
INSIGHTS DE CIBERSEGURANÇA
PARA SETORES NO BRASIL
EDIÇÃO:
RECURSOS
HÍDRICOS E
SANEAMENTO
heimdall
security research

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 Segurança cibernética é desafio para empresas de água e saneamento

A crescente digitalização dos sistemas hídricos e de saneamento os torna alvos atrativos para cibercriminosos.

Empresas estão investindo cada vez mais em automação, Internet Industrial das Coisas (IIoT) e a hiperconectividade dos sistemas, oferecendo, assim, maiores superfícies para ataques. Processos como o abastecimento, tratamento ou controle de qualidade são impensáveis hoje sem o uso de tecnologias de TI e OT.

A exploração de vulnerabilidades nessas infraestruturas críticas pode resultar em interrupções no fornecimento de água em larga escala, contaminação de fontes hídricas e até mesmo danos físicos irreparáveis às instalações.

Entre as principais ameaças cibernéticas enfrentadas estão **ransomware e APTs, phishing, vulnerabilidade de software e conectividade remota**, além de ataques à cadeia de suprimentos.

Neste e-book elaborado pela **equipe de Threat Intelligence da ISH, a Heimdall**, vamos apresentar uma análise aprofundada das ameaças cibernéticas que atingem o setor, fornecendo informações cruciais para a implementação de medidas de segurança, garantindo a continuidade das operações.

2 Principais tipos de ameaças e motivações

A diversidade de atores de ameaça, com motivações que vão desde o cibercrime até espionagem industrial, torna o setor de recursos hídricos e saneamento um alvo atrativo e lucrativo.

Embora o número de ataques relatados até o momento seja menor em comparação com outros setores, a falta de manutenção e atualizações regulares dos sistemas digitais deixam esse cenário ainda mais preocupante.

Confira duas categorias de **atores de ameaças** com foco no segmento:

CIBERCRIMINOSOS:

Podemos considerar que esses atores possuem o foco estritamente em realizar ataques do tipo ransomware, nos quais exploram vulnerabilidades em diversos sistemas e causam interrupções generalizadas no abastecimento, tratamento e distribuição de água.

ATORES DE ESTADO-NAÇÃO:

Este tipo de ator de ameaça combina operações cibernéticas e de informações políticas para realizar ataques direcionados a esses serviços. Pode ser mencionado, por exemplo, a guerra entre Ucrânia e Rússia, em que foram observados ataques para interromper setores como energia e abastecimento de água. O foco principal é causar problemas na distribuição e minar a confiança da população nessas instituições, gerando pânico e medo, atingindo, assim, alguns dos seus principais objetivos.

Atualmente, **grupos de ransomware** representam a ameaça mais imediata e lucrativa para o setor de água e saneamento. A interrupção desses serviços essenciais pode gerar grandes lucros para os atacantes e causar **danos irreparáveis à sociedade.**

No próximo tópico, confira as principais táticas e técnicas empregadas por esses e outros grupos de ameaça.

3 Conheça os grupos de cibercriminosos

Com o objetivo de fornecer insights sobre as ameaças emergentes, acompanhe uma análise de casos reais de ataques cibernéticos que impactaram o setor de recursos hídricos e saneamento.

3.1 Ransomwares

3.1.1 Ransomware LockBit

O LockBit, um dos grupos de ransomware mais proeminentes no mundo, têm se destacado pela sua capacidade de adaptação, maior capacidade de ataques e evolução desde o seu surgimento em meados de 2019, com o nome **“abcd ransomware”.**

Utilizando táticas agressivas e um modelo de negócio eficaz, o grupo se tornou uma das maiores ameaças para organizações. O sucesso do LockBit pode ser atribuído ao seu modelo de **Ransomware-as-a-Service (RaaS)**, que permite que outros cibercriminosos utilizem sua infraestrutura e ferramentas para realizar ataques, em troca de uma parte do lucro obtido.

O grupo, inclusive, já é conhecido no setor de recursos hídricos e saneamento por criptografar e exigir pagamentos para liberar a chave necessária para recuperar os arquivos criptografados.

Como já identificado em pesquisas anteriores pela Heimdall, o grupo já se envolveu com outros atores de ameaças, criando, em 2020, o que se chama de “Cartel de Ransomwares”. O cartel teria o envolvimento de outros grupos no passado, como Suncrypt, Maze, Egregor, Ragnar Locker, Ryuk e CONTI.

