INSIGHTS DE CIBERSEGURANÇA PARA SETORES NO BRASIL

EDIÇÃO:

SETOR ELÉTRICO

heimdall
security research

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 Introdução

Ataques cibernéticos contra infraestruturas críticas são uma realidade e o setor elétrico está no centro desse novo campo de batalha digital.

Campanhas avançadas, organizadas por grupos de **Ameaça Persistente Avançada (APT),** estão mirando diretamente em **sistemas OT/ICS,** explorando vulnerabilidades estruturais para causar impactos severos, como **apagões regionais, colapsos operacionais e crises de segurança pública.**

Segundo levantamento feito pelas equipes de **Threat Intelligence** e **Purple Team** da ISH, o Heimdall, o padrão desses ataques é claro: ofensores adotam táticas de permanência prolongada em ambientes com baixa visibilidade, promovem movimentos laterais e aproveitam a fragmentação entre os mundos IT e OT para escalar acessos e comprometer sistemas industriais de alto valor.

Não se trata mais de "e se acontecer", mas de "quando e como vai acontecer" e o seu negócio precisa estar preparado.

Neste e-book, você encontra um panorama do cenário de ameaças cibernéticas contra infraestruturas industriais. Com foco em sistemas de controle (ICS), detalhamos os grupos ofensores, vetores de ataque, motivações, técnicas utilizadas e as consequências observadas em ataques notáveis, além de apresentar os riscos no contexto brasileiro.

2 Contexto dos Sistemas de Controle Industrial (ICS)

Os Sistemas de Controle Industrial (ICS) formam a base da automação e operação em ambientes industriais, como usinas de energia, estações de tratamento de água, refinarias e plantas de manufatura.

Eles são compostos por diferentes tipos de tecnologias que permitem o monitoramento, o controle e a operação segura e contínua desses processos.

Apesar de sua criticidade, muitos desses sistemas foram projetados originalmente sem considerar cenários de ameaças cibernéticas, o que os torna alvos altamente sensíveis e vulneráveis no contexto atual.

ICS são ambientes onde segurança, confiabilidade e continuidade precisam coexistir e onde o risco cibernético tem consequências reais para a vida das pessoas e a estabilidade de serviços essenciais.

Principais componentes dos ambientes ICS:

- **SCADA (Supervisory Control and Data Acquisition):** sistemas amplamente utilizados para supervisão e aquisição de dados, geralmente integrando redes geograficamente distribuídas.
- **PLC (Programmable Logic Controllers):** equipamentos responsáveis por controlar processos industriais em tempo real, como abertura de válvulas, controle de temperatura e ativação de alarmes.
- **RTU (Remote Terminal Units):** dispositivos que coletam dados de sensores remotos e os transmitem ao sistema SCADA.
- **HMI (Human-Machine Interface):** interfaces gráficas que permitem a operadores humanos interagir com o processo industrial.

Muitos desses dispositivos operam com sistemas legados, interfaces expostas e autenticação fraca, criando pontos de entrada que ofensores experientes conseguem explorar com facilidade.

Desafios de segurança em ambientes ICS:

1. **Ambientes altamente heterogêneos,** com tecnologias de diferentes gerações.
2. **Baixa visibilidade de tráfego OT,** dificultando a detecção de comportamentos anômalos.
3. **Dependência de sistemas legados,** sem atualizações de segurança regulares.
4. **Falta de segmentação entre IT e OT,** criando caminhos de ataques diretos.

Além disso, o tempo de indisponibilidade em ambientes industriais pode gerar perdas catastróficas. Isso torna a **resiliência operacional** e a **capacidade de resposta a incidentes** elementos tão críticos quanto a própria detecção de ameaças.

INSIGHTS ISH

ICS: o que os olhos não veem, o risco entrega

Muitos ambientes ICS ainda operam com protocolos inseguros, autenticação fraca e pouca visibilidade de tráfego. Para esses casos, a detecção tradicional não basta. A combinação entre segmentação, inventário contínuo e análise comportamental é o primeiro passo para uma defesa real.

3 Panorama de ameaças e incidentes em ICS

A expansão da conectividade em ambientes industriais tem acelerado a transformação digital em setores como energia, transporte, manufatura e saneamento. No entanto, essa evolução também ampliou drasticamente a **superfície de ataque** e expôs as redes OT a ameaças antes restritas ao domínio da TI.

As infraestruturas críticas já se tornaram alvos prioritários. Casos como **Industroyer, Triton, BlackEnergy e NotPetya** revelaram o potencial destrutivo dos ataques cibernéticos em sistemas industriais, com impactos que vão de blecautes em regiões inteiras à manipulação de processos físicos capazes de causar perdas humanas e ambientais.

Mas essas campanhas não são exceção. Elas fazem parte de uma tendência crescente, com grupos avançados (APTs) desenvolvendo **ferramentas específicas para ICS/OT,** explorando protocolos industriais, invadindo redes com engenharia reversa e buscando comprometer os níveis mais sensíveis da cadeia de controle.

Por que isso importa para as empresas brasileiras?

Embora grandes ataques tenham ocorrido em outros países, o Brasil já é alvo de campanhas com potencial disruptivo em ambientes industriais. A combinação de baixa visibilidade, redes legadas, baixa maturidade em segmentação e ausência de planos integrados de resposta tornam o cenário ainda mais crítico.

Vale destacar:

Ataques contra o setor elétrico já foram identificados no Brasil e América Latina com foco em engenharia social e acesso inicial via credenciais expostas.

Infraestruturas industriais brasileiras operam, em muitos casos, com **protocolos antigos sem autenticação ou criptografia,** como Modbus ou DNP3.

Fornecedores terceirizados e dispositivos móveis utilizados em campo têm sido portas de entrada, em especial, em setores como energia, saneamento e óleo & gás.

