# Atestado de Capacidade Técnica

Fundação Cesgranrio, com sede na Rua Santa Alexandrina, número 1011, CEP 20.261-903, Bairro Rio Comprido, Rio de Janeiro/RJ, regularmente inscrita no CNPJ n.º 42.270.181/0001-16, atesta para os devidos fins que a empresa CLAVIS BBR CONSULTORIA EM INFORMATICA S.A., regularmente inscrita no CNPJ n.º 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades e Cyber Threat Intelligence, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contrato n.º N4382 e seus termos aditivos**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação e GRC – Governança, Risco e Compliance - com foco na LGPD (Lei Geral de Proteção de Dados Pessoais), além de consultoria na área de Desenvolvimento Seguro e Suporte Técnico Presencial. Licenças do software relacionado ao serviço (Plataforma Clavis).

**Vigência**: de 31 de janeiro de 2020 até o presente.

**Descrição da Plataforma de Cibersegurança:**

Dentre os recursos disponibilizados por meio de subscrição da plataforma, destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (Cyber Threat Intelligence), com mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Gestão de Vulnerabilidades
- Gestão de Superfície de Ataques
- Inteligência contra Ameaças Cibernéticas
- Segurança Ofensiva / Testes de Penetração
- Segurança da Nuvem (Cloud Security)
- Governança, Risco e Conformidade em Segurança da Informação
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 06 de janeiro de 2025

_____

Wesley Tenório
Gerente de Desenvolvimento
wesley@cesgranrio.org.br
+55 (21) 96480-6689

# AtestadoCapacidadeTecnica-Cesgranrio-v2.docx.pdf

Documento número #48429d0b-b514-4630-83c3-9a52282962b3

**Hash do documento original (SHA256):** 27d73f6d379e96e4fa6c8b7b1a18b2ec5d96250b4f7ba49786a5191236b593fb

## Assinaturas

**Wesley Tenório**
CPF: 097.847.617-42
Assinou em 07 jan 2025 às 09:55:42

## Log

| | |
|---|---|
| 06 jan 2025, 18:07:22 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número 48429d0b-b514-4630-83c3-9a52282962b3. Data limite para assinatura do documento: 05 de fevereiro de 2025 (18:07). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 06 jan 2025, 18:08:43 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: wesley@cesgranrio.org.br para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Wesley Tenório. |
| 07 jan 2025, 09:55:42 | Wesley Tenório assinou. Pontos de autenticação: Token via E-mail wesley@cesgranrio.org.br. CPF informado: 097.847.617-42. IP: 179.218.17.182. Componente de assinatura versão 1.1088.0 disponibilizado em https://app.clicksign.com. |
| 07 jan 2025, 09:55:43 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 48429d0b-b514-4630-83c3-9a52282962b3. |

**Documento assinado com validade jurídica.**
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 48429d0b-b514-4630-83c3-9a52282962b3, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

# Atestado de Capacidade Técnica

FULL NINE DIGITAL CONSULTORIA LTDA, com sede na Rua Vereador Walter Borges, 439, Apt. 301, Campinas, São José - SC, CEP 88101-030, regularmente inscrita no CNPJ n.º 30.120.829/0001-99, atesta para os devidos fins que a empresa CLAVIS BBR CONSULTORIA EM INFORMATICA S.A., regularmente inscrita no CNPJ n.º 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contratos n.º N9807 e N33228**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação (SOC).

**Vigência**: de 17 de maio de 2022 até o presente.

**Descrição da Plataforma de Cibersegurança:**

A Plataforma de Cibersegurança é executada em ambiente próprio da Clavis e opera na modalidade SaaS (Software as a Service). Dentre os recursos disponibilizados por meio de subscrição da plataforma, destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (Cyber Threat Intelligence), com mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Gestão de Vulnerabilidades
- Segurança Ofensiva / Testes de Penetração
- Governança, Risco e Conformidade em Segurança da Informação
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

**Equipe Técnica**

As soluções e serviços estão sob a responsabilidade técnica do Diretor Raphael Machado, Doutor em Engenharia de Sistemas e Computação, sócio-fundador da Clavis com mais de 20 anos de experiência no mercado de cibersegurança.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 08 de janeiro de 2025

_____

Rafael Souza
CTO
rafaelsouza@conectala.com.br
+55 (21) 98125-6792

# AtestadoCapacidadeTecnica-Conecta lá.docx.pdf

Documento número #b48f3df2-b610-4ab5-90b9-20f2d9cee94b

**Hash do documento original (SHA256):** b053567ee1f3f3f5902d6a9a757eaf95f6a1f272550d5ca1806c9714d2548e0f

## Assinaturas

**Rafael Souza**
CPF: 057.436.817-59
Assinou em 09 jan 2025 às 09:03:07

## Log

| | |
|---|---|
| 08 jan 2025, 17:08:53 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número b48f3df2-b610-4ab5-90b9-20f2d9cee94b. Data limite para assinatura do documento: 07 de fevereiro de 2025 (17:08). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 08 jan 2025, 17:09:40 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: rafaelsouza@conectala.com.br para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Rafael Souza. |
| 09 jan 2025, 09:03:07 | Rafael Souza assinou. Pontos de autenticação: Token via E-mail rafaelsouza@conectala.com.br. CPF informado: 057.436.817-59. IP: 186.223.179.160. Componente de assinatura versão 1.1091.0 disponibilizado em https://app.clicksign.com. |
| 09 jan 2025, 09:03:08 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número b48f3df2-b610-4ab5-90b9-20f2d9cee94b. |

# Atestado de Capacidade Técnica

ELOGROUP CONSULTING LTDA, com sede na Rua da Quitanda, 60 - 3° andar - Centro, Rio de Janeiro - RJ, CEP 20011-030, regularmente inscrita no CNPJ n.º 30.819.292/0001-50, atesta para os devidos fins que a empresa CLAVIS BBR CONSULTORIA EM INFORMATICA S.A., regularmente inscrita no CNPJ n.º 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contrato n.º N10150**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação (SOC) e GRC – Governança, Risco e Compliance.

**Vigência**: de 19 de maio de 2022 até o presente.

**Descrição da Plataforma de Cibersegurança:**

Dentre os recursos disponibilizados por meio de subscrição da plataforma, destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (Cyber Threat Intelligence), com mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Gestão de Vulnerabilidades
- Gestão de Superfície de Ataques
- Inteligência contra Ameaças Cibernéticas
- Threat hunting
- Auditorias Técnicas / Assesments
- Segurança Ofensiva / Testes de Penetração
- Postura de Segurança na Nuvem
- Conscientização, Comportamento e Cultura
- Governança, Risco e Conformidade em Segurança da Informação
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

**Equipe Técnica**

As soluções e serviços estão sob a responsabilidade técnica do Diretor Raphael Machado, Doutor em Engenharia de Sistemas e Computação, sócio-fundador da Clavis com mais de 20 anos de experiência no mercado de cibersegurança.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 08 de janeiro de 2025

_____

João Manoel Chagas
Controladoria
joao.chagas@elogroup.com.br
+55 (21) 99624-9614

# AtestadoCapacidadeTecnica-EloGroup.docx.pdf

Documento número #16603b05-ae4e-4e5d-ae8a-03739fced10d

**Hash do documento original (SHA256):** bab7616b5754711638eb1e3bc2b33be809963bcd2ac6c0d44ba1d3c553021826

## Assinaturas

**João Manoel Chagas**
CPF: 092.671.887-80
Assinou em 10 jan 2025 às 14:44:11

## Log

| | |
|---|---|
| 08 jan 2025, 17:06:21 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número 16603b05-ae4e-4e5d-ae8a-03739fced10d. Data limite para assinatura do documento: 07 de fevereiro de 2025 (17:06). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 08 jan 2025, 17:08:07 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: joao.chagas@elogroup.com.br para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo João Manoel Chagas. |
| 10 jan 2025, 14:44:11 | João Manoel Chagas assinou. Pontos de autenticação: Token via E-mail joao.chagas@elogroup.com.br. CPF informado: 092.671.887-80. IP: 200.172.62.242. Componente de assinatura versão 1.1093.0 disponibilizado em https://app.clicksign.com. |
| 10 jan 2025, 14:44:12 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 16603b05-ae4e-4e5d-ae8a-03739fced10d. |

**Documento assinado com validade jurídica.**
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 16603b05-ae4e-4e5d-ae8a-03739fced10d, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

# Atestado de Capacidade Técnica

**INGRESSO.COM LTDA**, com sede na Rua da Quitanda, número 86, 9º andar, bairro Centro, CEP 20091-005, Rio de Janeiro - RJ, regularmente inscrita no CNPJ n.º 00.860.640/0001-71, atesta para os devidos fins que a empresa CLAVIS BBR CONSULTORIA EM INFORMATICA S.A., regularmente inscrita no CNPJ n.º 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades e Cyber Threat Intelligence, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contrato n.º N151 e seus Termos Aditivos**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação, com acesso e utilização, pela INGRESSO.COM da plataforma desenvolvida pela CLAVIS denominada OCTOPUS. A plataforma OCTOPUS tem como objetivo possibilitar a integração de dados relevantes à segurança, a correlação de eventos para identificação de incidentes de segurança e a retenção de dados por questões de conformidade ou com vistas a potenciais ações de análise, ou investigação forense.

**Vigência**: de 31 de janeiro de 2018 até o presente

**Descrição da Plataforma de Cibersegurança:**

A Plataforma de Cibersegurança é executada em ambiente próprio da Clavis e opera na modalidade SaaS (Software as a Service). Dentre os recursos disponibilizados por meio de subscrição da plataforma, destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (Cyber Threat Intelligence), com mecanismo de captura

automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Inteligência contra Ameaças Cibernéticas
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 10 de janeiro de 2025

_____

Eduardo Tavares
Gerente de Segurança da Informação
eduardo.tavares@ingresso.com
+55 (21) 987442221

# AtestadoCapacidadeTecnica-Ingresso.docx.pdf

Documento número #540a6bd6-c9f0-4e95-b77c-583bd32e2cca

**Hash do documento original (SHA256):** 879a6ee82acbdabfaadb99029694866e1ae3e1781446b5ad7ba2efed521f488e

## Assinaturas

**Eduardo Tavares**
CPF: 090.554.037-92
Assinou em 10 jan 2025 às 15:52:45

## Log

| | |
|---|---|
| 10 jan 2025, 15:42:58 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número 540a6bd6-c9f0-4e95-b77c-583bd32e2cca. Data limite para assinatura do documento: 09 de fevereiro de 2025 (15:42). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 10 jan 2025, 15:44:29 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: eduardo.tavares@ingresso.com para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Eduardo Tavares. |
| 10 jan 2025, 15:52:45 | Eduardo Tavares assinou. Pontos de autenticação: Token via E-mail eduardo.tavares@ingresso.com. CPF informado: 090.554.037-92. IP: 186.213.80.75. Componente de assinatura versão 1.1093.0 disponibilizado em https://app.clicksign.com. |
| 10 jan 2025, 15:52:46 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 540a6bd6-c9f0-4e95-b77c-583bd32e2cca. |

**Documento assinado com validade jurídica.**
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 540a6bd6-c9f0-4e95-b77c-583bd32e2cca, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

# Atestado de Capacidade Técnica

M.I Montreal Informática S.A., com sede na Avenida Professor Magalhães Penido, número 77, CEP 31.270-383, bairro Aeroporto, Belo Horizonte/MG, regularmente inscrita no CNPJ n.º 42.563.692/0001-26, atesta para os devidos fins que a empresa CLAVIS BBR CONSULTORIA EM INFORMATICA S.A., regularmente inscrita no CNPJ n.º 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades e Cyber Threat Intelligence, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contrato n.º N9366**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação (SOC).