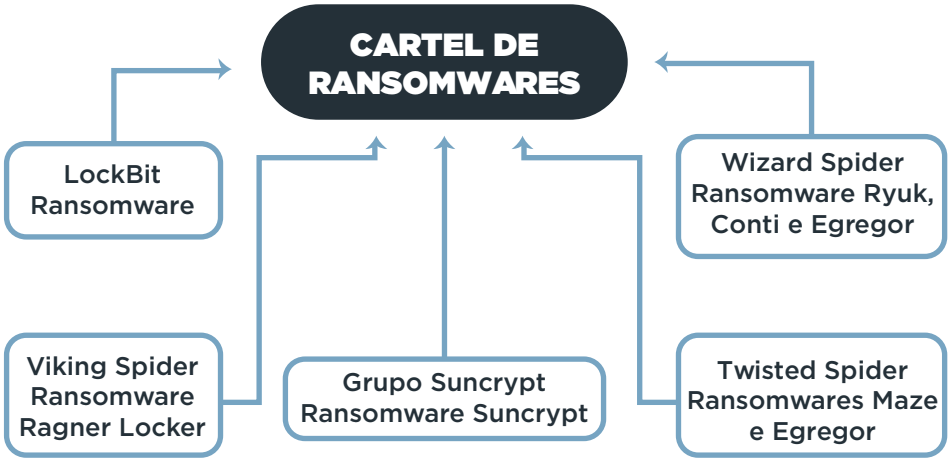

Figura 1 – Cartel de Ransomware formado por atores de ameaças.

Outro detalhe é que o grupo possui determinadas regras para os afiliados, dentre as quais destaca-se a proibição de realizar ataques a infraestruturas de saúde.

Em setembro de 2022, o grupo se envolveu em uma polêmica através de um desenvolvedor do ransomware, que teria vazado um “builder” (programa responsável por construir os arquivos maliciosos). Com isso, diversos novos grupos surgiram na sociedade utilizando desse builder e alterando apenas alguns detalhes, principalmente a marca. **A ISH Tecnologia reportou e detalhou esses fatos em um relatório próprio.**

Ao longo de sua operação, principalmente no final de 2023 e início de 2024, o LockBit teve seu site de DLS (Data Leak Site) apreendido pela polícia, prejudicando parcialmente sua operação e sua imagem.

A seguir, mencionamos algumas das principais vulnerabilidades identificadas e exploradas pelo grupo ou seus afiliados.

ID CVE	DESCRIÇÃO
CVE-2018-13379	Vulnerabilidade de path tranversal na VPN (Fortinet FortiOS Secure Sockets Layer (SSL).
CVE-2019-0708	Vulnerabilidade de execução remota de código nos serviços de RDP da Microsoft.
CVE-2020-1472	Vulnerabilidade utilizada para elevação de privilégios no Netlogon.
CVE-2021-22986	Vulnerabilidade de execução remota de código F5 BIG-IP e BIG-IQ de gerenciamento centralizado iControl REST.
CVE-2021-44228	Vulnerabilidade de execução remota de código no Apache Log4j
CVE-2023-27350	Vulnerabilidade de controle de acessos do PapperCut MF/MG.
CVE-2023-0669	Vulnerabilidade de execução remota de código no Fortra GoAnywhere Managed File Transfer (MFT).

Tabela 1 – Vulnerabilidades explorada pelo Ransomware LockBit.

3.1.2 Ransomware Cl0p

O grupo de ransomware conhecido como Clop ou Cl0p iniciou suas operações em meados de 2019, ficando conhecido por explorar vulnerabilidades para o comprometimento inicial das organizações.

Este grupo é uma variante de uma cepa de ransomware conhecida e apelidada como CryptoMix, e teria sido utilizado pela primeira vez também em 2019, entregues por meio de um ataque com motivação financeira via phishing pelos cibercriminosos rastreados como TA505.

O Cl0p é notável por suas diversas alterações durante sua operação, ou seja, está sempre modificando suas táticas, técnicas e procedimentos. Podemos mencionar, inclusive, que em meados de 2021, policiais prenderam diversos membros do grupo. Neste período, a Heimdall rastreou algumas campanhas utilizadas pelos atores do Clop.
Conforme apresentado a seguir, o grupo fez o uso de campanhas de phishing para a entrega final do ransomware.