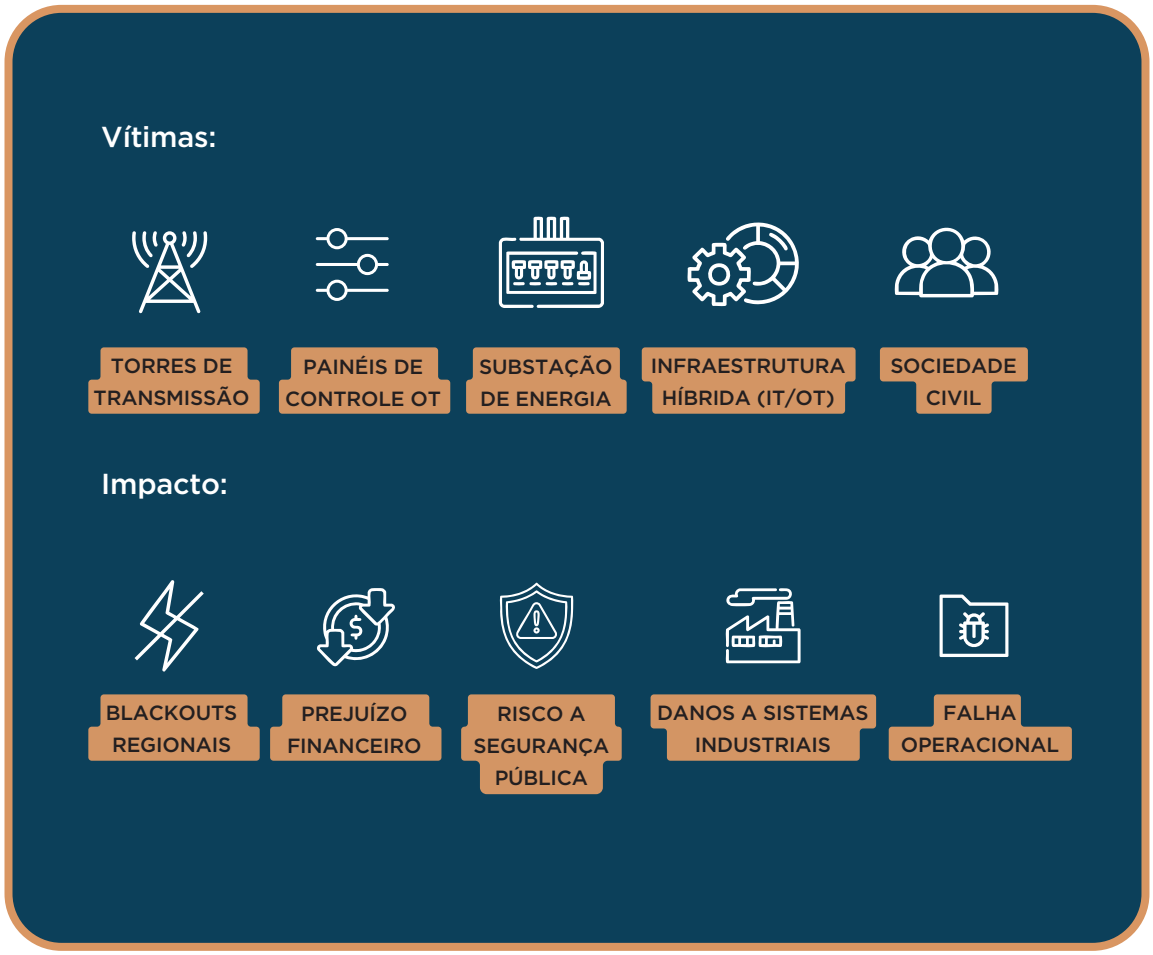


Figura 1 – Vítimas e impactos de incidentes voltados a infraestruturas críticas

As vítimas mais visadas incluem:

- Torres de transmissão e subestações de energia
- Painéis de controle OT e infraestrutura híbrida IT/OT
- Sistemas diretamente conectados à sociedade civil

Os riscos vão além do downtime

Ao contrário do que se pensa, o impacto de um ataque cibernético a ICS/OT não se resume à paralisação temporária das operações. Os efeitos podem incluir:

1. **Prejuízos financeiros de larga escala**
2. **Riscos à vida e à segurança pública**
3. **Danos físicos a equipamentos**
4. **Blackouts regionais**
5. **Perda de confiança institucional**
6. **Falhas de conformidade com órgãos reguladores**

Esses impactos estão diretamente associados à natureza do alvo, infraestruturas críticas que sustentam a vida moderna e a segurança de populações inteiras.

4 Vetores de ameaças e técnicas utilizadas

Os ataques a infraestruturas críticas e ambientes ICS não seguem um padrão único. A superfície de ataque é ampla e os ofensores frequentemente exploram diferentes pontos da arquitetura OT, seguindo caminhos indiretos até alcançar os sistemas de controle.