**Vigência**: de 07 de março de 2022 até o presente.

**Descrição da Plataforma de Cibersegurança:**

A Plataforma de Cibersegurança é executada em ambiente próprio da Clavis e opera na modalidade SaaS (Software as a Service). Dentre os recursos disponibilizados por meio de subscrição da plataforma, destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (CyberThreat Intelligence), com mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Gestão de Vulnerabilidades
- Gestão de Superfície de Ataques
- Inteligência contra Ameaças Cibernéticas
- Segurança Ofensiva / Testes de Penetração
- Segurança da Nuvem (Cloud Security)
- Governança, Risco e Conformidade em Segurança da Informação
- Conscientização, Comportamento e Cultura
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

**Equipe Técnica**

As soluções e serviços estão sob a responsabilidade técnica do Diretor Raphael Machado, Doutor em Engenharia de Sistemas e Computação, sócio-fundador da Clavis com mais de 20 anos de experiência no mercado de cibersegurança.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 06 de janeiro de 2025

_____

Sandro Ventura
Gerente de TI
sandro.ventura@montreal.com.br
+55 (21) 98868-6444

# AtestadoCapacidadeTecnica-Montreal.docx.pdf

Documento número #1b2e69fe-9644-4516-aa2f-2ad48c6e8414

**Hash do documento original (SHA256):** 5835df896f54f0400077574b7e269ff6d53f1b700179c5955cf0dcb041f43b87

## Assinaturas

**Sandro Luis Ventura Neto**
CPF: 008.405.387-90
Assinou em 06 jan 2025 às 17:52:42

## Log

| | |
|---|---|
| 06 jan 2025, 17:15:38 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número 1b2e69fe-9644-4516-aa2f-2ad48c6e8414. Data limite para assinatura do documento: 05 de fevereiro de 2025 (17:15). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 06 jan 2025, 17:17:10 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: sandro.ventura@montreal.com.br para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Sandro Luis Ventura Neto. |
| 06 jan 2025, 17:52:42 | Sandro Luis Ventura Neto assinou. Pontos de autenticação: Token via E-mail sandro.ventura@montreal.com.br. CPF informado: 008.405.387-90. IP: 177.131.149.2. Componente de assinatura versão 1.1087.0 disponibilizado em https://app.clicksign.com. |
| 06 jan 2025, 17:52:42 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 1b2e69fe-9644-4516-aa2f-2ad48c6e8414. |

**Documento assinado com validade jurídica.**
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 1b2e69fe-9644-4516-aa2f-2ad48c6e8414, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

# Atestado de Capacidade Técnica

PRAVALER S.A., com sede na Avenida Dra. Ruth Cardoso no 7221 - 21º andar, Pinheiros, São Paulo - SP, regularmente inscrita no CNPJ n.º 04.531.065/0001-14, atesta para os devidos fins que a empresa CLAVIS BBR CONSULTORIA EM INFORMATICA S.A., regularmente inscrita no CNPJ n.º 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades e Cyber Threat Intelligence, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contrato n.º N10128 e seus Termos Aditivos**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação (SOC) e GRC – Governança, Risco e Conformidade.

**Vigência**: de 26 de maio de 2022 até o presente.

**Descrição da Plataforma de Cibersegurança:**

Dentre os recursos disponibilizados por meio de subscrição da plataforma, destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (Cyber Threat Intelligence), com mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Gestão de Vulnerabilidades
- Gestão de Superfície de Ataques
- Inteligência contra Ameaças Cibernéticas
- Segurança Ofensiva / Testes de Penetração
- Governança, Risco e Conformidade em Segurança da Informação
- Conscientização, Comportamento e Cultura
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

**Equipe Técnica**

As soluções e serviços estão sob a responsabilidade técnica do Diretor Raphael Machado, Doutor em Engenharia de Sistemas e Computação, sócio-fundador da Clavis com mais de 20 anos de experiência no mercado de cibersegurança.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 08 de janeiro de 2025

_____

Marcos Pereira
Gerente de SI
marcos.pereira@pravaler.com.br
+55 (21) 96880-2159

# AtestadoCapacidadeTecnica-Pravaler.docx.pdf

Documento número #3f1d5716-31bf-4529-a4af-fb6d4d3e7b0e

**Hash do documento original (SHA256):** bd753468dab054134836147d44a0c0c157819cb1ba38eda69019f833b512ce5c

## Assinaturas

**Marcos Paulo Castro Pereira**
CPF: 140.353.047-51
Assinou em 09 jan 2025 às 19:21:43

## Log

| | |
|---|---|
| 08 jan 2025, 17:13:39 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número 3f1d5716-31bf-4529-a4af-fb6d4d3e7b0e. Data limite para assinatura do documento: 07 de fevereiro de 2025 (17:13). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 08 jan 2025, 17:16:41 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: marcos.pereira@pravaler.com.br para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Marcos Paulo Castro Pereira. |
| 09 jan 2025, 19:21:43 | Marcos Paulo Castro Pereira assinou. Pontos de autenticação: Token via E-mail marcos.pereira@pravaler.com.br. CPF informado: 140.353.047-51. IP: 104.28.63.99. Componente de assinatura versão 1.1091.0 disponibilizado em https://app.clicksign.com. |
| 09 jan 2025, 19:21:44 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 3f1d5716-31bf-4529-a4af-fb6d4d3e7b0e. |

**Documento assinado com validade jurídica.**
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 3f1d5716-31bf-4529-a4af-fb6d4d3e7b0e, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

# Atestado de Capacidade Técnica

Senior Sistemas SA, com sede em Rua São Paulo, 825, CEP 89012-001, Bairro Victor Konder, Blumenau, SC, regularmente inscrita no CNPJ nº 80.680.093-0001/81, atesta para os devidos fins que a empresa CLAVIS BBR CONSULTORIA EM INFORMATICA S.A., regularmente inscrita no CNPJ nº 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades e Cyber Threat Intelligence, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contrato N7934 e seus Termos Aditivos**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação e GRC – Governança, Risco e Compliance. Licenças do software relacionado ao serviço (Plataforma Clavis).

**Vigência**: 18 de maio de 2022 até o presente.

**Descrição da Plataforma de Cibersegurança:**

A Plataforma de Cibersegurança é executada em ambiente próprio da Clavis e opera na modalidade SaaS (Software as a Service). Dentre os recursos disponibilizados por meio de subscrição da plataforma de cibersegurança da Clavis destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (Cyber Threat Intelligence), com mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Gestão de Vulnerabilidades
- Gestão de Superfície de Ataque
- Inteligência contra Ameaças Cibernéticas
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 06 de janeiro de 2025

_____

Alan Ten Caten
IT Corporate Executive Manager
alan.caten@senior.com.br
+55 (41) 9669.3422 | +55 (47) 98829.2806

# AtestadoCapacidadeTecnica-Senior.docx.pdf

Documento número #e0e15b18-7603-47e7-ac04-4e1ea667e633

**Hash do documento original (SHA256):** 0d6df02392e613be112518dd206f53de8ada3b73cea9f32dac752dc5bc6737ed

## Assinaturas

**Alan Ten Caten**
CPF: 027.732.430-05
Assinou em 06 jan 2025 às 15:50:08

## Log

| | |
|---|---|
| 06 jan 2025, 15:38:56 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número e0e15b18-7603-47e7-ac04-4e1ea667e633. Data limite para assinatura do documento: 05 de fevereiro de 2025 (15:38). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 06 jan 2025, 15:42:01 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: alan.caten@senior.com.br para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Alan Ten Caten. |
| 06 jan 2025, 15:50:08 | Alan Ten Caten assinou. Pontos de autenticação: Token via E-mail alan.caten@senior.com.br. CPF informado: 027.732.430-05. IP: 201.159.186.248. Componente de assinatura versão 1.1087.0 disponibilizado em https://app.clicksign.com. |
| 06 jan 2025, 15:50:09 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número e0e15b18-7603-47e7-ac04-4e1ea667e633. |

**Documento assinado com validade jurídica.**
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº e0e15b18-7603-47e7-ac04-4e1ea667e633, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

# Atestado de Capacidade Técnica

**TARGET INSTITUICAO DE PAGAMENTO E SECURITIZADORA DE CREDITOS S.A**, com sede na Av. Embaixador Abelardo Bueno, 1111, Ed. Seletto, Bloco 2, sala 204 – Barra da Tijuca - Rio de Janeiro - RJ, CEP 22775-039, regularmente inscrita no CNPJ n.º 14.821.124/0001-42, atesta para os devidos fins que a empresa **CLAVIS BBR CONSULTORIA EM INFORMATICA S.A.**, regularmente inscrita no CNPJ n.º 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades e Cyber Threat Intelligence, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contrato n.º N6665 e seus Termos Aditivos**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação (SOC).

**Vigência**: de 17 de março de 2021 até o presente.

**Descrição da Plataforma de Cibersegurança:**

Dentre os recursos disponibilizados por meio de subscrição da plataforma, destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (Cyber Threat Intelligence), com mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Gestão de Vulnerabilidades
- Gestão de Superfície de Ataques
- Inteligência contra Ameaças Cibernéticas
- Threat hunting
- Segurança Ofensiva / Testes de Penetração
- Auditorias Técnicas / Assesments
- Postura de Segurança na Nuvem
- Conscientização, Comportamento e Cultura
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

**Equipe Técnica**

As soluções e serviços estão sob a responsabilidade técnica do Diretor Raphael Machado, Doutor em Engenharia de Sistemas e Computação, sócio-fundador da Clavis com mais de 20 anos de experiência no mercado de cibersegurança.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 08 de janeiro de 2025

_____

Renato Santos
Coordenador de TI
renato.santos@targetbank.com.br
+55 (21) 98555-0190

# AtestadoCapacidadeTecnica-Target.docx.pdf

Documento número #697259bf-1c48-4f5d-8bf6-d1ee3d74d96a

**Hash do documento original (SHA256):** 597f33d3b9e43d56927069c2a88f73e9329d21e80759d5c90c3233a5fb813277

## Assinaturas

**Renato Batista dos Santos**
CPF: 052.936.787-44
Assinou em 08 jan 2025 às 18:42:55

## Log

| | |
|---|---|
| 08 jan 2025, 17:12:13 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número 697259bf-1c48-4f5d-8bf6-d1ee3d74d96a. Data limite para assinatura do documento: 07 de fevereiro de 2025 (17:12). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 08 jan 2025, 17:13:09 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: renato.santos@targetbank.com.br para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Renato Batista dos Santos. |
| 08 jan 2025, 18:42:55 | Renato Batista dos Santos assinou. Pontos de autenticação: Token via E-mail renato.santos@targetbank.com.br. CPF informado: 052.936.787-44. IP: 177.38.101.74. Componente de assinatura versão 1.1090.0 disponibilizado em https://app.clicksign.com. |
| 08 jan 2025, 18:42:55 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 697259bf-1c48-4f5d-8bf6-d1ee3d74d96a. |

**Documento assinado com validade jurídica.**
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 697259bf-1c48-4f5d-8bf6-d1ee3d74d96a, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

# Atestado de Capacidade Técnica

Valemobi Consultoria Empresarial S.A., com sede na Avenida General Furtado Nascimento, Alto de Pinheiros, 740, 5º e 6º andares, São Paulo - SP, Brasil, CEP 05465-070, regularmente inscrita no CNPJ n.º 10.535.290/0001-21, atesta para os devidos fins que a empresa CLAVIS BBR CONSULTORIA EM INFORMATICA S.A., regularmente inscrita no CNPJ n.º 10.772.725/0001-51, mantém contrato ativo e disponibiliza uma plataforma de cibersegurança com soluções de Gestão de Eventos (SIEM), Gestão de Vulnerabilidades, prestando serviços de cibersegurança da informação, envolvendo as atividades de fornecimento de licença, suporte técnico, consultoria, operação assistida e treinamento.

**Contrato n.º N24199**

**Objeto**: Prestação de serviços de consultoria em informática, englobados na gestão de Projeto de Segurança da Informação, incluindo a realização mensal de horas de consultoria, para desempenho das atividades do Centro de Operações de Segurança da Informação (SOC).

**Vigência**: de 09 de setembro de 2021 até o presente.

**Descrição da Plataforma de Cibersegurança:**

Dentre os recursos disponibilizados por meio da plataforma, destacam-se os seguintes:

- Gestão de Eventos (SIEM - Security Information and Event Management), com possibilidade de coleta de eventos oriundos de hosts/endpoints/servidores, equipamentos de rede, tecnologias de borda, ambientes em nuvem, aplicações de software, dentre outros.

- Gestão de Ativos, Exposições e Vulnerabilidades, com recursos de conformidade ao benchmark CIS, priorização de vulnerabilidades baseados no CVSS e EPSS, e gestão de superfície de ataque.

- Inteligência Cibernética (Cyber Threat Intelligence), com mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

Todos os recursos acima descritos envolvem: Monitoramento e coleta automatizada; Geração de alertas em tempo real; Emissão de relatórios com análise de inteligência de ameaças.

**Descrição dos Serviços:**

Dentre as atividades executadas no âmbito do contrato, incluem-se:

- Suporte técnico à operação da Plataforma de Cibersegurança da Clavis
- Gestão de Vulnerabilidades
- Gestão de Superfície de Ataques
- Threat Hunting
- Governança, Risco e Conformidade em Segurança da Informação
- Auditoria e relatórios de boas práticas
- Conscientização, Comportamento e Cultura
- Treinamentos especializados em segurança da informação conforme disponíveis no catálogo da Academia Clavis.

**Equipe Técnica**

As soluções e serviços estão sob a responsabilidade técnica do Diretor Raphael Machado, Doutor em Engenharia de Sistemas e Computação, sócio-fundador da Clavis com mais de 20 anos de experiência no mercado de cibersegurança.

No mais, o desempenho da empresa na execução das atividades previstas tem atendido satisfatoriamente os objetivos, com o cumprimento a contento das obrigações contratuais.