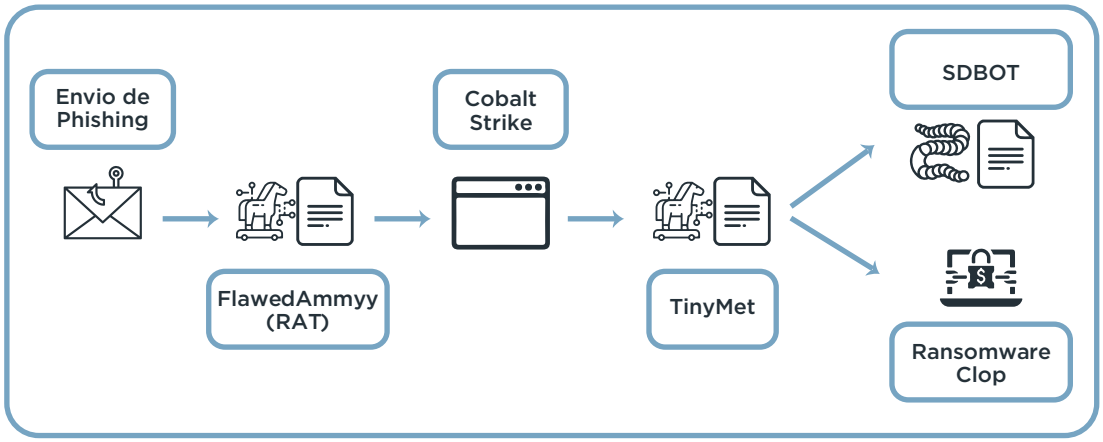

Figura 2 – Fluxo de ataque utilizando-se de phishing pelo Ransomware Cl0p.

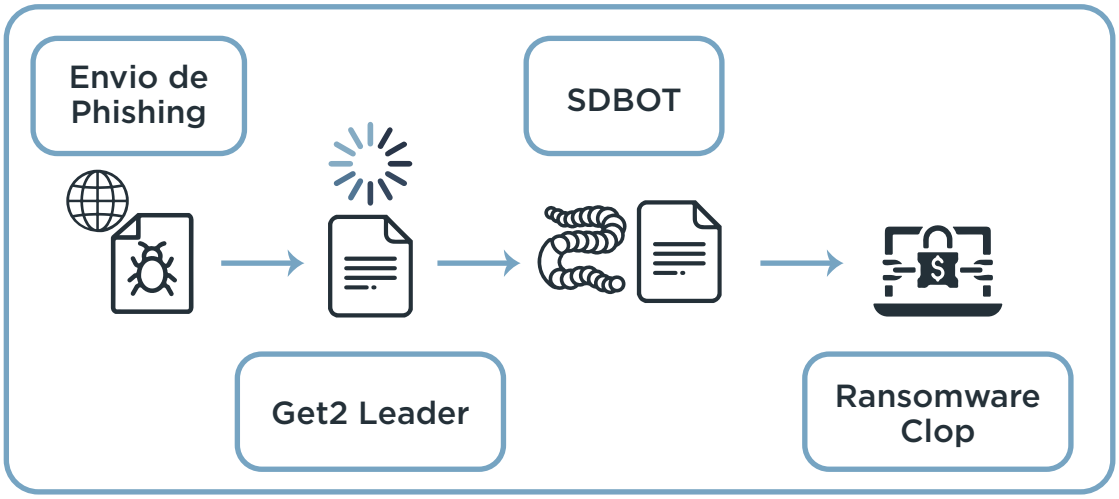

Figura 3 – Fluxo de ataque 2 utilizando-se de phishing pelo Ransomware Cl0p.

O grupo também é conhecido por explorar vulnerabilidades. Na imagem abaixo, é possível identificar esse fluxo de exploração pelo Cl0p.