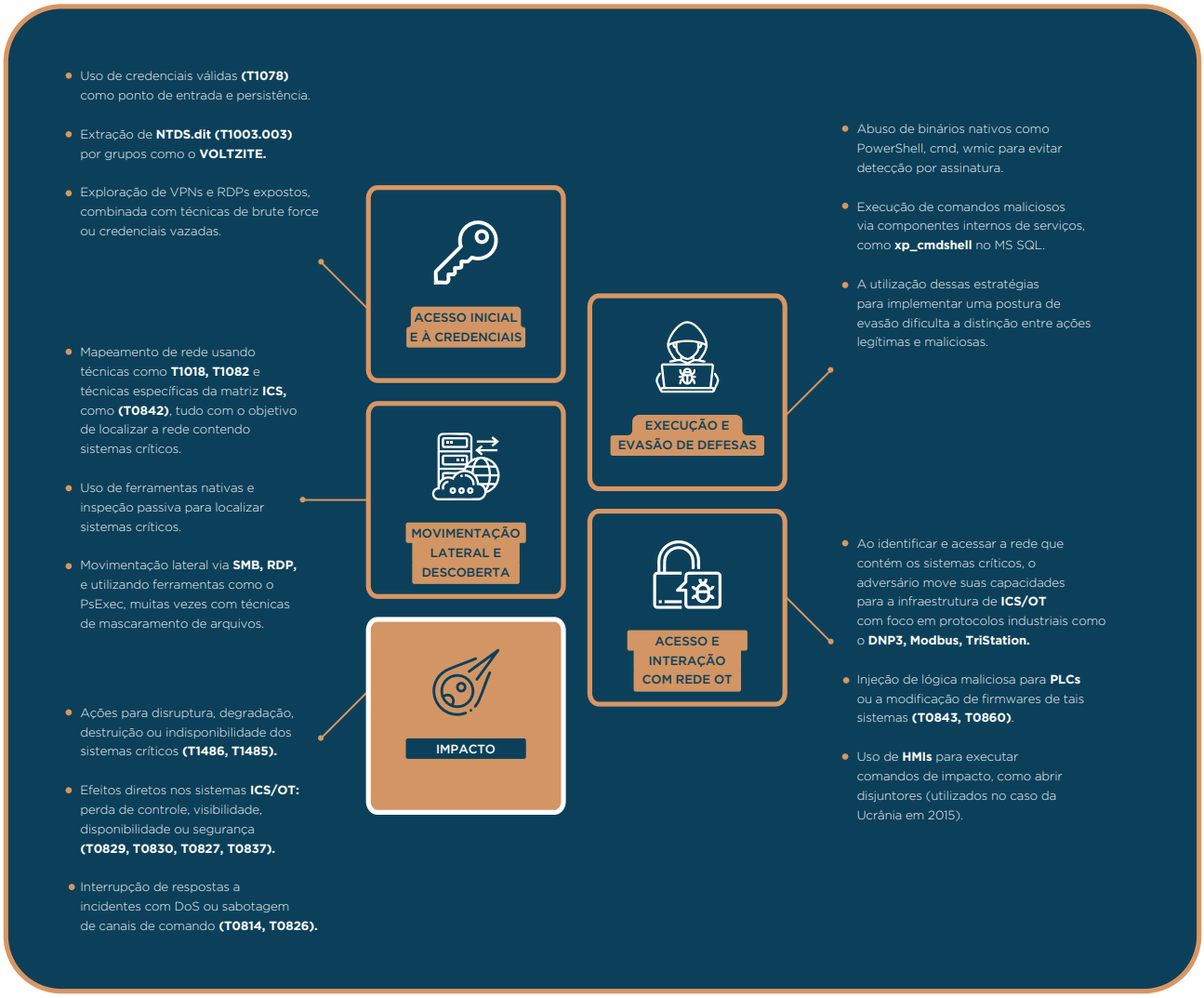


Figura 2 – Vetores de acesso a ambientes ICS/OT

Os vetores mais explorados incluem:

Dispositivos com acesso remoto
Uso indevido de conexões RDP e VPNs com autenticação fraca, sem MFA e muitas vezes mal segmentadas.

Sistemas de Engenharia e Atualização
Manipulação de estações de engenharia (EWS) e compromissos durante processos legítimos de atualização de firmware/software.

Serviços de gerenciamento e redes administrativas
Ataques começam na camada de TI tradicional, evoluindo para movimentos laterais em direção à rede OT por meio de credenciais compartilhadas, configurações inseguras ou ativos mal inventariados.

Supply Chain e Vendors
Exploração de conexões de terceiros para acesso privilegiado — como contratos de manutenção, supervisão remota e integração com ERPs e SCADAs híbridos.

Ataques direcionados à cadeia de suprimentos já representam um dos métodos mais eficazes de acesso furtivo aos ambientes ICS.

Técnicas utilizadas pelos ofensores

Os ataques mais sofisticados seguem uma lógica multivetorial, composta por etapas encadeadas de persistência, elevação de privilégios e movimentação lateral.

As principais táticas observadas foram:

☑ **Reconhecimento de ativos via protocolos OT (Modbus, DNP3, S7, etc.)**

☑ **Uso de malware customizado com capacidade de evasão**

☑ **Exfiltração de dados sensoriais e arquivos de configuração**

☑ **Execução remota de comandos com foco em paralisação ou sabotagem**

☑ **Persistência em firmwares e backdoors não visíveis em ferramentas convencionais de TI**

Exemplo prático: Em ambientes com integração entre SCADA e sistemas ERP/BI, ofensores exploraram APIs mal segmentadas para executar comandos OT remotamente, sem gerar alertas no sistema SIEM corporativo.

INSIGHTS ISH

RDP e VPN mal segmentados continuam sendo o elo mais fraco

Acesso remoto inseguro é ainda um dos principais vetores de intrusão. Adoção de MFA, redes segmentadas, firewalls industriais e monitoramento contínuo são medidas indispensáveis em qualquer arquitetura moderna.

Cadeia de ataque tradicional

Esse modelo representa a sequência mais comum em ataques cibernéticos, com forte presença em ambientes corporativos e, cada vez mais, adaptado a ambientes industriais:

FASE 1

01 – RECONNAISSANCE

Coleta de informações sobre a organização-alvo. Pode incluir varredura de redes, coleta de metadados em documentos públicos, análise de redes sociais de funcionários e mapeamento de portas e serviços expostos.

02 – TARGET

Escolha de ativos ou indivíduo específico que apresenta maior valor ou vulnerabilidades. Pode incluir usuários com altos privilégios, sistemas legados sem patch ou dispositivos OT expostos.

03 – WEAPONIZATION

Compra, construção ou personalização de ferramentas maliciosas para explorar os alvos identificados. Pode envolver trojans, scripts ofuscados em Powershell, malwares customizados ou toolkits inteiros.

04 – DELIVERY

O vetor de ataque é entregue ao alvo por meio de canais como e-mail phishing, links maliciosos, dispositivos USB, redes comprometidas ou downloads drive-by. A eficácia depende do meio de entrega ser convincente e passar despercebido pelas defesas iniciais.

05 – EXPLOIT

O vetor entregue e executado no alvo aciona um exploit que quebra a segurança do sistema ou pode ser uma falha em software, execução de macros maliciosas ou scripts com permissões elevadas.

06 – INSTALL

Após obter acesso, o atacante instala malware ou ferramentas de acesso remoto (RATs) para manter persistência no ambiente. Isso pode incluir alterações no registro, criação de serviços maliciosos, uso de backdoors ou modificação de arquivos legítimos.

07 – COMMAND AND CONTROL

É estabelecido um canal de comunicação entre o ambiente comprometido e a infraestrutura controlada pelo atacante. Técnicas comuns incluem DNS tunneling, canais HTTPS ofuscados e uso de serviços legítimos como GitHub ou Dropbox.

08 – ACTION

O atacante executa sua intenção final: exfiltração de dados sensíveis, sabotagem de sistemas, interrupção de processos industriais ou movimentação lateral em busca de outros ativos.

