códigos maliciosos relevantes ao ambiente

O módulo detecta e monitora códigos maliciosos, incluindo IOCs de malware e ransomware (hashes, domínios, IPs de C2), campanhas ativas e contexto de ameaça alinhado ao MITRE ATT&CK.

5.5 Monitoramento de reputação

Monitoramento da reputação da organização **como um todo**, considerando todos os seus ativos e usuários internos:

Capacidade	O que entrega
Domínios similares (typosquatting)	Detecção de domínios semelhantes e classificação da técnica de imitação; avalia se o domínio está registrado, ativo e apto a enviar e-mails de phishing
Ativos de marca	Cadastro de marcas, perfis sociais e palavras-chave protegidas
Perfis falsos / impersonação	Descoberta de perfis suspeitos que se passam pela organização ou seus executivos em redes sociais
Monitoramento de VIPs	Vigilância de executivos e contas-chave contra vazamentos e uso indevido
Usuários internos	Cobertura de credenciais e exposição de colaboradores da organização
Reputação setorial	Perfil de ameaças e reputação no contexto do setor de atuação

5.6 Monitoramento de adversários

Monitoramento contínuo de fontes externas **nacionais e internacionais** — fóruns, redes e mídias sociais, nuvens públicas e grupos hackers — nas camadas **Surface, Deep e Dark Web**. Vai além de CVEs: a plataforma acompanha e correlaciona ao setor da contratante os principais **atores de ameaça (threat actors), grupos APT e de ransomware**, seus **TTPs mapeados ao MITRE ATT&CK** e as **tendências de ameaça** relevantes ao segmento — contextualizados pela **exposição real** da organização (credenciais vazadas, serviços expostos e vulnerabilidades detectadas). Inclui menções em deep web, exposição em canais de cybercrime e atividade em redes sociais.

5.7 Takedown a partir do incidente

Diretamente a partir de uma detecção ou incidente aberto na ferramenta, é possível **solicitar o serviço de remoção de conteúdo infrator (takedown)** — domínios fraudulentos, perfis falsos e conteúdo indevido — com acompanhamento do andamento da solicitação dentro da própria plataforma.

5.8 Cobertura técnica (resumo)

Capacidades cobertas pela plataforma, nas categorias de ASM, CTI, Digital Risk Protection (DRP) e Vulnerability Intelligence:

- **Attack Surface Management / External Exposure** — Attack Surface Discovery · Subdomain Discovery · Shadow IT · Continuous Monitoring · Grafo de ativos
- **Vulnerability Intelligence** — CVE · EPSS · CISA KEV · exploração ativa · priorização por risco · correlação ao stack tecnológico
- **Cyber Threat Intelligence (CTI)** — Deep Web · Dark Web · Tor (onion) · Underground Forums · Telegram · Paste Sites · Credential Exposure · Threat Actors · APT/Ransomware Groups · MITRE ATT&CK (TTPs)
- **Digital Risk Protection (DRP)** — Brand Monitoring · Brand Protection · Typosquatting · Fake/Look-alike Domains · Phishing · Impersonation · Executive Monitoring · Takedown
- **Busca** — por palavra-chave · domínio · e-mail · IP · indicadores (IPs/URLs) · busca semântica por IA (NLP/ML)

6. Maturidade & Conformidade

Avaliações completas contra os principais frameworks de segurança, com pontuação, comparação temporal e apoio de IA.

6.1 Frameworks suportados

Framework	Escopo
NIST CSF 2.0	Govern · Identify · Protect · Detect · Respond · Recover
CIS Controls v8	18 controles + Implementation Groups (IG1/IG2/IG3)
ISO/IEC 27001:2022	Anexo A — 93 controles
SOC-CMM v4.0	Maturidade de SOC em 5 dimensões (business, people, process, technology, services)

6.2 Recursos de avaliação

Capacidade	O que entrega
Pontuação de maturidade	Cálculo de maturidade por categoria e controle, com pesos por framework
Validação de evidências por IA	Upload de evidências + análise automática de aderência ao controle
Reescrita para auditoria	Reformulação assistida de perguntas em linguagem de auditoria
Tradução automática	Perguntas disponíveis em pt/en/es
Mapeamento ASM → controles	Vincula achados da superfície de ataque a controles de framework
Hub de evidências	Central de gestão e revisão de evidências
Dashboards por framework	Visão de maturidade dedicada por framework
Benchmark setorial	Comparação da maturidade contra a média do setor

7. Risco, Plano de Ação & Roadmap

Transforma sinais brutos em trabalho priorizado e rastreável.