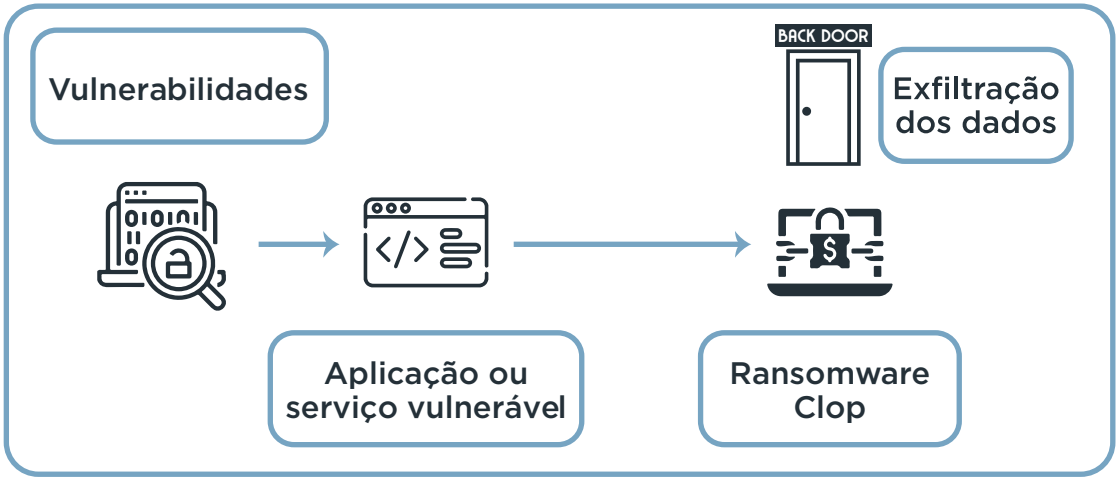

Figura 4 – Fluxo de exploração de vulnerabilidade resultando em criptografia do Clop.

ID CVE	DESCRIÇÃO
CVE-2021-2701	Injeção de SQL por meio de cabeçalho host criado.
CVE-2021-27102	Execução de comandos no sistema operacional por meio de uma chamada de serviços da web local.
CVE-2021-27103	SSRF por meio de uma solicitação POST criada.
CVE-2021-27104	Execução de comandos no sistema operacional por meio de uma solicitação POST criada.
CVE-2021-35211	Possibilidade de execução remota de código (RCE).
CVE-2022-41080	Vulnerabilidade elevação de privilégio.
CVE-2023-27350	Permite que os atores de ameaças realizem “by-pass” em autenticações.
CVE-2023-34362	Vulnerabilidade de injeção de SQL no aplicativo da Web.
CVE-2023-0669	Injeção de comandos pré-autenticado que pode ser controlado pelo ator de ameaça.

Tabela 2 – Vulnerabilidades explorada pelo Ransomware Cl0p.

3.2 Atores de Estado-Nação

3.2.1 Cyber Av3ngers (Irã)

O grupo de atores autodenominado **“Cyber Av3ngers”**, supostamente ligado ao Corpo da Guarda Revolucionária Islâmica do Irã (IRGC), ficou conhecido por focar em ataques a infraestruturas críticas, especialmente nos EUA e em Israel. O grupo tem como alvo principal sistemas SCADA fabricados em Israel, mas também utilizados em outros países.

Figura 5 – Dispositivo afetado pelo grupo “Cyber Av3ngers”.

Este grupo pode ser considerado um ator de Ameaça Persistente Avançada (APT), já que realiza a exploração de vulnerabilidades em dispositivos conectados à internet. O grupo emergiu em meio ao conflito entre Israel e Hamas, e seus primeiros ataques foram contra sistemas ferroviários e instalações de tratamento de água em Israel.

Figura 6 – Postagem no grupo do telegram do Cyber Av3ngers focando sistemas de água.

Em meados de dezembro de 2023, a CISA chegou a publicar um aviso sobre atores afiliados ao IRGC explorando PLCs em diversos setores, incluindo o setor de recursos hídricos e saneamento nos EUA. Os atores envolvidos deixam uma mensagem no dispositivo afetado: **“You have been hacked, down with Israel. Every equipment ‘made in Israel’ is CyberAv3ngers legal target.”**

Os dispositivos comprometidos foram expostos publicamente à internet com senhas padrão e na porta TCP 20256. Em 11 de dezembro, a CVE-2023-6448 foi atribuída para tratar das senhas padrão. Esses ataques realizados pelo grupo demonstram um risco significativo para este setor. Ao visar dispositivos conectados à internet com vulnerabilidades exploráveis, os atores podem realizar ataques e alcançar seus objetivos.