Figura 3 – Cadeia de ataque padrão com oito etapas

Cadeia de ataque adaptada para ICS

Em ambientes industriais, os atacantes adaptam suas ações às limitações físicas e aos protocolos específicos. As informações a seguir detalham a segunda fase dos ataques direcionados a infraestruturas críticas:

FASE 2

01 – DEVELOP

O adversário desenvolve ou customiza ferramentas e payloads especificamente voltados para ambientes industriais. Isso inclui malwares que reconhecem protocolos industriais (como Modbus, DNP3 ou OPC), arquivos de projeto de sistemas SCADA, exploits para PLCs ou até engenharia reversa de firmwares de controladores. Foco em criar componentes capazes de interagir diretamente com sistemas ciberfísicos e causar impactos operacionais.

02 – TEST

Teste de ferramentas e payloads em ambientes simulados ou redes parecidas com o alvo (testbeds, redes clonadas, sistemas de validação). O objetivo é garantir que os malwares não quebrem o processo de forma prematura, que se comportem conforme o planejado e que passem por defesas como firewalls industriais, HMI watchdogs ou sistemas de integridade. Em APTs, essa fase pode durar meses.

03 – DELIVER

O payload industrial é entregue ao ambiente-alvo e geralmente por pivotagem a partir de sistemas corporativos (TI), acesso remoto comprometido (VPNs/RDP), ou dispositivos de manutenção (como laptops de técnicos ou engenheiros de campo). Essa etapa é crítica em ambientes OT onde o isolamento lógico/físico (air gap) é uma barreira comum, então o vetor precisa ser inteligente ou oportunista.

04 – INSTALL/MODIFY

O atacante modifica configurações ou instala softwares ou módulos diretamente em ativos industriais. Isso pode incluir alterações em lógicas de PLC, mudanças em setpoints de sensores, upload de códigos falsos ou substituição de bibliotecas legítimas. Essa fase é geralmente silenciosa e bem controlada, pois qualquer falha visível pode ativar protocolos de segurança operacional.

05 – EXECUTE ICS ATTACK

A fase final é a execução do objetivo na camada operacional: parar processos industriais, causar danos físicos, manipular dados de sensores para enganar operadores, sobrecarregar equipamentos ou comprometer a segurança de pessoas e ambientes. Exemplos reais incluem o ataque do Stuxnet, que alterava a rotação de centrífugas, ou o TRITON, que visava sistemas de segurança (SIS) para permitir falhas catastróficas.

Figura 4 – Cadeia de ataque em ambientes ICS

5 Ataques notáveis e repercussões

À medida que os ambientes ICS se tornam mais conectados, a lista de adversários com foco específico em operações industriais cresce em volume e sofisticação.

Nas últimas décadas, diversos grupos APTs realizaram ataques voltados a infraestruturas críticas em setores como energia elétrica, petróleo e gás, telecomunicações, transportes e água.

O objetivo, em muitos casos, não é apenas roubar dados, mas interromper, sabotar e até destruir operações industriais inteiras.

Em comum, esses grupos compartilham algumas características:

- Longo tempo de permanência nos ambientes antes de qualquer ação visível
- Ferramentas especializadas para interação com controladores industriais
- Exploração de vulnerabilidades em equipamentos de campo e sistemas legados
- Utilização de táticas de acesso inicial silenciosas e evasivas
- Interesses estratégicos ligados à infraestrutura nacional ou geopolítica

Reunimos os principais atores identificados globalmente com atuação ou capacidade técnica direcionada a ICS, conforme monitoramento do Heimdall Security Research:

ICS CYBER THREAT	INTELIGÊNCIA DE SUAS OPERAÇÕES
SANDWORM (a.k.a ELECTRUM)	Sandworm, atribuído à Unit 74455 do GRU russo, é conhecido por ataques disruptivos contra infraestruturas críticas, especialmente no setor de energia da Ucrânia. Suas campanhas OT/ICS envolveram malwares como Industroyer/CrashOverride, projetado para manipular disjuntores elétricos, e BlackEnergy, usado em ataques anteriores. Embora FrostyGoop não seja diretamente associado a ataques OT/ICS do Sandworm, sendo mais um downloader genérico ou uma ferramenta de acesso inicial, utiliza um vasto arsenal que inclui também wipers, como KillDisk e NotPetya (este último com impacto global). Além disso, utiliza backdoors e ferramentas de reconhecimento para comprometer e persistir em Redes OT.
XENOTIME	Conhecido pelo ataque TRISIS/TRITON ao sistema de instrumentação de segurança (SIS) de uma instalação petroquímica no Oriente Médio. Focado em comprometer a segurança de processos industriais, com potencial para causar danos físicos e interrupções.
DYMALLOY	Ativo desde meados de 2015, com foco em alvos de energia elétrica, petróleo e gás na América do Norte, Europa e Turquia. Conhecido por usar uma variedade de táticas, incluindo Spear Phishing e exploração de vulnerabilidades.
ALLANITE	Ativo desde 2016, visando principalmente organizações do setor elétrico no Reino Unido e nos Estados Unidos. Focado em reconhecimento e coleta de informações, possivelmente para futuros ataques.
CHRYSENE	Ativo desde 2017, visando entidades de petróleo e gás, manufatura e construção em múltiplos países, incluindo EUA, Índia, Paquistão e Arábia Saudita. Utiliza principalmente Spear Phishing para obter acesso inicial.
COVELLITE	Ativo desde 2018, visando principalmente concessionárias de energia elétrica na América do Norte, Europa e Ásia-Pacífico. Conhecido por usar malware de acesso remoto (RATs) e ferramentas de código aberto.
KAMACITE (Também conhecido como Berserk Bear, Dragonfly, Crouching Yeti)	Focado em alvos do setor elétrico ucraniano, responsável pelos ataques de 2015 e ligado ao desenvolvimento do malware CRASHOVERRIDE (utilizado pelo ELECTRUM em 2016).
PARISITE	Ativo desde 2017, visando principalmente o setor de aviação e transporte na América do Norte e Europa. Também demonstrou interesse em empresas de energia e petróleo e gás. Utiliza Spear Phishing e watering holes.
HEXANE (Também conhecido como Lyceum, OilRig, APT34)	Ativo desde 2018, com foco em organizações de petróleo e gás e telecomunicações no Oriente Médio e África. Conhecido por suas capacidades de acesso e coleta de informações.
MAGNALLIUM	Ativo desde 2013, visando organizações nos setores de energia, aeroespacial e outros setores industriais, principalmente na Arábia Saudita e em outros países do Oriente Médio. Ligado à atividade do grupo conhecido como APT33 ou Elfin.