Rio de Janeiro, 08 de janeiro de 2025

_____

Moacir Campos
Gerente de Infraestrutura
moacir.campos@valemobi.com.br
+55 (11) 98596-0132

# AtestadoCapacidadeTecnica-Valemobi.docx.pdf

Documento número #f3104d2a-aee3-4fab-85f7-2eb76a3994fe

**Hash do documento original (SHA256):** 93eb32e3e129f9a8caa08957ce195a3c46e70df9a6702674c80e357d106bc112

## Assinaturas

**Moacir Campos**
CPF: 889.095.221-00
Assinou em 10 jan 2025 às 11:53:21

## Log

| | |
|---|---|
| 08 jan 2025, 17:10:05 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf criou este documento número f3104d2a-aee3-4fab-85f7-2eb76a3994fe. Data limite para assinatura do documento: 07 de fevereiro de 2025 (17:10). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 08 jan 2025, 17:11:40 | Operador com email denise.reis@clavis.com.br na Conta 132f78cf-0b49-4ab5-b06d-053a6d4960bf adicionou à Lista de Assinatura: moacir.campos@valemobi.com.br para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Moacir Campos. |
| 10 jan 2025, 11:53:21 | Moacir Campos assinou. Pontos de autenticação: Token via E-mail moacir.campos@valemobi.com.br. CPF informado: 889.095.221-00. IP: 177.92.93.158. Localização compartilhada pelo dispositivo eletrônico: latitude -23.5526732 e longitude -46.7203345. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1093.0 disponibilizado em https://app.clicksign.com. |
| 10 jan 2025, 11:53:21 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número f3104d2a-aee3-4fab-85f7-2eb76a3994fe. |

**Documento assinado com validade jurídica.**
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

CLAVIS
segurança da informação

**SOC Clavis - Centro de Operações de Segurança com Inteligência**

# Uma visão completa do seu ambiente digital em uma plataforma única.

Com **tecnologia própria e parcerias estratégicas**,
o Centro de Operações de Segurança (SOC) da Clavis
fornece uma arquitetura de segurança adaptativa para identificação,
prevenção e resposta a ameaças cibernéticas.

## Como o SOC Clavis funciona?

O **SOC Clavis** opera por meio da correlação de dados do ambiente do cliente
e dados de **Threat Intelligence** coletados na Internet aberta

- **Threat Intel**
- **Monitoramento de segurança 24x7**
- **Gestão de vulnerabilidades**
- **Resposta a incidentes**
- **Análise de conformidade**
- **Gerenciamento da superfície de ataque**
- **Simulação de violação e ataques**
- **Programa de conscientização**

# Benefícios do SOC Clavis

Melhor
custo x benefício
do mercado

Serviços e soluções próprias
aderentes às principais
normas do mercado

Captura automatizada
de informações da Internet aberta
(Threat Intel)

Regras de correlacionamento
e inteligência personalizáveis
para o seu negócio

Centro de Operações
de Segurança certificado
ISO 27001

Buscas na surface/deep/dark web,
sites/fóruns, apps de mensagens,
redes sociais, logs, dentre outros.

Clavis SIEM

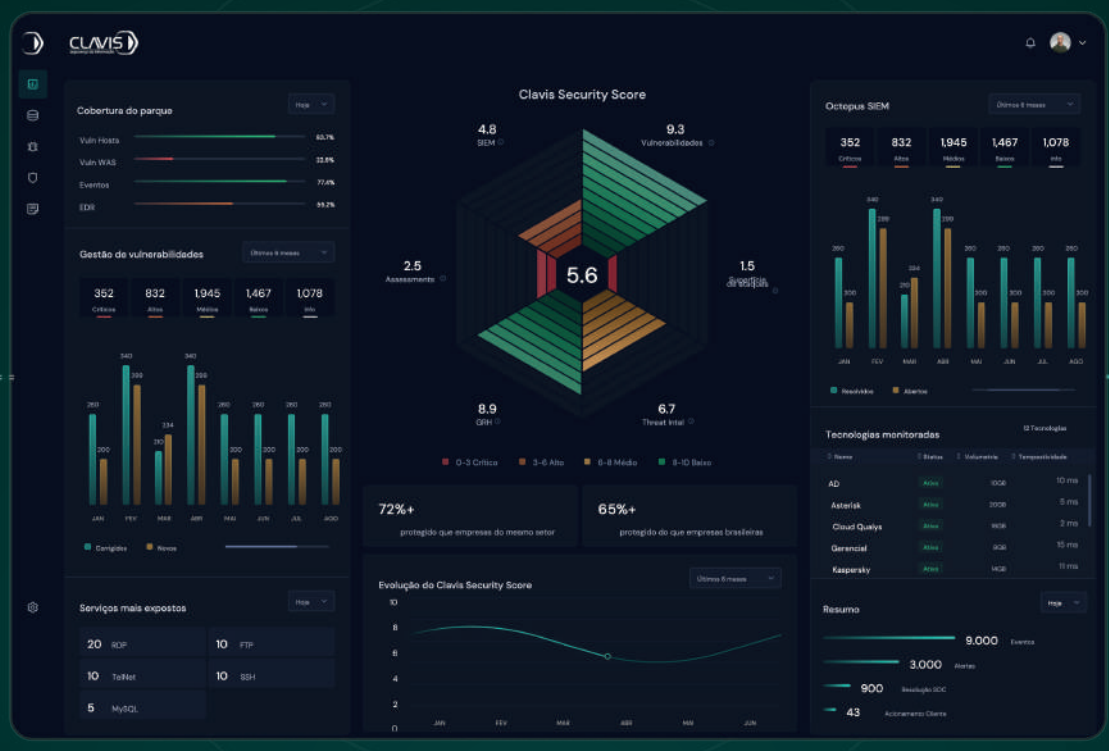
Gestão de vulnerabilidades

Análise de superfície de ataque

Threat Intel

Cloud Security

Gestão do risco humano




Visão holística

Priorização

Redução de esforço

Detecções mais assertivas

# Somos homologados pelo Ministério da Defesa Nacional

A Clavis é uma plataforma de cibersegurança, homologada como Empresa Estratégica de Defesa pelo Ministério da Defesa desde 2016, que combina uma mentalidade inovadora com a vasta experiência de mercado.

Através da combinação de uma plataforma inovadora e um time de profissionais altamente especializado a Clavis fornece à sua organização uma alternativa acessível, ágil e abrangente para cuidar da segurança das suas informações enquanto você se dedica exclusivamente ao seu negócio.

**Leia o QRcode e acesse nosso site**

MINISTÉRIO DA DEFESA
EED
EMPRESA ESTRATÉGICA DE DEFESA

MINISTÉRIO DA DEFESA
PED
PRODUTO ESTRATÉGICO DE DEFESA

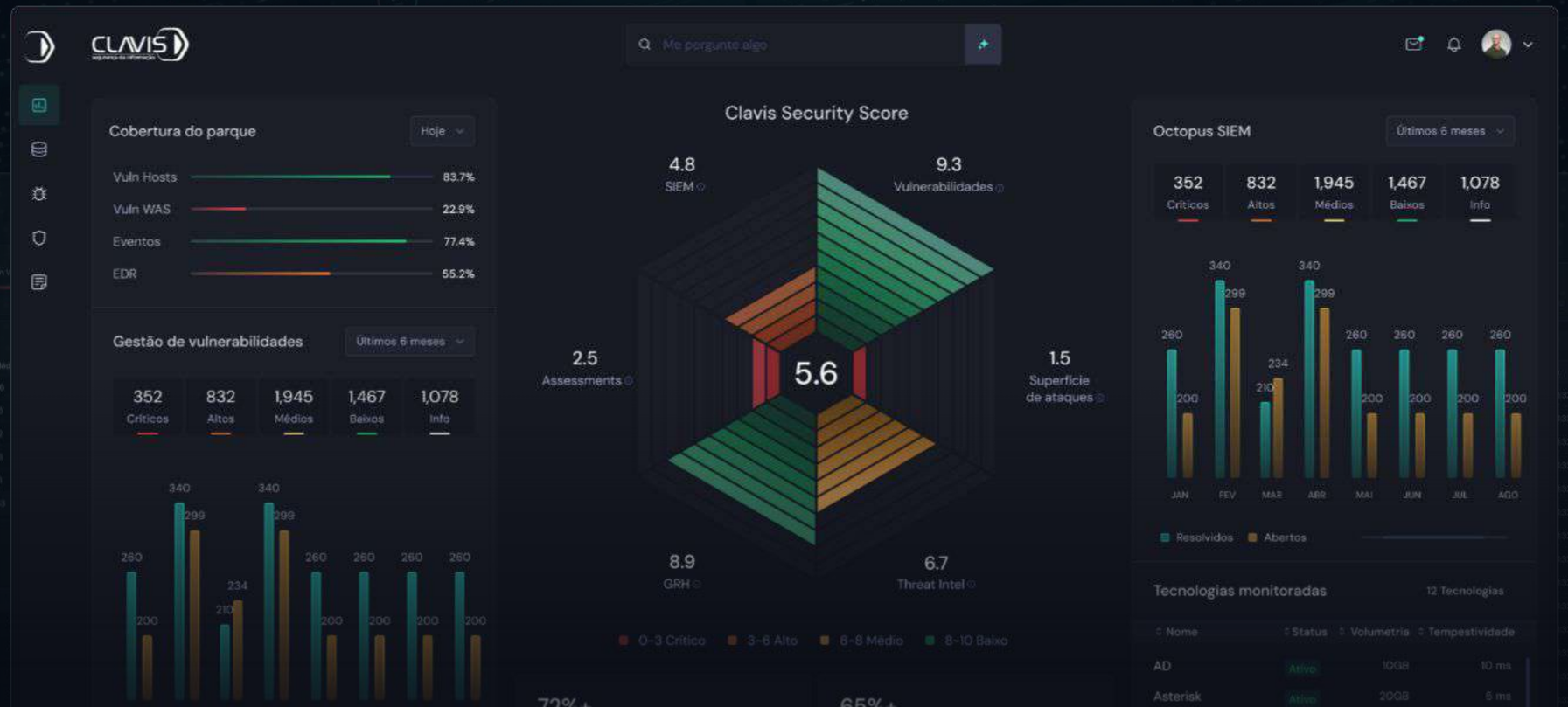
Information Security Management
ISO 27001
Certified

ISO 27701

CLAVIS
segurança da informação

# Visão Geral do SOC Clavis:

## Centro de Operações de Segurança com Inteligência



SOC Clavis: Centro de Operações de Segurança com Inteligência


# Visão Unificada da Cibersegurança

O Centro de Operações de Segurança da Clavis (SOC) agrega e unifica os nossos principais serviços e soluções, fornecendo aos nossos clientes uma arquitetura de segurança adaptativa, para identificação de ameaças, correlacionando eventos internos ao ambiente monitorado com inteligência obtida em fontes externas (Threat Intelligence).

O SOC Clavis se sustenta na tecnologia **Octopus**, um software de coleta e correlação de dados de cibersegurança reconhecido pelo Ministério da Defesa (Port. GM-MD 3.896/2021) como um **Produto Estratégico de Defesa**.

## Monitoramento de Segurança 24x7

Tenha visibilidade plena sobre os eventos e informações de segurança da sua organização.

## Inteligência de Ameaças

Detecte ameaças emergentes com inteligência de ameaças continuamente atualizada.

## Gestão de Superfície de Ataque

Identifique ativos e serviços expostos e que possam representar riscos ao negócio.

## Gerenciamento Contínuo de Vulnerabilidades

Gerencie todo o ciclo de identificação, tratamento e correção de vulnerabilidades.

## Integração com outras visões de segurança

A Plataforma de Cibersegurança da Clavis possui, ainda, capacidade de integração com serviços de Gestão do Risco Humano, Segurança Ofensiva, Governança, Risco e Conformidade.


# Gerenciamento de eventos internos e externos de cibersegurança

Conte com o **Octopus** para o gerenciamento de eventos e informações de segurança. O Octopus coleta tanto eventos internos a partir de busca em logs, bancos de dados e arquivos em ativos da organização  quanto eventos externos a partir de buscas na surface web e deep/dark web, além de sites, fóruns e aplicativos de mensagens

MINISTÉRIO DA DEFESA
PED
PRODUTO ESTRATÉGICO DE DEFESA

O **Octopus** é reconhecido como **Produto Estratégico de Defesa** (PED), conforme a **PORTARIA GM-MD No 3.896, DE 21 DE SETEMBRO DE 2021**. Trata-se de um reconhecimento do Ministério da Defesa de que este software é de interesse estratégico para a defesa nacional

## Coleta de eventos nas mais Diversas Tecnologias

O **Octopus** tem capacidade de coleta de eventos nas mais diversas tecnologias,usando métodos baseados em Syslog, SNMP, APIs, logs, bancos de dados, agentes, dentre outros.

## Inteligência de Detecção

O **Octopus** busca eventos em todo tipo de tecnologia - incluindo endpoints, redes, nuvens, ambientes colaborativos, dentre outros - gerando inteligência de detecção de ameaças.

## Correlação com Eventos de Threat Intelligence

O **Octopus** possui capacidade de busca em surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

## Correlação com Eventos de Exposição e Vulnerabilidades

O **Octopus** possui capacidade de monitoramento de ativos expostos (Superfície de Ataque) e fragilidades (Gerenciamento de Vulnerabilidades), potencializando a detecção de ameaças.


# Proteção proativa para sua organização.

Empresas estão expostas a diversas ameaças cibernéticas, que incluem não apenas ataques diretos, mas também ações prejudiciais como boatos, notícias falsas e difamação online. essas ameaças podem afetar gravemente a imagem e os negócios de uma organização.