4 Indicadores de Comprometimentos

Exemplos de indicadores vinculados aos atores de ameaças em questão:

	Indicadores de compromisso do artefato – Ransomware Lockbit
md5:	7a83a738db05418c0ae6795b317a45f9
sha1:	bbd1c1fe4a01b698963c28a2231c33d70338014c
sha256:	1520e4cb2748aa5725d8b6c242ff 6cf365f6672db35df2745c920ed228666317

Tabela 3 – Indicadores de Compromissos de artefatos do Ransomware LockBit

	Indicadores de compromisso do artefato – Cyber Av3ngers
md5:	ba284a4b508a7abd8070a427386e93e0
sha1:	66ae21571faee1e258549078144325dc9dd60303
sha256:	440b5385d3838e3f6bc21220caa83b65cd5f 3618daea676f271c3671650ce9a3

Tabela 4 – Indicadores de Compromissos de artefatos vinculado ao Cyber Av3ngers

	Indicadores de compromisso do artefato – Ransomware Clop
md5:	31e0439e6ef1dd29c0db6d96bac59446
sha1:	46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5
sha256:	09d6dab9b70a74f61c41eaa485b37de9a40c86 b6d2eae7413db11b4e6a8256ef

Tabela 5 – Indicadores de Compromissos de artefatos do Ransomware Clop

5 Soluções para sua segurança cibernética

A infraestrutura de TI está cada vez mais conectada a sistemas de controle automatizados, drones, sensores e dispositivos IoT.

Nesse contexto, a aplicação de soluções do ISH Vision pode ser uma estratégia eficaz para mitigar ameaças cibernéticas. Tal metodologia se divide em:

1. **GERENCIAMENTO DE DETECÇÃO E RESPOSTA (SIEM/MDR):** envolve a criação de uma visão de longo alcance do ambiente digital, com monitoramento contínuo e detecção avançada de ameaças. Ele detecta ataques antes que causem danos, investiga incidentes e aplica políticas personalizadas para fortalecer a segurança;

2. **DETECÇÃO E RESPOSTA EM ENDPOINTS (EDR):** fornece alta visibilidade em todos os endpoints do parque tecnológico, detectando ameaças potenciais por meio de machine learning e análise comportamental, oferecendo respostas a incidentes;

3. **DETECÇÃO E RESPOSTA EM REDES (NDR):** realiza a detecção no tráfego de rede com base na análise de protocolos e conteúdo transferido, extraindo arquivos de seções monitoradas.

Além dessas ferramentas, é importante integrar uma solução eficaz de OT (Tecnologia Operacional), como o **Vision OT.** Ele oferece funcionalidades projetadas para melhorar a segurança cibernética em infraestruturas críticas como água e saneamento, como:

1 VISIBILIDADE DE ATIVOS E REDE:

Permite a descoberta automática e o gerenciamento de inventário de ativos de OT, IoT e TI, fornecendo visibilidade completa da rede e dos dispositivos conectados, o que é essencial para entender o ambiente operacional e identificar possíveis vulnerabilidades;

2 DETECÇÃO DE AMEAÇAS E RESPOSTA:

Utiliza tecnologias avançadas, incluindo inteligência artificial, para detectar ameaças e anomalias em tempo real, proporcionando uma resposta rápida a incidentes cibernéticos e ajudando a mitigar riscos antes que possam causar danos significativos;

4 GESTÃO DE VULNERABILIDADES E RISCOS:

Ajuda na identificação e priorização de vulnerabilidades nos ativos de OT e IoT, facilitando a gestão de riscos e a implementação de medidas de segurança adequadas para a proteção contra ataques cibernéticos;

5 MONITORAMENTO CONTÍNUO DA REDE:

Fornece monitoramento contínuo da rede para detecção comportamentos suspeitos e violações de segurança, permitindo uma vigilância constante sobre o ambiente;

6 CONFORMIDADE E PADRÕES DE SEGURANÇA:

Auxilia na manutenção da conformidade com padrões e regulamentações de segurança relevantes, como ISA/IEC 62443, NERC CIP, NIS2 Directive, SEC Cybersecurity Rules e TSA Security Directives, garantindo que as práticas de segurança estejam alinhadas com as exigências do setor.

Empresas especializadas em cibersegurança podem **facilitar a implementação**, **otimização e gerenciamento da solução de segurança**, garantindo que se possam maximizar o valor e a eficácia de estratégias de segurança cibernética em OT e IoT.