ICS CYBER THREAT	INTELIGÊNCIA DE SUAS OPERAÇÕES
WASSONITE	Ativo desde 2018, visando setores industriais, incluindo geração de energia elétrica, manufatura e tecnologia, com foco geográfico na Coreia do Sul, Japão e Índia.
TALONITE	Ativo desde 2013, com foco inicial em alvos do setor elétrico nos Estados Unidos. Embora menos ativo recentemente, suas ferramentas e técnicas continuam a ser observadas.
VANADINITE	Ativo desde 2018, com foco em entidades de energia e transporte na América do Norte, Europa e Austrália. Conhecido por atividades de reconhecimento e acesso.
ERYTHRITE	Ativo desde 2019, com foco em organizações governamentais e do setor de energia nos Estados Unidos e Canadá. Conhecido pelo uso de credenciais roubadas e exploração de vulnerabilidades em dispositivos de acesso remoto.
STYGMOLOCH	Ativo desde 2019, visando organizações de petróleo e gás, energia elétrica e manufatura. Seu foco geográfico e táticas específicas ainda estão sendo ativamente pesquisados.
LAURIONITE	Descoberto em 2023, este grupo tem como alvo entidades portuárias e de logística na América do Norte. As táticas observadas incluem Spear Phishing e exploração de vulnerabilidades em servidores web.
VOLTZITE	Descoberto em 2023, este ator de ameaça tem como alvo entidades do setor elétrico dos EUA. A Dragos observou o Voltzite conduzindo reconhecimento de rede e tentando obter acesso a Redes OT e Sistemas ICS.
BENTONITE	Ativo desde 2021, com foco em organizações marítimas, governamentais, de petróleo e gás e manufatura em vários países. A Dragos observou o Bentonite explorando vulnerabilidades em dispositivos de borda de rede.

Tabela 1 – Principais atores e grupos com foco em ICS/OT

INSIGHTS ISH

Ameaça persistente é estratégia, não exceção

Grupos como Sandworm, Xenotime e Dymalloy planejam campanhas com meses de antecedência. Operam de forma silenciosa, modular e evasiva. O Heimdall monitora continuamente esses atores para gerar alertas contextualizados para ambientes industriais reais.

Esses grupos não operam com as mesmas dinâmicas de ameaças convencionais. O que os torna tão perigosos é justamente sua abordagem estratégica: ataques silenciosos, modulares, voltado para reconhecimento, persistência e ativação apenas em momento crítico.

E para o setor industrial, isso significa:

☑ **Sistemas críticos sendo monitorados sem que a organização perceba**

☑ **Códigos maliciosos estados previamente em ambientes semelhantes ao seu**

☑ **Técnicas de ataque desenvolvidas com meses ou anos de antecedência**

A maioria das empresas não tem visibilidade sobre atividades anômalas em suas redes OT, nem controle granular sobre acessos e movimentações internas entre IT e OT.

Mais do que nunca, é preciso encarar esses grupos como o que de fato são:

ameaças reais, com capacidade comprovada de impactar cadeias de fornecimento, produção, segurança pública e estabilidade institucional.

6 Estratégias de defesa e monitoramento em ambientes OT/ICS

A defesa eficaz de redes industriais vai muito além da identificação de adversários. Ela começa no desenho da própria arquitetura de rede, com ênfase em segmentação, controle de acesso e visibilidade.

No centro dessa abordagem está o Modelo Purdue, uma referência internacional que organiza redes industriais em camadas funcionais para orientar políticas de segurança e segmentação.