A solução de Threat Intelligence da Clavis conta com os motores de busca e tecnologias da Plataforma Axur, consolidada no mercado brasileiro e capaz de fornecer insights curados e acionáveis, eliminando a sobrecarga manual.

///AXUR

## Planejamento

Análise, priorização e planejamento de ações definidas a partir das diretrizes e objetivos gerais apresentados pelo cliente.

## Coleta

Obtenção de dados em fontes de inteligência de ameaças cibernéticas - externas e internas - e armazenamento em um único local.

## Processamento

Contextualização, organização e priorização dos dados coletados com base em parâmetros estabelecidos no planejamento.

## Análise

Investigação abrangente sobre os dados coletados, a fim de identificar ameaças cibernéticas e compreender como afetam os interesses do cliente.


# Gerencie a superfície de ataque de sua organização

Com a Clavis Segurança da Informação, você ganha muito mais do que uma avaliação da superfície de ataque de sua organização.

Tenha acesso a uma plataforma de segurança com uma visão completa do ambiente. Além de contar com o apoio de especialistas que ajudarão a construir uma jornada de evolução de maturidade da companhia.

## Apresentação

Apresentação em tempo real do ambiente com gráficos e tabelas interativas, oferecendo uma visão clara e imediata para decisões rápidas e informadas.

## Tempestividade

Agilidade e tempestividade na identificação e solução de problemas detectados, garantindo respostas rápidas e eficazes para mitigar riscos.

## Descoberta

Descoberta detalhada de ativos e subdomínios, proporcionando um mapeamento completo e maior controle sobre a infraestrutura.

## Identificação

Identificação de subdomain takeover, detectando vulnerabilidades que podem ser exploradas por agentes maliciosos, fortalecendo a segurança da infraestrutura.


# Gerencie as Vulnerabilidades nos Ativos de sua Organização

Vulnerabilidades de Segurança são um dos principais vetores de ataque utilizados por agentes maliciosos.

A Clavis possui uma abordagem versátil para a identificação de vulnerabilidades, priorizando riscos e apoiando em todo o ciclo de identificação, tratamento e correção de vulnerabilidades,

## Versatilidade na Identificação

As tecnologias utilizadas pela Clavis permitem utilizar métodos baseados em agentes, appliances físicos e appliances virtualizados.

## Priorização Orientada a Riscos

A Plataforma Clavis combina informações de importância do ativo, severidade da vulnerabilidade e explorabilidade para estabelecer um ranking das vulnerabilidades mais relevantes.

## Correlação com Threat Intelligence

A Plataforma Clavis utiliza informações de inteligência - tais como a existência de exploits e a tendência de exploração por APTs - para priorizar vulnerabilidades.

## Correlação com Superfície de Ataque

A Plataforma Clavis utiliza informações de superfície de ataque - tais como exposição de um ativo ou serviço - para priorizar vulnerabilidades.

# Pesquisa, Desenvolvimento e Inovação: Projetos de Alta Complexidade

A Clavis possui uma capacidade diferenciada para a execução de projetos de alta complexidade. A empresa conta com um time de mestres e doutores com formação acadêmica e experiência de mercado, atuantes em virtualmente todas as áreas da Cibersegurança.

Conte com a Clavis para apoiar projetos de grande complexidade em cibersegurança, desde seu planejamento, passando pela captação de recursos, até a sua gestão e execução.

## Competência em todas as áreas de cibersegurança

Conte com a Clavis para projetos de alta complexidade em temas como Detecção de Ameaças, CyberThreat Intelligence, Exposições e Vulnerabilidades, Segurança Ofensiva, dentre outros.

## Equipe técnica com formação científica e experiência de mercado

A Clavis conta com mestres e doutores que combinam vivência acadêmica com experiência de mercado, preparados para abordar de forma rigorosa os mais desafiadores problemas.

## Experiência em projetos de pesquisa subvencionados

A Clavis já executou diversos projetos com apoio de órgãos como **Faperj**, **AgeRio**, **Finep** e **CNPq**, sempre alcançando resultados de impactos científico e corporativo.

## Parceria com Universidades

A Clavis possui parcerias formalmente estabelecidas com **UFRJ**, **UFF**, **UFMG** e **UNIFEI**.

## Clavis CyberLabs

Os laboratórios de pesquisa mantém a Clavis na fronteira do conhecimento em cibersegurança.

## Empresa Estratégica de Defesa (EED)

O selo de **EED** é o reconhecimento, pelo Ministério da Defesa, da imprescindibilidade do conhecimento acumulado pela Clavis ao longo de duas décadas de atuação em cibersegurança

# Treinamento e campanhas de conscientização.

As ações de treinamento e conscientização conduzidas pela Clavis diferenciam-se pelo fato de serem planejadas a partir de um cuidadoso levantamento prévio das necessidades de cada organização, baseado na execução de entrevistas, auditorias, testes de segurança e de engenharia social.

A Clavis diferencia-se, ainda, pela sua ampla experiência no fornecimento de treinamento na área de Segurança da Informação — tanto treinamentos próprios quanto vinculados às principais entidades de certificação internacional.

## Produção de conteúdo

A Clavis é responsável por projetos de grande alcance e repercussão, como o WarDrivingDay e o WarTrashingDay.

## Campanhas para o grande público

A Clavis é responsável por projetos de grande alcance e repercussão, como o WarDrivingDay e o WarTrashingDay.

## Pesquisa e desenvolvimento

A Clavis é reconhecida pela sua inovação e alinhamento com os avanços em segurança da informação.

## Programas de certificação profissional

A Clavis é a principal empresa de treinamento e certificação profissional em Segurança da Informação.

CLAVIS
segurança da informação

clavis.com.br

contato@clavis.com.br

+55 (21) 2210-6061 I +55 (21) 2561-0867

CLAVIS
segurança da informação

# Centro de Operações de Segurança com Inteligência

## Uma ferramenta proativa de Cibersegurança

*(SOC - Security Operations Center)*

www.clavis.com.br

# SUMÁRIO



SUMÁRIO

# Resumo
# SOC CLAVIS

**Octopus: o SIEM da Clavis**

**Gestão de vulnerabilidades**

**Soluções próprias**

**Consultoria em conformidade, risco e compliance**

**Serviços e atividades técnicas**

**Treinamento e conscientização**

Centrais de Operações de Segurança (SOC - Security Operations Centers) são tradicionalmente vistas como uma ferramenta para monitoramento de alertas e a detecção de ameaças de cibersegurança - portanto, fundamentais para uma resposta tempestiva a incidentes de segurança. No entanto, um SOC pode ter uma atuação muito mais abrangente do que a de uma ferramenta de resposta a incidentes  O presente e-book discute como os SOC podem ter um papel pró-ativo em cibersegurança - não apenas antecipando-se aos ataques por meio de métodos avançados de detecção, mas também, atuando como indutores de boas práticas de proteção prévia.

Capítulo 1

# Apresentação

Central de Operações de Segurança (conhecida pela sigla SOC, do inglês Security Operation Center) é uma estrutura organizacional que atua no monitoramento de eventos relacionados à segurança e eventuais tomadas de ação relacionadas a tais eventos. Pelo seu caráter intrínseco de "ferramenta de monitoramento", SOCs são tradicionalmente vistos pelos especialistas em cibersegurança como uma ferramenta de segurança reativa. De fato, o SOC é uma ferramenta fundamental para uma efetiva postura de resiliência cibernética: o monitoramento constante e a detecção tempestiva de problemas é o ponto de partida para a resposta a eventuais incidentes de segurança, para a mitigação de danos e para a recuperação plena do negócio.

No entanto, como veremos, o SOC pode ser muito mais do que uma ferramenta de Resposta a Incidentes: um moderno SOC Proativo tem o potencial de induzir boas práticas e evoluções em praticamente todas as áreas da cibersegurança corporativa. A "virada de chave" de um SOC Reativo para um SOC Proativo acontece a partir do entendimento que eventos e alertas não são apenas evidências de incidentes, mas podem ser a matéria-prima para a identificação de vulnerabilidades em tecnologias, fragilidades em processos e falhas em comportamento humano.


Desta forma, tais eventos e alertas podem ser o ponto de partida para a tomada de ações de evolução da maturidade, apontando para a necessidade de correção de vulnerabilidades, revisão de processos, ações de conscientização de usuários, contratação de serviços e ferramentas, dentre outros.

Para que esta virada de chave aconteça, no entanto, é necessária uma mudança de mentalidade em relação ao papel do SOC, aproximando o time do SOC dos outros times de segurança e tecnologia e permitindo que as descobertas realizadas a partir dos eventos e alertas analisados no SOC induzam ações corretivas e preventivas conduzidas pelos times de Governança, Riscos e Conformidade, de Desenvolvimento Seguro, de Treinamento e Conscientização, dentre outros.

Capítulo 2

# Modelo “Clássico”de atuação dos SOC’s: o “SOC Reativo”

Em sua concepção mais “clássica”, o SOC de uma organização era o departamento responsável por coletar todos os eventos relevantes do ponto de vista de cibersegurança, monitorando alertas e respondendo a incidentes de segurança. Nesta concepção, o papel do SOC é eminentemente responsivo: ao detectar uma situação que represente um potencial cenário de ataque, o SOC inicia as tratativas para conter os efeitos de tal ataque. Ações de prevenção a incidentes de segurança ou mesmo de antecipação a ataques ficam relegadas a segundo plano.

Ainda que - como defendemos nesta discussão - o papel moderno de um SOC deva ser muito mais proativo, o modelo clássico do “SOC Reativo” foi fundamental para consolidar conceitos básicos relacionados ao monitoramento e resposta a incidentes de segurança, alguns dos quais, gostaríamos de destacar aqui.

## **Hierarquia:** Evento > Alerta > Incidente (de Segurança)


Um conjunto básico de conceitos relacionados a Centrais de Operações de Segurança e a Resposta a Incidentes é o de **evento, alerta e incidente**.

## Evento de segurança

É qualquer registro de evento associado a um ativo ou tecnologia e que possa ser de potencial interesse na detecção ou análise de ameaças cibernéticas. Exemplos de Eventos de Segurança são o login de um usuário ou o download de um arquivo.

Tais registros são a matéria-prima para a detecção de ameaças - e se espera que a maioria absoluta dos eventos registrados em uma organização não representem qualquer risco de segurança.

## Alerta de segurança

É um evento ou conjunto de eventos que possam indicar uma ameaça cibernética. Exemplos de Alertas de Segurança baseados em um único evento são uma falha de login de usuário ou uma tentativa de download não autorizado a um arquivo. Um outro exemplo de alerta - desta vez, caracterizado por um conjunto não-unitário de eventos - seria um conjunto de logins simultâneos de um mesmo usuário a partir de posições geograficamente distantes.
De maneira geral, os alertas representam um potencial risco de segurança, devendo, sempre, receber algum tipo de tratamento - seja manual ou automatizado.

## Incidente de segurança

É a materialização de uma ameaça cibernética na forma de um conjunto de eventos de segurança que dá convicção de um ataque está em curso. Vale observar que não é necessário que o ataque tenha sido concluído (e causado dano) para que se caracterize um incidente. Por exemplo, o vazamento de credenciais de acesso é um exemplo claro de incidente de segurança, ainda que tais credenciais não tenham sido utilizadas para ganhar acesso a um sistema.

Os incidentes demandam um tratamento cuidadoso, quase sempre, manual, de forma a mitigar potenciais danos.

## Ferramenta SIEM de gestão de eventos e informações de segurança

O SOC consolidou a ferramenta **SIEM *(do inglês Security Information and Event Management)*** como a **ferramenta fundamental para coleta e centralização de eventos e informações de segurança** - portanto, elemento básico para a operação do SOC. Em seu papel mais básico, o SIEM tem a função de acessar ativos e tecnologias para coletar registros de eventos (*logs*)

Em um papel mais sofisticado, o SIEM tem a possibilidade de correlacionar diferentes eventos com o objetivo de identificar potenciais ameaças. Importante observar que essas correlações podem ser extremamente sofisticadas, envolvendo diferentes tecnologias em diferentes locais e contemplando grandes intervalos de tempo, como forma de detectar ameaças avançadas e persistentes, por exemplo.

## Criticidade de alertas e níveis de serviço

Outro conceito que se consolidou a partir dos modelos clássicos de SOC é o de **"criticidade de alertas"** como uma medida de risco associado a um alerta de segurança.

Além disso, define-se o "nível de serviço como uma descrição dos parâmetros associados à análise e ao tratamento de um alerta - com destaque para o parâmetro de tempo de atendimento.

Naturalmente, espera-se que alertas de maior criticidade tenha níveis de serviço com menor tempo de atendimento. Os níveis de serviço associados a cada criticidade de alerta são, em geral, formalizados na forma de um Acordo de Nível de Serviço (SLA, do inglês Service Level Agreement).

Em um Centro de Operações de Segurança, os níveis de alerta e as ações correspondentes podem variar dependendo da organização e da sua política de segurança. No entanto, há uma estrutura comum que é frequentemente seguida.