Capacidade	O que entrega
Avaliação de risco	Cálculo de risco combinando confidencialidade/integridade/disponibilidade, severidade técnica e contexto de exposição
Plano de ação por IA	Geração automática de recomendações de remediação a partir dos gaps identificados
Plano de ação (Kanban)	Board de remediação com origem em maturidade e ASM, com ciclo de vida das tarefas
Roadmap executável	Priorização visual de riscos e iniciativas de segurança
Attack path mapping	Encadeamento dos caminhos de ataque prováveis
Tarefas e responsáveis	Atribuição e acompanhamento das tarefas de remediação
Histórico de risco	Trilha de evolução do risco ao longo do tempo

8. Dashboards & Executivo

Capacidade	O que entrega
Dashboard principal	Consolidação operacional: ativos, achados, riscos e tendências
Dashboard executivo	Visão C-suite — radar de postura e KPIs consolidados
Painel de sinais (24h)	Feed das ameaças e mudanças mais recentes
Scorecards	Índices resumidos por dimensão
Export PDF	Relatório executivo *board-ready*
Export Excel	Exportação tabular de achados e avaliações

9. Pentest Marketplace

Capacidade	O que entrega
Marketplace sob demanda	Solicitação de pentest por modalidade: Web, BlackBox, GreyBox e Active Directory
Modelo de créditos	Consumo de créditos por solicitação, com saldo e histórico
Acompanhamento	Gestão das solicitações e entregas dentro da plataforma

10. Multi-tenancy, Administração & Planos

Capacidade	O que entrega
Multi-tenancy	Isolamento lógico total entre organizações
Provisionamento	Criação e configuração guiada de novas organizações
Gestão de organizações	Listagem, detalhamento e configuração de tenants

Convites de usuário	Fluxo de convite e aceite (acesso apenas por convite)
Controle de acesso por papel	Papéis e permissões granulares por usuário
Trilha de auditoria	Histórico das ações dos membros da organização
Planos e módulos	Habilitação de módulos por plano e gestão de limites
Limites por plano	Domínios, usuários, volume de varreduras, cotas de VIP e de revelação de credenciais

11. Integrações & Notificações

Capacidade	O que entrega
Integração Jira	Exportação de itens de ação como issues no Jira
Integração Linear	Exportação de itens de ação para o Linear
Notificações push	Alertas em tempo real no navegador
Notificações por e-mail	Alertas transacionais e resumos
Central de notificações	Preferências e histórico de alertas in-app
API keys	Chaves de integração para consumo programático

12. Autenticação & Conta

Capacidade	O que entrega
Login seguro	Autenticação por e-mail e senha
MFA (TOTP)	Autenticação de dois fatores com verificação obrigatória em acessos sensíveis
Recuperação de senha	Fluxo de redefinição por e-mail
Acesso por convite	Cadastro apenas mediante convite da organização

13. Segurança & Conformidade

Dimensão	Garantia
Isolamento multi-tenant	Dados de cada organização isolados de forma estrita
Autenticação forte	MFA/TOTP com verificação obrigatória em ações sensíveis
Controle de acesso	Papéis e permissões granulares por usuário
Trilha de auditoria	Registro das ações relevantes de plataforma e de organização
Privacidade (LGPD)	Tratamento de dados aderente à LGPD, com expiração automática de dados sensíveis
Coleta não-intrusiva	Operação 100% *outside-in*, sem agentes no ambiente do cliente
Confidencialidade de fontes	Modelo *white-label* — fontes de inteligência não são expostas

14. Diferenciais

- **Cobertura CTEM ponta-a-ponta** — ASM, Threat Intelligence e Maturidade num único produto, não três ferramentas costuradas.
- **Priorização por risco real** — cada vulnerabilidade ponderada por probabilidade de exploração e exploração ativa conhecida, não apenas pela severidade nominal.
- **A correlação de maior valor** — credencial corporativa vazada cruzada com serviço de acesso remoto exposto.
- **Proteção de marca completa** — typosquatting, perfis falsos, exposição em fóruns e Telegram, e fluxo de takedown integrado ao incidente.
- **IA com rede de segurança** — validação de evidências e planos de ação assistidos por IA, sempre com alternativa determinística.
- **Aderente a frameworks e RFPs** — NIST CSF, CIS, ISO 27001, SOC-CMM, PCI DSS e requisitos de monitoramento de ameaças em deep/dark/surface web.
- **Experiência premium** — interface dark-first, editorial, responsiva e trilíngue.

Documento de referência funcional. As capacidades descritas refletem a solução em produção.