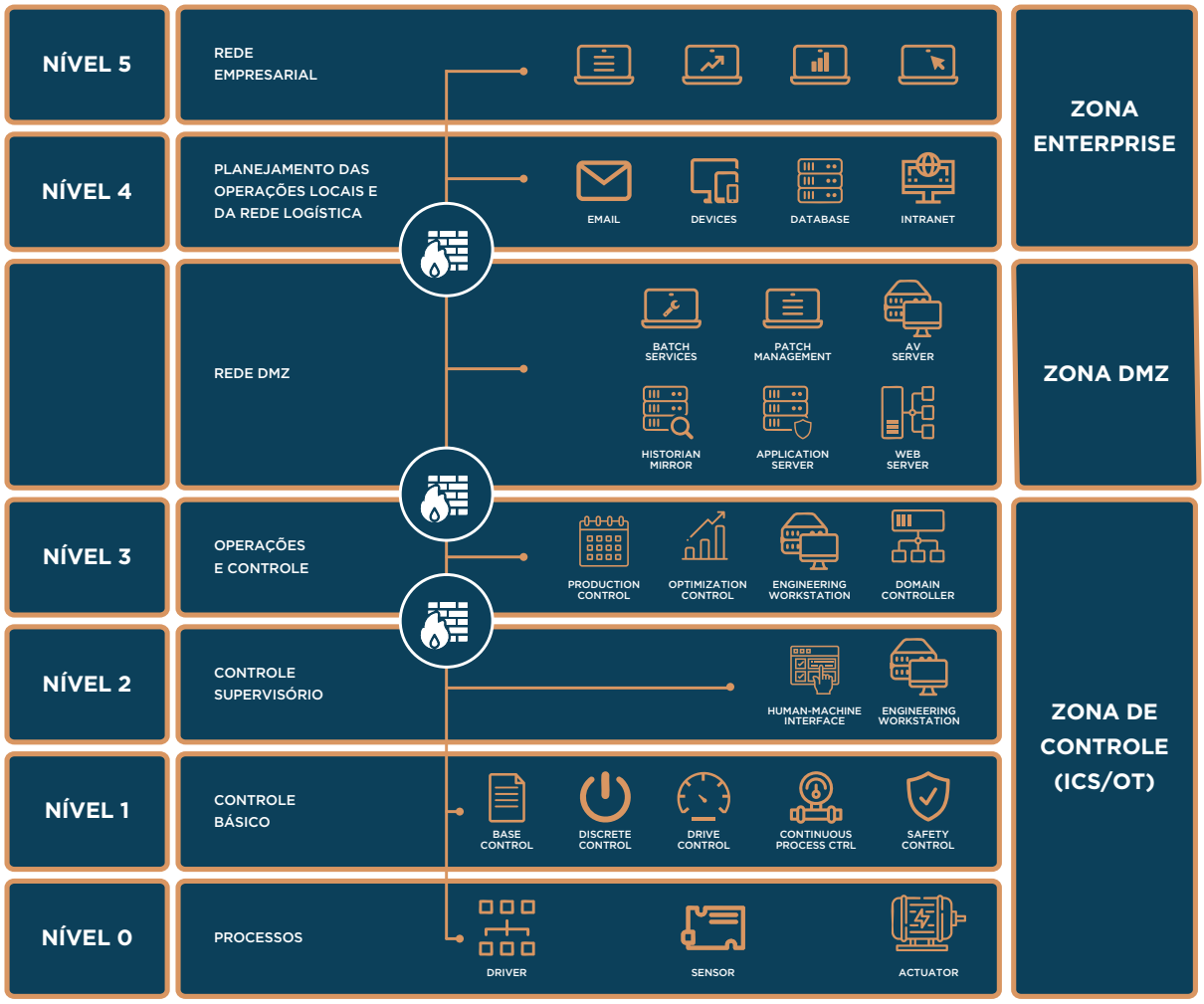


Figura 5 – Modelo Purdue para Cibersegurança de ICS/OT

A lógica é clara: quanto mais próximo da operação física, maior a criticidade dos ativos e maior o controle necessário.

Segmentação baseada no Modelo Purdue

Níveis 0, 1 e 2
(Processo físico, controle básico e supervisório)

☑ Dispositivos como PLCs, sensores e atuadores operam diretamente os processos industriais.

☑ A proteção exige a criação de "zonas de segurança" com segmentação lógica e física — via VLANs e firewalls industriais.

☑ Esses firewalls devem entender protocolos OT (Modbus, DNP3, S7comm etc.) e aplicar políticas que bloqueiem comandos não autorizados e tentativas de reprogramação.

Níveis 3
(Controle de operações e produção)

☑ Aqui residem sistemas SCADA, historiadores e aplicações de controle de produção.

☑ Este nível exige um segmento próprio, com políticas que limitem rigorosamente o acesso vindo dos níveis superiores e inferiores.

☑ A troca de dados com a TI deve ser feita via pontos de controle e proxies.

Zona Desmilitarizada (DMZ)
(Camada intermediária entre TI e OT)

☑ É a primeira linha de defesa contra ataques que migram da TI para o chão de fábrica.

☑ Serviços como proxies, jump servers, coletores de logs e servidores de patch devem operar dentro da DMZ.

☑ O uso de data diodes pode reforçar ainda mais a segurança, garantindo que o tráfego seja unidirecional da OT para a TI.

Níveis 4 e 5
(TI corporativa)

☑ Representam o ambiente onde normalmente se inicia a cadeia de ataque.

☑ A segmentação garante que qualquer acesso à OT passe obrigatoriamente pela DMZ, bloqueando ameaças como ransomwares e backdoors de origem corporativa.

Defesa em profundidade não é uma escolha, é uma necessidade para quem gerencia processos industriais críticos. A segmentação em múltiplos níveis reduz o raio de impacto e aumenta a capacidade de resposta.

INSIGHTS ISH

A aplicação do Purdue vai além do conceito: firewalls industriais, DMZs bem definidas, segmentação por zonas de segurança e regras adaptadas à criticidade operacional são pilares que precisam sair do papel — e fazem parte da estratégia do ISH Vision.

Monitoramento e detecção de ameaças em ambientes OT

Segmentar é proteger. Mas sem visibilidade, não há reação. O monitoramento contínuo é o que garante que as barreiras colocadas estejam de fato funcionando e que qualquer anomalia seja detectada em tempo hábil.

A centralização de logs e eventos é o ponto de partida. Devem ser incluídos:

1. Logs de **sistemas de engenharia** e **controladores de domínio** com acesso à rede OT
2. Eventos de **HMI e PLCs** com comportamento anormal
3. Alertas de **firewalls industriais, EDRs e IDSs** posicionados entre zonas críticas
4. Dados de **softwares de proteção e segurança operacional**

Esses registros devem ser enviados para um **SIEM (Security Information and Event Management)** com capacidade de:

1. Gerar alertas em tempo real com base em **casos de uso específicos**
2. Correlacionar eventos de múltiplos segmentos
3. Criar baselines de comportamento para identificar desvios operacionais
4. Utilizar Machine Learning para antecipar possíveis compromissos

Uma defesa integrada exige equipes integradas

Para uma defesa eficiente, é necessário contar com especialistas que entendam o contexto de cada segmento da rede.

A resposta a alertas de firewall, SIEM, EDR ou IDS deve ser contextualizada, automatizada e orquestrada para conter o avanço das ameaças sem comprometer a operação.

☑ **SOC, Blue Team e equipes OT devem trabalhar com regras alinhadas.**

☑ **Playbooks automatizados reduzem tempo de resposta.**

☑ **Monitoramento proativo evita que pequenos sinais virem grandes falhas.**

7 Desafios para o gerenciamento de vulnerabilidades em infraestruturas com OT/ICS

A integração entre sistemas industriais e corporativos tem evoluído com a Indústria 4.0, transformando a relação entre TI e OT. O que antes era uma rede fechada e isolada, agora está exposto a um cenário digital mais amplo, complexo e hostil.

Isso obriga as organizações a tratarem o gerenciamento de vulnerabilidades não mais como uma etapa de TI, mas como um processo **estratégico, contínuo e vital para a integridade da operação industrial.**

No entanto, essa integração ampliou drasticamente a superfície de ataque. Os sistemas OT, historicamente projetados para estabilidade e longevidade, não foram construídos com foco em segurança cibernética.

Muitos ativos estão em operação há décadas, utilizando protocolos inseguros, sem suporte ativo dos fornecedores e com baixíssima tolerância a interrupções. Assim, o ambiente ideal para a continuidade da operação se transforma em um terreno frágil diante das ameaças modernas.