Aqui está um exemplo típico:

| Alerta de criticidade baixa | Alerta de criticidade média |
|---|---|
| **Descrição** | **Descrição** |
| Indica atividades que não são necessariamente maliciosas, mas que podem indicar uma possível vulnerabilidade ou comportamento anômalo que deve ser monitorado. | Indica atividades suspeitas que podem representar um risco potencial, exigindo uma análise mais detalhada para determinar se são maliciosas. |
| **Ações** | **Ações** |
| • **Agregação e relatórios:** Esses alertas são normalmente agregados e enviados em um relatório semanal ou mensal.<br>• **Monitoramento contínuo:** Continuar monitorando para verificar se o comportamento persiste ou se agrava.<br>• **Análise de tendências:** Utilizar para identificar tendências ao longo do tempo e ajustar as regras de segurança, se necessário. | • **Notificação imediata por email:** Enviar um email imediato aos analistas de segurança com detalhes do alerta.<br>• **Investigação:** Requer uma investigação manual para confirmar se o alerta é um falso positivo ou se representa uma ameaça real.<br>• **Acompanhamento e documentação:** Documentar os resultados da investigação e acompanhar quaisquer ações corretivas que sejam necessárias. |
| **Alerta de criticidade alta** | **Alerta de criticidade crítica** |
| **Descrição** | **Descrição** |
| Indica uma atividade que é altamente suspeita ou confirmada como maliciosa, representando um risco imediato à segurança da organização. | Indica uma ameaça ativa e confirmada que está em andamento e representa um risco significativo e imediato para a organização. |
| **Ações** | **Ações** |
| • **Alerta imediato:** Envio imediato de alertas através de múltiplos canais (email, SMS, ferramentas de colaboração como Slack ou Teams) para os analistas de segurança e outras partes interessadas.<br>• **Resposta rápida:** Iniciar procedimentos de resposta a incidentes, que podem incluir contenção, erradicação e recuperação.<br>• **Investigação detalhada:** Realizar uma investigação detalhada para compreender o alcance e o impacto do incidente.<br>• **Relatório de incidente:** Produzir um relatório detalhado do incidente para os executivos e para futuras análises de segurança. | • **Alerta de emergência:** Notificação de emergência para toda a equipe de resposta a incidentes, muitas vezes através de todos os meios de comunicação disponíveis.<br>• **Mobilização total:** Mobilizar todos os recursos disponíveis para conter e mitigar o incidente.<br>• **Comunicação com executivos:** Manter a liderança executiva informada sobre a situação em tempo real.<br>• **Resposta em tempo real:** Implementar ações de resposta em tempo real, como isolamento de sistemas afetados, bloqueio de endereços IP, e outras medidas de contenção.<br>• **Análise pós-incidente:** Após a contenção e erradicação, realizar uma análise pós-incidente detalhada para entender a causa raiz e melhorar as defesas. |

# Playbooks

SOC não é lugar de improviso: quando um incidente de segurança se concretiza, cada segundo é importante para conter danos e recuperar a operação. Playbooks são exatamente roteiros pre-estabelecidos de ações a serem executadas em cada cenário de incidente que tenha sido mapeado. Playbooks estão fortemente associados ao tipo de tecnologia envolvida no incidente, mas consideram, ainda, uma série de outros fatores tais como o setor de atuação da empresa, regulações aplicáveis, contratos com clientes, política de relações públicas dentre outros.

**Veja um exemplo de playbook associado ao vazamento de credenciais de acesso na deep web:**

**Playbook de Resposta a Incidentes: Vazamento de Credenciais de Acesso na Deep Web**

| 1- Identificação e classificação do incidente | 2 - Notificação e mobilização |
|---|---|
| • **Recepção do alerta:** Receber o alerta de que credenciais de acesso da organização foram encontradas na deep web.<br><br>• **Classificação da criticidade:** Classificar o incidente como de alta criticidade devido ao risco de acesso não autorizado a sistemas internos. | • **Notificação imediata:** Notificar imediatamente a equipe de resposta a incidentes (CSIRT) e os responsáveis pela segurança da informação.<br><br>• **Convocação de reunião de emergência:** Convocar uma reunião de emergência para discutir o incidente e planejar a resposta. |
| **3 - Contenção imediata** | **4 - Investigação inicial** |
| • **Bloqueio de acessos:** Bloquear imediatamente as contas comprometidas ou aplicar políticas de senha para expirar e forçar a redefinição das senhas comprometidas.<br><br>• **Monitoramento de atividade suspeita:** Aumentar a vigilância e o monitoramento de atividades suspeitas relacionadas às contas comprometidas em todos os sistemas. | • **Coleta de Evidências:** Coletar todas as evidências disponíveis relacionadas ao vazamento, incluindo logs de acesso, detalhes das credenciais vazadas e informações sobre a origem do vazamento.<br><br>• **Análise de Logs:** Analisar os logs de segurança para identificar possíveis acessos não autorizados utilizando as credenciais comprometidas.<br><br>• **Validação das Credenciais:** Validar se as credenciais são válidas e se ainda estão ativas. |
| **5 - Comunicação interna** | **6 - Mitigação e recuperação** |
| • **Informação à liderança:** Informar a liderança da organização sobre a situação e as medidas tomadas.<br><br>• **Comunicação com os usuários afetados:** Notificar os usuários afetados sobre o vazamento e instruí-los a alterar suas senhas e ativar a autenticação multifator (MFA), se disponível. | • **Redefinição de senhas:** Forçar a redefinição de senhas para todas as contas comprometidas.<br><br>• **Atualização de políticas de segurança:** Revisar e atualizar as políticas de segurança de senha e autenticação para incluir requisitos mais fortes.<br><br>• **Implementação de MFA:** Se ainda não estiver implementado, considerar a adoção de autenticação multifator para aumentar a segurança das contas. |
| **7 - Análise pós-incidente** | **8 - Prevenção futura** |
| • **Revisão do incidente:** Realizar uma revisão detalhada do incidente para entender como o vazamento ocorreu e identificar pontos fracos na segurança.<br><br>• **Documentação:** Documentar todas as ações tomadas durante a resposta ao incidente.<br><br>• **Lições aprendidas:** Realizar uma sessão de lições aprendidas com a equipe para identificar melhorias nos processos de segurança e resposta a incidentes. | • **Monitoramento contínuo:** Estabelecer monioramento contínuo da deep web para detectar futuros vazamentos de credenciais.<br><br>• **Treinamento de conscientização:** Conduzir treinamentos de conscientização de segurança para todos os funcionários, destacando a importância de práticas seguras de gerenciamento de senhas.<br><br>• **Auditoria de segurança:** Realizar auditorias de segurança periódicas para garantir que as medidas de segurança estejam sendo seguidas e sejam eficazes. |

3

Capítulo 3

# Estratégias e abordagens para construir um SOC corporativo

Diferentes organizações podem optar por diversas estratégias para o estabelecimento de SOCs de acordo com suas características.

Destacamos, a seguir, os principais tipos de SOC, apresentando suas características, vantagens e desvantagens.

| SOC dedicado | Vantagens | Desvantagens |
|---|---|---|
| Um SOC dedicado é um centro de operações de segurança exclusivo para uma única organização. Ele é projetado, implementado e mantido pela própria empresa, utilizando recursos internos. Este tipo de SOC oferece um alto nível de controle e customização, mas também requer um investimento significativo em termos de infraestrutura, pessoal e recursos. | • Controle total sobre as operações de segurança;<br>• Customização conforme as necessidades específicas da organização;<br>• Integração profunda com os processos e sistemas internos. | • Alto custo de implementação e manutenção;<br>• Necessidade de equipe altamente qualificada e especializada;<br>• Escalabilidade pode ser um desafio. |
| **SOC distribuido** | **Vantagens** | **Desvantagens** |
| Um SOC distribuído é uma abordagem onde as funções do SOC são dispersas geograficamente ou entre diferentes equipes dentro da organização. Isso permite que várias equipes em diferentes locais colaborem e compartilhem responsabilidades de segurança. | • Resiliência aumentada devido à distribuição geográfica;<br>• Capacidade de operar em fusos horários diferentes, oferecendo cobertura 24/7;<br>• Flexibilidade e escalabilidade melhoradas. | • Desafios de comunicação e coordenação entre equipes dispersas;<br>• Complexidade na gestão de processos e tecnologias integradas;<br>• Necessidade de políticas e procedimentos robustos para manter a coesão. |
| **SOC gerenciado** | **Vantagens** | **Desvantagens** |
| Um SOC gerenciado é operado por um provedor de serviços de segurança (MSSP), que oferece monitoramento e gestão de segurança como um serviço para várias organizações. Os MSSPs utilizam seus próprios recursos e expertise para fornecer esses serviços. | • Custo mais baixo comparado a um SOC dedicado, devido à economia de escala;<br>• Acesso a expertise e tecnologia de ponta sem a necessidade de investimento interno;<br>• Rápida implementação e escalabilidade. | • Menor controle sobre as operações de segurança;<br>• Dependência de um provedor externo, o que pode gerar preocupações com a confidencialidade e privacidade;<br>• Possíveis limitações na customização conforme as necessidades específicas da organização. |
| **SOCaaS** | **Vantagens** | **Desvantagens** |
| Um SOCaaS utiliza tecnologias de computação em nuvem para oferecer capacidades de monitoramento e resposta a incidentes sem a necessidade de uma infraestrutura física específica. Ele pode ser operado por equipes internas ou por provedores externos. | • Flexibilidade e escalabilidade melhoradas;<br>• Redução de custos associados à infraestrutura física;<br>• Acesso remoto e mobilidade para os analistas de segurança. | • Dependência de conectividade à internet e de serviços de nuvem;<br>• Potenciais preocupações com a segurança dos dados na nuvem;<br>• Necessidade de integração com os sistemas de TI existentes na organização. |
| **SOC co-gerenciado** | **Vantagens** | **Desvantagens** |
| Um SOC co-gerenciado é uma abordagem híbrida onde a responsabilidade pela operação do SOC é compartilhada entre a organização e um provedor externo. Isso permite que a organização mantenha algum controle interno enquanto aproveita a expertise e os recursos do provedor. | • Equilíbrio entre controle interno e expertise externa;<br>• Maior flexibilidade e capacidade de resposta;<br>• Compartilhamento de responsabilidades e recursos. | • Necessidade de uma coordenação eficiente entre as equipes internas e externas;<br>• Possíveis desafios na definição de responsabilidades e processos;<br>• Dependência parcial de um provedor externo. |

Esses são os principais tipos de SOCs, cada um com suas vantagens e desvantagens, e a escolha do tipo adequado depende das necessidades específicas, recursos e estratégias de segurança da organização.

Capítulo 4

# O SIEM como ferramenta central do SOC

Conforme discutimos anteriormente, SIEM é a ferramenta para coleta, processamento e centralização de logs de eventos de segurança. Adicionalmente, o SIEM pode implementar algoritmos de correlação de eventos com fins de detecção de ameaça.

Devido ao seu papel de "centralizador de eventos de segurança", o SIEM - ou ferramenta similar tal como UTM ou XDR - é uma ferramenta central para a operação de qualquer SOC. É o SIEM que irá alertar quando um determinado evento ou conjunto de eventos enquadra-se em um padrão associado a alerta. E é a partir do SIEM que especialistas irão realizar análises quanto um incidente de segurança demandar o acesso a logs para aprofundar a compreensão sobre um incidente.

## Endpoint

**Tipos de Logs/Eventos Coletados:**

- Registros de antivírus/antimalware;
- Logs de firewall de host;
- Eventos de login/logout;
- Logs de instalação/desinstalação de software;
- Logs de acesso a arquivos e modificações;
- Eventos do sistema operacional (Windows Event Logs, syslog).

**Tipos de Ameaças Detectadas:**

- Malware e vírus;
- Tentativas de acesso não autorizado;
- Atividade de software malicioso;
- Modificações não autorizadas em arquivos críticos;
- Execução de scripts ou programas não autorizados;
- Comportamento anômalo de usuários.

## Servidores

**Tipos de Logs/Eventos Coletados:**

- Logs de sistema operacional (Windows Event Logs, syslog);
- Logs de aplicativos de servidor (web servers, databases);
- Eventos de autenticação e autorização;
- Logs de acesso remoto (SSH, RDP);
- Logs de configuração de sistema;
- Registros de desempenho e integridade do sistema.

**Tipos de Ameaças Detectadas:**

- Tentativas de exploração de vulnerabilidades;
- Ataques de força bruta
- Acesso não autorizado a dados sensíveis;
- Modificações não autorizadas na configuração do sistema;
- Atividades de escalonamento de privilégios;
- Ataques de negação de serviço (DoS).

## Infraestrutura de rede

**Tipos de Logs/Eventos Coletados:**

- Logs de firewall de rede;
- Logs de roteadores e switches;
- Logs de sistemas de detecção e prevenção de intrusões (IDS/IPS);
- Registros de tráfego de rede;
- Logs de VPN;
- Logs de DNS.

**Tipos de Ameaças Detectadas:**

- Ataques de rede (DDoS, Man-in-the-Middle);
- Scanning de portas e vulnerabilidades;
- Tentativas de infiltração e exfiltração de dados;
- Acesso não autorizado a recursos de rede;
- Atividade de malware propagando na rede;
- Anomalias no tráfego de rede.