Medidas como essas não apenas protegem os ativos e dados, mas também asseguram que o setor de recursos hídricos e saneamento seja capaz de operar eficazmente em um ambiente cada vez mais digital.

6 Como manter sua organização protegida

Além das **soluções do ISH Vision**, para elevar ainda mais a maturidade em segurança cibernética do setor de recursos hídricos e de saneamento, recomendamos as seguintes medidas de proteção contra ataques como ransomware e ações de grupos como o **Cyber Av3nger:**

- Implemente um plano de recuperação na empresa, mantenha múltiplas cópias de dados sensíveis ou proprietários e servidores em um local fisicamente separado, segmentado e seguro, como por exemplo, em disco rígido, dispositivo de armazenamento ou na nuvem;
- Exija que todas as contas com login e senha (contas de serviço, contas de administrador e contas de administrador de domínio) cumpram os padrões do NIST. Além disso, solicite que os funcionários usem senhas longas e considere não exigir alterações de senha recorrentes, pois isso pode enfraquecer a segurança;
- Revise controladores de domínio, servidores, estações de trabalho e diretórios ativos para identificar contas novas e/ou não reconhecidas;
- Implemente autenticação multifator para todos os serviços, principalmente para correio eletrônico, redes privadas virtuais e contas que acessam sistemas críticos;
- Audite contas de usuário com privilégios administrativos e configure controles de acesso de acordo com o princípio do menor privilégio;

- Implemente acesso baseado em tempo para contas definidas no nível de administrador e superior;
- Mantenha todos os sistemas operacionais, software e firmware atualizados. A atualização recorrente é uma das medidas mais eficientes e econômicas que uma organização pode tomar para minimizar sua exposição a ameaças de segurança cibernética;
- Segmente redes para evitar a propagação de ransomware. Essa medida pode ajudar a controlar os fluxos de tráfego entre várias sub-redes, restringindo o movimento lateral dos adversários;
- Identifique, detecte e investigue atividades anormais e potenciais travessias de ransomware usando uma ferramenta de monitoramento de rede. Filtre o tráfego de rede para impedir que origens desconhecidas ou não confiáveis acessem serviços remotos em sistemas internos;
- Instale, atualize regularmente e ative a detecção em tempo real de software antivírus em todos os hosts;
- Desative portas não utilizadas;
- Considere adicionar um banner de e-mail para mensagens recebidas de fora da sua organização e desative hiperlinks em e-mails recebidos;
- Desative atividades e permissões de linha de comando e script;
- Mantenha backups offline de dados e realize regularmente backup e restauração; Assegure-se de que todos os dados de backup sejam criptografados, imutáveis e cubram toda a infraestrutura de dados da organização;

Para se defender das atividades dos CyberAv3ngers, as organizações de infraestrutura crítica devem implementar diversas medidas de segurança cibernética. Isso inclui a implementação da autenticação multifator (MFA), o uso de firewalls ou VPNs para acesso remoto, a criação de backups robustos usando a estratégia 3-2-1 recomendada pela CISA (três cópias dos dados: uma de produção e duas de backup, em duas mídias diferentes, com uma cópia externa para recuperação de desastres) e, por fim, a manutenção dos dispositivos PLC atualizados.

7 Construindo um setor mais resiliente e eficaz

A segurança cibernética no setor de água e saneamento não é mais uma opção, mas sim uma necessidade. Ataques cibernéticos, como dos grupos LockBit, Cl0p e Cyber Av3ngers, representam uma ameaça crescente e sofisticada, capaz de interromper o fornecimento de água potável e comprometer a saúde pública.

Essas ameaças evoluem rapidamente, exigindo que as empresas do setor adotem medidas de segurança proativas e robustas. Ao compreender as táticas, técnicas e procedimentos utilizados pelos atacantes, é possível fortalecer as defesas, minimizar riscos e garantir a continuidade dos serviços essenciais.

É preciso uma revisão dos procedimentos das empresas, para estabelecer uma governança adequada e implementar políticas para apoiar os controles técnicos.

AUTORES

Caique Barqueta
Especialista em Inteligência de Ameaças

Ismael Rocha
Analista de Inteligência de Ameaças Sênior

REFERÊNCIAS

Heimdall by ISH Tecnologia

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