Diferenças entre o gerenciamento de vulnerabilidades em ambientes Enterprise e OT/ICS

CARACTERÍSTICA	GERENCIAMENTO DE VULNERABILIDADES EM INFRAESTRUTURA OT/ICS	GERENCIAMENTO DE VULNERABILIDADES EM INFRAESTRUTURA ENTERPRISE
Prioridade principal	Segurança física, disponibilidade operacional, integridade do processo	Confidencialidade de dados, integridade de dados, disponibilidade de sistemas
Tolerância a downtime	Muito baixa / inexistente	Baixa a moderada (janelas de manutenção planejadas)
Ciclo De vida de ativos	Longo (15-20+ anos), muitos sistemas legados	Curto a médio (3-7 anos), tecnologia mais atualizada

CARACTERÍSTICA	GERENCIAMENTO DE VULNERABILIDADES EM INFRAESTRUTURA OT/ICS	GERENCIAMENTO DE VULNERABILIDADES EM INFRAESTRUTURA ENTERPRISE
Protocolos comuns	Modbus, DNP3, IEC 60870-5-104, Profinet, EtherNet/IP (muitas vezes inseguros)	TCP/IP, HTTP/S, SMTP, DNS (com mais mecanismos de segurança embutidos)
Impacto típico de incidentes	Interrupção de produção, danos físicos/ambientais, riscos à vida	Perda/roubo de dados, perdas financeiras, dano à reputação
Abordagem de patching	Complexa, arriscada, infrequente, requer planejamento extensivo, uso de controles compensatórios	Rotineira, mais automatizada, janelas de manutenção regulares
Ferramentas de segurança	Monitoramento passivo, IDS/IPS com reconhecimento de protocolo OT, análise comportamental	Scanners ativos, EDR, antivírus tradicional, SIEM
Visibilidade de ativos	Desafiadora (diversidade, protocolos proprietários, "shadow OT")	Mais direta (ferramentas de descoberta maduras)
Foco da avaliação de risco	Impacto no processo físico, segurança, confiabilidade operacional	Severidade da vulnerabilidade (CVSS), criticidade do ativo, impacto no negócio
Consequências regulatórias	NERC CIP, diretivas setoriais de infraestrutura crítica, HSE (Health, Safety, Environment)	LGPD/GDPR, HIPAA, PCI DSS, SOX

Tabela 2 – Diferenças entre o gerenciamento de vulnerabilidades em ambientes Enterprise e OT/ICS

Sendo assim, aplicar as mesmas ferramentas e lógicas de segurança utilizadas em ambientes corporativos não funciona nos sistemas industriais. A realidade de OT exige abordagens próprias, que levem em conta os riscos físicos, a disponibilidade contínua e a complexidade dos ativos legados.

Além disso, o conceito de risco em OT precisa ser reformulado: não basta avaliar a severidade técnica de uma vulnerabilidade, é necessário entender **as possíveis consequências no mundo físico,** como falhas de controle, danos materiais, interrupção de processos essenciais ou riscos à vida humana.

A simples aplicação de um patch, por exemplo, pode gerar instabilidade ou parada de um sistema que não pode ser desligado. Isso cria um paradoxo: **quanto mais crítico o sistema, mais difícil sua manutenção e atualização.**

Principais desafios para o gerenciamento de vulnerabilidades em OT/ICS e estratégias de mitigação

DESAFIO ESPECÍFICO PARA INFRAESTRUTURA OT/ICS	DESCRIÇÃO DETALHADA DO DESAFIO	ESTRATÉGIAS DE MITIGAÇÃO RECOMENDADAS
Sistemas legados e fim de vida (EOL)	Hardware/software desatualizados, sem patches do fornecedor, protocolos inseguros por design, difícil integração com tecnologias de segurança modernas.	Controles compensatórios (hardening de sistemas, monitoramento de rede focado, listas de permissão de aplicações, remoção de funcionalidades desnecessárias), segmentação de rede rigorosa (isolamento de sistemas legados), planejamento de modernização/substituição a longo prazo, avaliação de soluções de patching virtual.
Restrições severas de patching e intolerância a downtime	Operações contínuas (24/7), receio de interrupções operacionais ao aplicar patches, janelas de manutenção inexistentes ou extremamente curtas, dificuldade ou impossibilidade de realizar testes adequados de patches.	Gerenciamento de patches baseado em risco (priorização extrema focada no impacto operacional), uso extensivo de controles compensatórios, exploração de patching virtual, identificação e aproveitamento de janelas de oportunidade coordenadas com a produção, adoção de soluções de patching que minimizem o risco operacional (ex: com rollback facilitado).
Protocolos de comunicação inseguros por design	Protocolos como Modbus, DNP3, IEC 104, entre outros, frequentemente sem autenticação ou criptografia nativa, tornando-os vulneráveis a interceptação, manipulação de dados e comandos, e ataques de replay.	Segmentação de rede robusta (DMZs, zonas e condutos baseados no Modelo Purdue/ISA/IEC 62443), implementação de firewalls com capacidade de inspeção profunda de pacotes (DPI) para protocolos OT, monitoramento contínuo da rede para detecção de anomalias e tráfego suspeito, uso de VPNs para proteger o tráfego OT em redes não confiáveis, e, quando possível, criptografia em camada de aplicação ou encapsulamento seguro.
Falta de visibilidade de rede e inventário de ativos	Dificuldade em identificar todos os ativos OT presentes na rede, suas configurações, versões de firmware, e os padrões de comunicação entre eles; existência de "shadow OT" (dispositivos não documentados).	Implementação de soluções de descoberta de ativos passivas (que não interferem no tráfego) e, com cautela, ativas (seguras para OT), adoção de plataformas de monitoramento de segurança OT que criem e mantenham um inventário de ativos detalhado e atualizado, mapeamento de fluxos de dados e topologia de rede.
Convergência enterprise/OT e aumento da superfície de ataque	Conexão crescente entre redes OT (anteriormente consideradas isoladas ou "air-gapped") e Redes Enterprise, expondo os sistemas OT a ameaças e vetores de ataque provenientes da rede Enterprise.	Segmentação rigorosa e controlada entre as Redes Enterprise e Redes OT (uso de DMZs é mandatório), implementação de firewalls robustos na fronteira Enterprise/OT com políticas de acesso "least privilege", monitoramento intensivo do tráfego que cruza essa fronteira, desenvolvimento de políticas de segurança coordenadas entre as equipes de Enterprise e OT, consideração de arquiteturas Zero Trust para acesso à rede OT.
Limitações de ferramentas de segurança de TI tradicionais	Scanners de vulnerabilidade ativos podem ser disruptivos para sistemas ICS sensíveis, ferramentas baseadas em assinatura podem não reconhecer ameaças ou protocolos OT, desalinhamento com as prioridades operacionais de OT.	Adoção de ferramentas de segurança projetadas especificamente para infraestruturas OT (ex: monitoramento passivo de rede, análise comportamental de tráfego industrial, IDS/IPS para OT), avaliação de risco contextualizada para o impacto operacional em OT, integração de dados de segurança OT com plataformas SIEM/SOAR.