## E-mail

**Tipos de Logs/Eventos Coletados:**

- Logs de servidores de e-mail (Exchange, SMTP);
- Logs de gateways de e-mail;
- Logs de sistemas de filtragem de spam e malware;
- Registros de envio e recebimento de e-mails;
- Logs de autenticação de e-mail (DKIM, SPF);

**Tipos de Ameaças Detectadas:**

- Phishing e spear-phishing;
- Malwares e anexos maliciosos;
- Comprometimento de contas de e-mail;
- Ataques de engenharia social;
- Envio de spam;
- Tentativas de spoofing de e-mail.

## Ambientes colaborativos

**Tipos de Logs/Eventos Coletados:**

- Logs de plataformas de colaboração (Microsoft Teams, Slack);
- Logs de compartilhamento de arquivos (SharePoint, Google Drive);
- Eventos de criação, modificação e exclusão de documentos;
- Registros de atividade de usuário;
- Logs de integração de aplicativos de terceiros.

**Tipos de Ameaças Detectadas:**

- Acesso não autorizado a documentos e arquivos;
- Exfiltração de dados sensíveis;
- Modificações não autorizadas de documentos;
- Comportamento anômalo de usuários;
- Atividades de contas comprometidas;
- Violação de políticas de compartilhamento de arquivos.

## Equipamentos de segurança

**Tipos de Logs/Eventos Coletados:**

- Logs de firewalls;
- Logs de sistemas de detecção e prevenção de intrusões (IDS/IPS);
- Logs de gateways de segurança;
- Logs de sistemas de controle de acesso físico;
- Logs de sistemas de segurança de endpoint.

**Tipos de Ameaças Detectadas:**

- Tentativas de intrusão e ataques externos;
- Atividades maliciosas detectadas por IDS/IPS;
- Tentativas de acesso físico não autorizado;
- Atividades anômalas de rede e endpoint;
- Violações de políticas de segurança;
- Atividades de malware.

## Infraestrutura em nuvem

**Tipos de Logs/Eventos Coletados:**

- Logs de serviços de nuvem (AWS CloudTrail, Azure Monitor, Google Cloud Logging);
- Logs de autenticação e autorização em serviços de nuvem;
- Logs de API e atividades de administração;
- Logs de segurança de rede em nuvem (VPC Flow Logs);
- Logs de auditoria de conformidade.

**Tipos de Ameaças Detectadas:**

- Acessos não autorizados a recursos de nuvem;
- Modificações não autorizadas em configurações de serviços de nuvem;
- Atividades de contas comprometidas
- Atividade anômala de APIs;
- Violações de conformidade;
- Ataques a infraestrutura de nuvem (exploits de vulnerabilidades).

## Aplicações de software

**Tipos de Logs/Eventos Coletados:**

- Logs de aplicações web;
- Logs de bancos de dados;
- Logs de autenticação e autorização de aplicativos;
- Logs de desempenho e integridade de aplicativos;
- Registros de API.

**Tipos de Ameaças Detectadas:**

- Ataques de injeção SQL;
- Ataques de Cross-Site Scripting (XSS);
- Tentativas de acesso não autorizado a dados de aplicativos;
- Modificações não autorizadas em dados de aplicativos;
- Atividade de contas comprometidas;
- Exploração de vulnerabilidades de aplicativos.

Para acessar logs de eventos de segurança em tais tecnologias, o Clavis SIEM faz uso dos mais diversos métodos de coleta, incluindo os seguintes:

**• Syslog**
É um padrão amplamente utilizado para mensagens de log, permitindo que diferentes dispositivos de rede e sistemas operacionais enviem logs para um servidor central. O SIEM pode configurar um servidor Syslog para receber e processar esses logs. Exemplo de Tecnologias: Servidores Linux/Unix, dispositivos de rede como roteadores e switches, firewalls.

**• SNMP**
O Protocolo Simples de Gerenciamento de Rede (SNMP) é usado para coletar informações e gerenciar dispositivos em redes IP. O SIEM pode usar SNMP para coletar logs e eventos de dispositivos de rede. Exemplo de Tecnologias: Roteadores, switches, servidores, impressoras de rede.

**• Agentes de Software**
São programas instalados nos dispositivos que coletam logs localmente e os enviam para o SIEM. Esses agentes podem ser configurados para capturar uma ampla gama de logs de diferentes fontes. Exemplo de Tecnologias: Estações de trabalho, servidores, dispositivos de armazenamento.

**• Arquivos de Log**
O SIEM pode ser configurado para ler e processar arquivos de log armazenados localmente ou em servidores remotos. Isso pode ser feito por meio de acesso a diretórios específicos e leitura dos arquivos de log. Exemplo de Tecnologias: Servidores web (Apache, Nginx), servidores de aplicativos, sistemas operacionais.

**• APIs**
*Application Programming Interfaces* permitem que um SIEM interaja diretamente com aplicativos e serviços para coletar logs. As APIs fornecem uma maneira programática de acessar dados e eventos de segurança. Exemplo de Tecnologias: Serviços em nuvem (AWS CloudTrail, Microsoft Azure Monitor), aplicações web, soluções de segurança específicas (como antivírus e sistemas de prevenção de intrusões).

**• Bancos de Dados**
O SIEM pode se conectar diretamente a bancos de dados para extrair logs de eventos de segurança. Isso geralmente é feito usando drivers e conectores específicos de banco de dados, como ODBC, JDBC ou conectores nativos. Exemplo de Tecnologias: Bancos de dados SQL (MySQL, PostgreSQL, Microsoft SQL Server), bancos de dados NoSQL (MongoDB, Cassandra).

**• Integrações Nativas e Conectores**
Muitos SIEMs modernos oferecem integrações nativas e conectores específicos para uma ampla variedade de tecnologias. Essas integrações permitem a coleta direta e otimizada de logs. Exemplo de Tecnologias: Microsoft Active Directory, sistemas de email (Microsoft Exchange, Gmail), plataformas de virtualização (VMware, Hyper-V).

**• Syslog-ng e Rsyslog**
São versões avançadas do Syslog que permitem uma coleta mais robusta e flexível de logs. Eles podem ser usados para filtrar, formatar e direcionar logs para o SIEM. Exemplo de Tecnologias: Sistemas Linux/Unix, aplicativos empresariais.

Capítulo 5

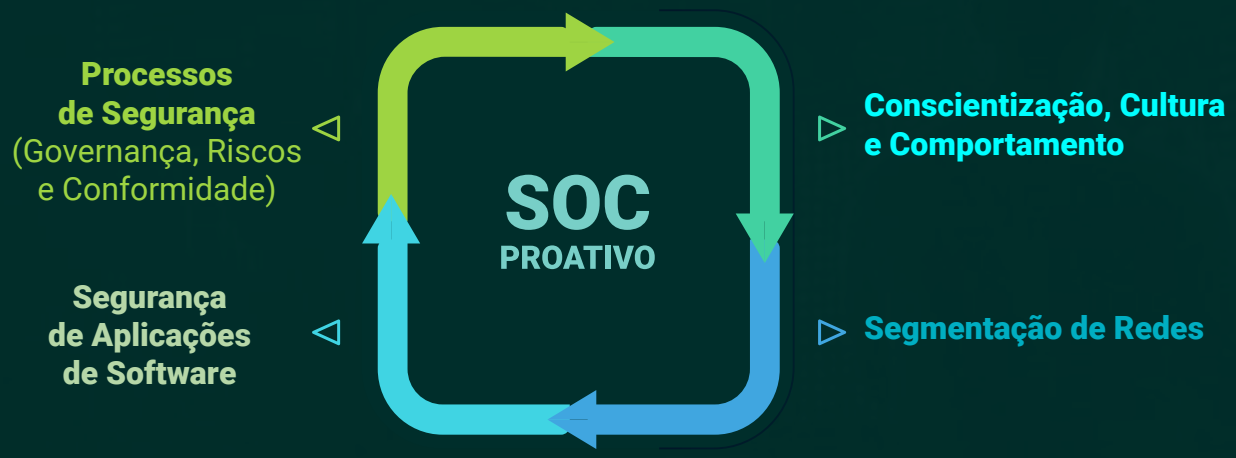
# SOC como ferramenta proativa indutora de segurança

Quando observamos as “core functions” do NIST Cybersecurity Framework, entendemos claramente que a cibersegurança envolve atividades de segurança “a priori”, associadas às funções “Identificar” e “Proteger”, e atividades de segurança “a posteriori”, associadas às funcões “Responder” e “Recuperar”, com a função “Detectar” sendo o “ponto de partida” para as ações de resposta a incidentes. Neste sentido, as atividades conduzidas por uma Central de Operações de Segurança estão tradicionalmente associadas à segurança “a posteriori”, por meio da detecção de ameaças e posterior resposta a incidentes.

No entanto, apesar da associação natural do SOC a atividades reativas, há muito tempo os SOCs deixaram de ser uma área cuja função é simplesmente aguardar um incidente para reagir. Atividades como threat intelligence, threat hunting e compartilhamento de informações podem ajudar a antecipar ameaças antes que elas se concretizem na forma de ataques. Mais do que isso: muitos dos alertas gerados e analisados em um SOC podem apontar para não-conformidade e falhas em mecanismos de proteção. Por exemplo, um alerta associado a um evento de autenticação/login pode indicar que um usuário está acessando um sistema corporativo a partir de um dispositivo pessoal, apontando para a necessidade de revisão de políticas e ferramentas. Desta forma, em vez de o alerta desdobrar em atividades de resposta a incidentes, ele pode ser o ponto de partida para ações de proteção prévia - por exemplo, a revisão de uma política de gestão de acessos e identidades ou mesmo a aquisição de ferramentas para tal finalidade.

Formalmente, dizemos que o SOC executa uma *atividade proativa* quando induz um conjunto de ações que reduzem a probabilidade de ocorrência de incidentes de segurança, no futuro. Em outras palavras, o SOC Proativo é capaz de detectar fragilidades e exposições que poderiam ser exploradas em cenários de ataque - e atua no sentido de eliminar tais fragilidades e exposições.

Importante destacar que as ações induzidas por um SOC Proativo englobam potencialmente todas as áreas de atuação e classes de controles em cibersegurança, conforme exemplificamos a seguir.




**Processos de Segurança (Governança, Riscos e Conformidade)**

Alertas de Segurança podem ser excelentes aliados na identificação de fragilidades em processos de segurança. Por exemplo, um login de sistema realizado por um funcionário em período de férias pode sinalizar para a ausência de um processo de suspensão do acesso a sistemas pelo setor de Recursos Humanos ou pelo setor deste funcionário.

**Conscientização, Cultura e Comportamento**

Altos índices de acesso a URLs classificadas como endereços associados a phishing podem ser um forte indicativo de baixa maturidade dos colaboradores e sinalizar para uma oportunidade de ação na construção de um programa de Conscientização, Cultura e Comportamento.

**Segurança de Aplicações de Software**

Alertas gerados por um Web Application Firewall (WAF) podem apontar para um grande número de vulnerabilidades potencialmente exploráveis em uma aplicação web, sinalizando para a necessidade de uma revisão dos processos de desenvolvimento seguro de software por parte de uma empresa.

**Segmentação de Redes**

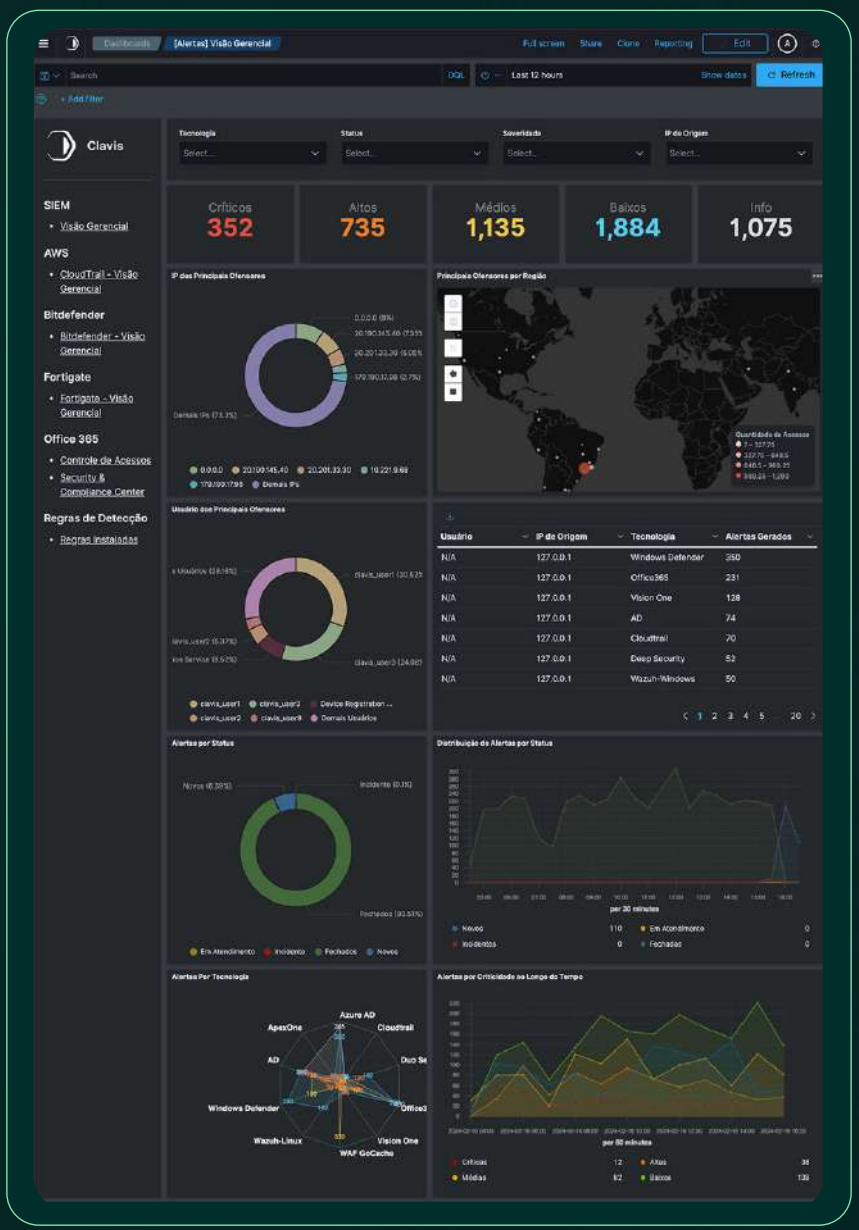
Alertas de falha de autenticação de usuários em ativos que deveriam estar em segmentos isolados de rede podem indicar falhas na segmentação de rede ou na configuração de firewalls.

Em todos os exemplos acima, os alertas destacados permitem identificar fragilidades que, de outra forma, demandariam a auditoria de processos e a revisão de configurações de equipamentos e sistemas. No entanto, a simples observação de um evento indesejado (o alerta) permite evidenciar a fragilidade e instanciar ações para resolvê-la

Capítulo 6

# Estudo de Caso: “SOC como Serviço” O SOC Gerenciado da Clavis

O “SOC como Serviço” oferecido pela Clavis é um exemplo perfeito de SOC Gerenciado com profundas características de SOC Proativo - podendo, ainda, ser utilizado no modelo Co-Gerenciado. Trata-se de um exemplo concreto de como uma Central de Operações de Segurança pode ter profundo impacto na postura de segurança de uma organização. Mais do que isso, evidencia as vantagens dos modelos “gerenciado” e “co-gerenciado” para a contratação de um SOC, em que a empresa contratante herda todo um corpo de conhecimentos técnicos avançados detidos pelo provedor de serviços de segurança.



## Octopus: o SIEM da Clavis


O SOC da Clavis sustenta-se em uma tecnologia própria para a coleta, centralização e análise de eventos de segurança, o Octopus. (Historicamente, o SIEM da Clavis é conhecido pelo nome Octopus. Para o futuro, a Clavis deve abordar um tom “minimalista” e usar o novo nome "Clavis SIEM" para sua principal ferramentade segurança, privilegiando a clareza e a transparência.)

O Octopus vem sendo desenvolvido pela Clavis há mais de uma década. Ao longo de todo este período, o Octopus desenvolveu uma capacidade de coleta de dados oriundos de centenas de tecnologias. Mais importante: se uma tecnologia relevante para o cliente ainda não está “coberta” pelo Octopus, a empresa pode colocar no roadmap de atendimento do cliente o desenvolvimento de coletores, algoritmos de detecção e playbooks associados a tal tecnologia.

## Inteligência de Detecção

Muito mais do que a capacidade de coletar dados de diferentes tecnologias, o Octopus se destaca pela "inteligência de detecção" desenvolvida ao longo de mais de uma década de desenvolvimento. Isso significa que o Octopus executa um enorme conjunto de algoritmos que correlacionam os eventos mais relevantes do ponto de vista de detecção de potenciais ameaças. Para potencializar sua capacidade de detecção de ameaças, o Octopus faz uso de grande variedade de estratégias de detecção:

• **Alertas nativosinatos do Octopus versus alertas herdados de outras ferramentas**
Ao conectar-se às mais diversas tecnologias, o Octopusganha a possibilidade de "herdar" a inteligência de detecção destas tecnologias, já que muitas delas já possuem seus próprios alertas. Ao mesmo tempo, ao ter acesso aos eventos gerados nestas tecnologias, o Octopus tem a possibilidade de definir novas regras de alertas inatos da ferramenta. Assim, ao conectar-se a um firewall, um alerta gerado pelo Octopus pode estar diretamente associado a um alerta deste firewall (por exemplo, associado a um bloqueio/drop de conexão) ou estar associado a um conjunto de eventos que não caracterize um alerta por parte do firewall, mas que a inteligência do Octopus entenda ser um alerta (por exemplo, um padrão temporal de conexões ao longo de um intervalo de tempo).

• **Alertas *single-asset versus* alerta *multi-asset***
Dizemos que um alerta é do tipo single-asset quando ele é constituído a partir de eventos oriundos de um único ativo - por exemplo, um endpoint ou servidor. Alertas multi-asset são constituídos a partir de eventos oriundos de mais de um ativo. A estratégia multi-asset é interessante para aumentar a assertividades em alertas com elevada taxa de falsos-positivos. Assim, numa estratégia de detecção de malware, uma assinatura (sequência de bits) claramente associada a um malware, tipicamente com baixo índice de falso-positivos, pode levantar um alerta mesmo que identificada em um único ativo (single-asset); por outro lado, um padrão comportamental (por exemplo, aumento súbito de consumo de recursos por um dispositivos) pode não ser suficiente para um alerta, se identificado em apenas um ativo, mas certamente demanda atenção, se identificado simultaneamente em diversos ativos.

• **Alertas *single-technology versus* alerta *multi-technology***
Dizemos que um alerta é do tipo single-technology quando ele é constituído a partir de eventos oriundos de um único tipo de tecnologia - por exemplo, um anti-malware. Alertas multi-technology são constituídos a partir de eventos oriundos de mais de uma tecnologia - por exemplo, um anti-malware e um firewall. Assim como no caso dos alertas multi-asset, a correlação de eventos oriundos de múltiplas tecnologias permite incrementar índices de assertividade na detecção de ameaças. Por exemplo, um evento indicativo de malware em um endpoint pode ser reforçado por um alerta de firewall de que aquele endpoint está tentando acessar um endereço "denylist".

• **Alertas *single-environment versus* alerta *multi-environment***

Dizemos que um alerta é do tipo single-environment quando ele é constituído a partir de eventos oriundos de um único "ambiente" - por exemplo, uma única filial de organização ou uma única organização anti-malware. Alertas multi-environment são constituídos a partir de eventos oriundos de mais de um ambiente - por exemplo, várias filiais de uma organização ou mesmo, no caso de um SOC compartilhado, de várias organizações. Assim como no caso dos alertas multi-asset e multi-technology, a correlação de eventos oriundos de múltiplos ambientes permite incrementar índices de assertividade na detecção de ameaças. Por exemplo, um evento indicativo de malware em uma única organização pode representar um evento isolado, mas este mesmo evento em múltiplas organizações pode ser um indicativo de uma campanha orquestrada por um ator de ameaças avançadas e persistentes (APT - Advanced and Persistent Threat).

• **Alertas SOC-*only versus* alerta CTI-*enhanced***

Dizemos que um alerta é do tipo SOC-only quando ele é constituído apenas a partir de eventos oriundos de eventos de SOC. Alertas CTI-enhanced são constituídos a partir da correlação entre eventos oriundos de SOC com eventos de CTI (CyberThreat Intelligence). Mais uma vez, a correlação de eventos permite enriquecer o processo detecção de ameaças, na medida em que eventos de CTI . Seguindo a linha dos exemplos já apresentados, um evento indicativo de malware no SOC pode representar um evento isolado, mas se este evento ocorre de maneira simultânea a movimentações de um APT na deep web, podemos ter um indicativo de uma campanha orquestrada por este APT.

**Inteligência de Detecção**

Mais do que “coletar dados”, é preciso gerar inteligência a partir dos dados coletados das diversas tecnologias monitoradas. E aí, é importante reconhecer a importância de um entendimento aprofundado a respeito de cada tecnologia. Concretamente, isso significa que, se o SOC monitora um conjunto de tecnologias de borda baseadas em um determinado modelo de firewall, isso significa que o time do SOC deve possuir especialistas naquele modelo de firewall, de modo a tratar adequadamente os eventos e alertas gerados a partir daquela tecnologia. E isso vale para cada uma das centenas de tecnologias monitoradas - tecnologias de nuvem, endpoints, ambientes de colaboração dentre muitos outros.

## Organização do SOC Clavis

Como a maioria das Centrais de Operações de Segurança, o SOC Clavis está organizado em diversos times e estruturado em camadas de atendimento associadas a um fluxo que se inicia nas camadas inferiores (Nível 1) e segue para as camadas superiores (Nível 2 e, possivelmente, Nível 3). No entanto, conforme vimos discutindo ao longo deste e-book, a instanciação de atividades no SOC nem sempre é decorrência de um alerta ou incidente de segurança - mas pode ser parte de um planejamento de ações proativas de fortalecimento de segurança.

Descrevemos, a seguir, como está organizado o SOC da Clavis:

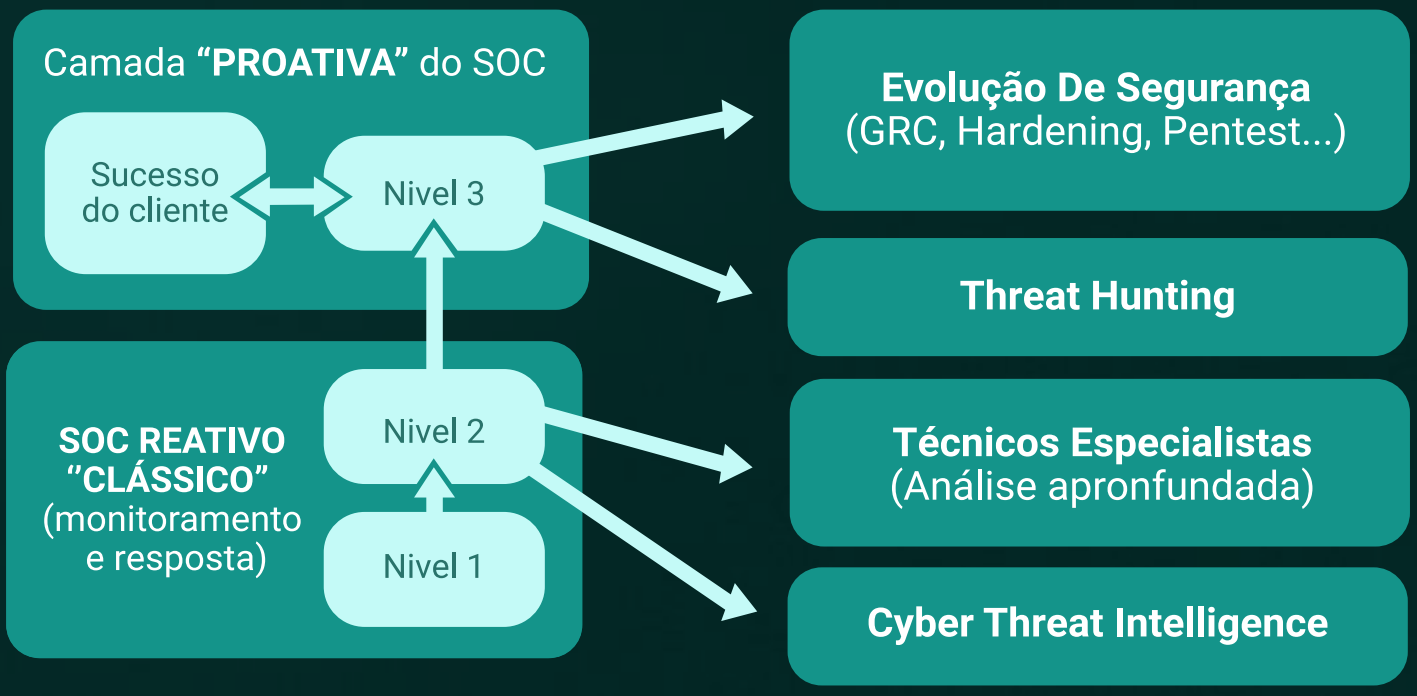
• **Nível 1 (N1): Monitoramento, Análise, Triagem e Escalada**

Trata-se do primeiro time acionado a partir de alertas gerados pelo Octopus. Este time permanece em operação 24 horas por dia, monitorando e dando um primeiro tratamento aos alertas gerados pelo Octopus - e mesmo que grande parte dos alertas mais simples já tenha um encaminhamento automático, cabe a este time monitorar a efetividade destes encaminhamentos. Para os alertas que demandam um tratamento manual, cabe ao time de N1 fazer a primeira análise e decidir sobre tipo de encaminhamento a ser dado - se é um alerta de baixa criticidade para o qual baste dar ciência às equipes responsáveis (no cliente e na Clavis) ou se é um alerta que pode estar associado a um cenário de ataque e que portanto demande o acionamento do time N2 e dos pontos focais no cliente.