Tabela 3 – Principais desafios para o gerenciamento de vulnerabilidades em OT/ICS e estratégias de mitigação

As estratégias de defesa, portanto, devem ser calibradas com inteligência: **segmentação de rede, monitoramento passivo, identificação de ativos invisíveis (shadow OT), hardening de sistemas e uso de soluções não intrusivas** são parte de uma abordagem que reconhece as limitações operacionais, mas não abre mão da segurança.

O desafio é manter o controle sem interromper a operação e, para isso, o gerenciamento de vulnerabilidades precisa ser visto como **um ciclo contínuo de adaptação e melhoria.** Não basta identificar falhas. **É necessário priorizar, proteger, monitorar e responder** com velocidade e contexto.

Frameworks como o NIST CSF e as diretrizes da IEC 62443 fornecem boas bases, mas a maturidade de segurança só se constrói com investimento em processos, equipes especializadas e ferramentas ajustadas à realidade industrial.

8 A energia circula — e os riscos seguem o mesmo caminho

A digitalização acelerada da indústria trouxe ganhos de eficiência, mas também ampliou drasticamente a superfície de ataque. Ambientes OT antes isolados agora estão expostos. E quando o impacto de um ataque pode comprometer produção, segurança e continuidade, a resposta não pode ser adiada.

A segurança OT não é mais opcional. É parte da sobrevivência operacional.

Da visibilidade à ação: o que precisa mudar

As ameaças estão se tornando mais sofisticadas, enquanto muitos ambientes industriais ainda operam com ferramentas desatualizadas, pouca visibilidade e uma falsa sensação de isolamento.

O desafio hoje não é apenas técnico, é estratégico. O cenário atual exige:

- Visibilidade contínua e em tempo real de ativos e tráfego;
- Segmentação inteligente e rígida da rede, com foco em contenção;
- Monitoramento adaptativo e alerta antecipado para ameaças em OT;
- Políticas claras, baseadas em risco real, e adaptadas à criticidade da operação.

Quem não enxerga sua própria rede, já está em desvantagem.

O que fazer a partir de agora

A partir de tudo que foi explorado, algumas medidas são prioritárias e precisam deixar de ser debatidas para começar a ser executadas:

- **Segmente sua rede OT.** Não conecte ambientes críticos diretamente à rede corporativa.
- **Integre logs de ativos industriais em uma plataforma SIEM.** A detecção começa pela coleta certa.
- **Implemente controles compensatórios.** Muitos ativos legados não aceitam patching — mas podem ser protegidos com arquitetura, regras e monitoramento.
- **Avalie seu inventário de ativos agora.** Não conecte ambientes críticos diretamente à rede corporativa.
- **Quebre o sigilo entre OT, TI e segurança.** Resposta coordenada exige visão compartilhada.

A maturidade em segurança OT começa com decisões práticas.

A ISH está pronta para te apoiar

Nenhuma indústria é igual e nenhum ambiente OT é padrão. É por isso que a ISH atua de forma integrada, combinando:

☑ **Profundidade técnica com foco em resultados;**

☑ **Ferramentas de visibilidade com análise contextual;**

☑ **Arquitetura defensiva com monitoramento contínuo.**

Através do **ISH Vision,** sua empresa ganha um ecossistema de proteção e inteligência, que transforma dados em ação e reduz o tempo entre o risco e a resposta.

Sobre o Heimdall Security Research

O Heimdall Security Research é o núcleo de inteligência e pesquisa em cibersegurança da ISH. Criado para antecipar riscos, analisar ameaças emergentes e apoiar decisões estratégicas em ambientes críticos, o Heimdall atua na fronteira entre análise técnica profunda e aplicação prática para a defesa de redes OT e IT.

Com foco contínuo em **infraestruturas críticas,** o Heimdall realiza:

- ☑ **Análises técnicas de ameaças reais, campanhas e vetores ativos no Brasil e no mundo;**
- ☑ **Estudos aprofundados de vulnerabilidades, com ênfase em impacto industrial;**
- ☑ **Testes de validação e simulação de ataques, para reforçar estratégias defensivas;**
- ☑ **Publicações técnicas e relatórios estratégicos, como este que você está lendo.**

A atuação do Heimdall está integrada ao ISH Vision, fortalecendo o ciclo de proteção com dados concretos, alertas contextualizados e recomendações que nascem da realidade do campo.

Proteger infraestruturas críticas exige mais do que boas práticas. Exige conhecimento profundo sobre quem são os adversários, como se movimentam e onde atacam.

Segurança eficaz começa com inteligência confiável.

REFERÊNCIAS

Heimdall Security Research. Ameaças Cibernéticas em Ambientes ICS/OT – 2024.

CISA – Cybersecurity and Infrastructure Security Agency.

ISA/IEC 62443 – Standards for Industrial Automation and Control Systems.

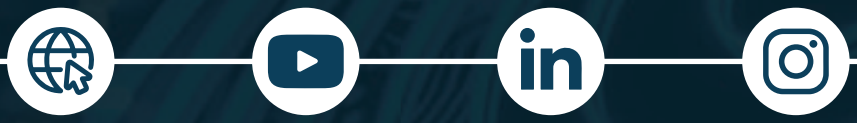
NIST Cybersecurity Framework (NIST CSF).

MITRE ATT&CK for ICS.

Relatórios de inteligência cibernética do setor privado e de segurança nacional.

A ISH pode ajudar a implementar a melhor estratégia de segurança cibernética para a sua empresa

Entre em contato com nosso time de especialistas e conheça as melhores soluções de cibersegurança do mercado



ISH | heimdall security research