• **Nível 2 (N2): Resposta a Incidentes**

Trata-se do time de especialistas em respostas a incidentes. Este time é acionado caso o time de N1 entenda que um determinado alerta (ou conjunto de alertas) é relevante e pode estar associado a um cenário de ataque. O time N2 possui especialistas capacitados a fazer uma análise mais aprofundada do cenário e dar início às ações de contenção de danos e recuperação de sistemas, além de apoiar na execução de playbooks de comunicação com clientes, imprensa e autoridades. Em termos de operação, o núcleo do time N2 é de especialistas em Resposta a Incidentes, mas o time tem à sua disposição nos outros times da Clavis todo um corpo de especialistas nas mais diversas tecnologias, os quais poderão ser acionados durante a resposta a incidentes. Assim, se ao longo da Resposta a Incidentes identifica-se a conveniência de realizar uma ação de hunting em um conjunto de tecnologias para se certificar da erradicação da ameaça (por exemplo, um conjunto de máquinas de desenvolvedores e um ambiente de DevOps), o time de especialistas em desenvolvimento seguro pode ser acionado para apoiar na execução de tal atividade.

• **Nível 3 (N3): Segurança Proativa**
Este é o time que mais claramente materializa a abordagem "proativa" proposta pelo SOC da Clavis - ainda que a visão proativa seja uma mentalidade (mindset) propagada por todas as equipes e squads envolvidas no atendimento ao cliente. O papel do time N3 é acompanhar o histórico de eventos, alertas e incidentes da organização e instanciar ações de fortalecimento de segurança - seja executando "huntings" (busca por indicadores de comprometimento e presença de atacantes) em ambientes da organização, seja acionando times especialistas para atuar sobre tecnologias específicas. Assim, por exemplo, se o longo do histórico de eventos de um cliente, o time N3 observa uma grande incidência de eventos relacionados a problemas de segurança na infraestrutura em nuvem, o time N3 atuará em parceria com o time de Sucesso do Cliente (externo ao SOC) para estabelecer uma ação de fortalecimento dos ambientes de nuvem da organização em questão.



## A Plataforma SOC-as-a-Service da Clavis

Para permitir ainda mais flexibilidade e agilidade no uso de seu SOC gerenciado, a Clavis disponibiliza sua plataforma tecnológica no modelo “as-a-Service”, minimizando as intervenções necessárias no ambiente do cliente e viabilizando um processo de *onboarding* extremamente rápido e eficiente.

O modelo SOC-as-a-Service é hoje o padrão de prestação de serviços da Clavis. Neste modelo, cada cliente possui uma instância do *software* Octopus na infraestrutura em nuvem da Clavis, operando em um modelo *single-tenant* com arquitetura segura e configurações personalizadas.

Como já mencionamos anteriormente, o Octopus possui capacidade de coleta de dados e análise de eventos de centenas de tecnologias. Cada cliente que inicia operações com a Clavis tem mapeadas as tecnologias mais relevantes do ponto de vista de monitoramento de segurança - sempre levando-se em conta a significância dos eventos gerados e o impacto de eventuais ameaças envolvendo aquela tecnologia. Uma vez definidas as coletas que serão realizadas, implanta-se uma instância do Octopus dedicada àquele cliente, coletando eventos e gerando alertas conforme definido - e direcionando-os ao time do SOC que será responsável por analisar tais eventos e alertas e tratá-los conforme *playbooks* previamente acordados com o cliente.

Capítulo 7

# Considerações finais: o futuro dos Centros de Operações de Segurança

Os Centros de Operações de Segurança estão evoluindo rapidamente para enfrentar as ameaças cibernéticas cada vez mais sofisticadas. Algumas das tendências para o futuro das SOCs incluem:

### 1. Automação e orquestração

A automação de processos repetitivos e a orquestração de respostas a incidentes são tendências importantes para SOCs. Utilizar tecnologias como SOAR (Security Orchestration, Automation, and Response) permite:

- **Redução do tempo de resposta:** respostas mais rápidas e eficientes aos incidentes;
- **Eficiência operacional:** liberação de analistas para se concentrarem em tarefas mais complexas;
- **Redução de erros humanos:** processos automatizados reduzem a possibilidade de erros.

### 2. Inteligência artificial (IA) e machine learning (ML)

A aplicação de IA e ML está se tornando crucial para a análise de grandes volumes de dados e a detecção de ameaças avançadas. Os benefícios incluem:

- **Detecção proativa:** identificação de ameaças emergentes antes que causem danos significativos;
- **Análise comportamental:** monitoramento de comportamentos anômalos que podem indicar uma ameaça;
- **Análise preditiva:** previsão de futuros vetores de ataque com base em padrões históricos.

### 3. Integração de Threat Intelligence

A integração de dados de *Threat Intelligence* em tempo real melhora a capacidade de um SOC de responder a ameaças:

- **Atualizações constantes:** dados frescos sobre ameaças conhecidas e emergentes;
- **Contextualização de incidentes:** melhor compreensão do contexto e da gravidade das ameaças;
- **Compartilhamento de informações:** colaboração com outras organizações para melhorar a defesa coletiva.

### 4. Segurança em nuvem

Com a migração de muitos serviços para a nuvem, as SOCs precisam adaptar suas estratégias para incluir a segurança de ambientes em nuvem:

• **Visibilidade na nuvem:** ferramentas que fornecem visibilidade e monitoramento em tempo real de ativos em nuvem;

• **Conformidade e governança:** garantia de que as operações em nuvem atendam aos requisitos regulatórios;

• **Proteção de dados:** implementação de medidas de segurança para proteger dados sensíveis armazenados na nuvem.

### 5. Resiliência cibernética e continuidade de negócios

Os SOCs estão focando mais na resiliência cibernética para garantir a continuidade dos negócios mesmo após um incidente de segurança:

• **Planos de resposta a incidentes:** desenvolvimento de planos detalhados para resposta a diferentes tipos de incidentes;

• **Testes de *stress* e simulações:** realização de exercícios regulares para testar a eficácia dos planos de resposta;

• **Recuperação rápida:** estratégias para rápida recuperação e restauração das operações após um ataque.

### 6. Segurança Zero Trust

A adoção do modelo de segurança Zero Trust está se tornando comum, em que a confiança é continuamente verificada e nenhum usuário ou dispositivo é considerado confiável por padrão:

• **Autenticação contínua:** verificação contínua da identidade dos usuários e dispositivos;

• **Segmentação de rede:** redução de superfícies de ataque através da segmentação e isolamento de redes;

• **Acesso mínimo necessário:** garantia de que os usuários tenham apenas o acesso estritamente necessário para suas funções.

**7. Colaboração e compartilhamento de informações**
Com a migração de muitos serviços para a nuvem, as SOCs precisam adaptar suas estratégias para incluir a segurança de ambientes em nuvem:

• **Comunidades de segurança:** participação em grupos e redes de compartilhamento de inteligência;

• **Plataformas colaborativas:** uso de plataformas que facilitam o compartilhamento de informações e coordenação de respostas.

**8. Foco em habilidades e treinamento**
A formação e retenção de talentos qualificados são desafios constantes:

• **Programas de treinamento:** desenvolvimento contínuo de programas de treinamento para atualizar as habilidades dos analistas;

• **Certificações e educação:** incentivo a certificações e cursos de especialização para a equipe de segurança;

• **Simulações e exercícios:** uso de simulações de ataque e exercícios práticos para preparar a equipe para cenários reais.

Capítulo 8

# Para saber mais

## Conceitos básicos de SOC:

**LIVRO**

### "The practice of network security monitoring: understanding incident detection and response"

**Autor: Richard Bejtlich**
Descrição: este livro fornece uma visão prática sobre a monitoração de segurança de rede e resposta a incidentes. Richard Bejtlich, um especialista respeitado na área, oferece uma abordagem prática e detalhada sobre como configurar e operar um SOC.

LIVRO

## “Security Operations Center: building, operating, and maintaining your SOC”

**Autores: Joseph Muniz, Gary McIntyre e Nadhem AlFardan**
Descrição: este livro cobre todos os aspectos de construção, operação e manutenção de um SOC. Aborda desde a arquitetura e tecnologia até processos e pessoal, oferecendo uma referência abrangente para qualquer pessoa interessada em operar um SOC.

LIVRO

## “Intelligence-driven incident response: outwitting the adversary”

**Autores: Scott J. Roberts e Rebekah Brown**
Descrição: este livro foca na resposta a incidentes baseada em inteligência, um conceito crucial para operações eficientes em um SOC. Os autores discutem como coletar, analisar e usar informações de inteligência para melhorar a resposta a incidentes.

LIVRO

## “SOC 2.0: Managing advanced threats with a unified security architecture”

**Autor: Dinesh Chandra**
Descrição: este livro discute a evolução dos SOCs e a necessidade de uma arquitetura de segurança unificada para gerenciar ameaças avançadas. É uma leitura essencial para entender os desafios modernos e as soluções para a operação de SOCs.

LIVRO

### “Cybersecurity Ops with bash”

**Autor: Paul Troncone e Carl Albing**
Descrição: este livro oferece uma abordagem prática ao uso de *scripts bash* para operações de segurança cibernética, uma habilidade útil para profissionais que trabalham em SOCs. Ele cobre automação de tarefas, coleta de dados e outras técnicas úteis.

## Conceitos básicos sobre SIEM:

LIVRO

### “Security Information and Event Management (SIEM) implementation”

**Autor: David Miller**
Descrição: este livro é uma referência abrangente para a implementação de SIEM. Ele cobre desde a arquitetura e o design até a configuração e o gerenciamento de um sistema SIEM. Inclui exemplos práticos e estudos de caso.

LIVRO

### “Designing and Building Security Operations Center”

**Autores: David Nathans**
Descrição: embora este livro seja focado em SOC, ele tem uma seção dedicada ao SIEM, cobrindo a seleção, implementação e otimização de soluções SIEM no contexto de um SOC.

LIVRO

## “Security Information and Event Management (SIEM) handbook”

**Autor: Jae Chung e Adam Powers**
Descrição: este livro fornece uma visão geral dos conceitos de SIEM, incluindo coleta de *logs*, correlação de eventos, gerenciamento de incidentes e conformidade. É uma boa introdução para quem está começando na área.

LIVRO

## “Applied SIEM: integrating Security Information and Event Management”

**Autor: Jay Chen**
Descrição: este livro é um guia prático para a integração e aplicação de SIEM em ambientes corporativos. Ele aborda estratégias para maximizar a eficiência do SIEM, incluindo a integração com outras ferramentas de segurança.

LIVRO

## “The log management imperative: using SIEM technology to distill security & compliance information”

**Autor: Phillip Q. Maier**
Descrição: este livro enfatiza a importância do gerenciamento de *logs* como base para uma solução eficaz de SIEM. Ele cobre técnicas para coletar, armazenar e analisar *logs* para melhorar a segurança e conformidade.

## Futuro dos SOC

LIVRO

### Automação e orquestração
### “Security orchestration, automation, and response for dummies”

**Autor: Joseph Krull**
Descrição: este livro oferece uma introdução acessível e prática ao uso de SOAR (Security Orchestration, Automation, and Response) para melhorar a eficiência e a eficácia das operações de segurança.

LIVRO

### Inteligência artificial e machine learning
### “Artificial intelligence in cybersecurity”

**Autores: Mark Stamp e Richard Alan Clark**
Descrição: este livro aborda como a inteligência artificial e o machine learning podem ser aplicados para melhorar a segurança cibernética, com exemplos e estudos de caso práticos.

LIVRO

### Integração de Threat Intelligence
### “The Threat Intelligence handbook”

**Autores: Chris Cochran e Ron Eddings**
Descrição: este livro oferece uma visão abrangente sobre a coleta, análise e aplicação de Threat Intelligence em operações de segurança.

LIVRO

**Segurança em nuvem**
**"Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS)"**

**Autor: Michael J. Kavis**
Descrição: este livro detalha as melhores práticas para projetar e implementar soluções seguras em ambientes de nuvem, abordando desafios e soluções específicas.

LIVRO

**Resiliência Cibernética e Continuidade de Negócios**
**"Cyber resilience: how to protect your business in the global risk environment"**

**Autor: Phil Mennie**
Descrição: este livro fornece estratégias práticas para desenvolver a resiliência cibernética e garantir a continuidade dos negócios em um ambiente de risco global.

LIVRO

**Segurança Zero Trust**
**"Zero Trust networks: building secure systems in untrusted networks"**

**Autores: Evan Gilman e Doug Barth**
Descrição: este livro apresenta o modelo de segurança Zero Trust, explicando como construir redes seguras em que nenhum dispositivo ou usuário é implicitamente confiável.

LIVRO

## Colaboração e compartilhamento de informações

**"Collaborative Cyber Threat Intelligence: detecting and responding to advanced cyber attacks at the national level"**

**Autores: Florian Skopik e Paul T. Kilpatrick**
Descrição: este livro discute a importância da colaboração no compartilhamento de inteligência de ameaças cibernéticas e como implementá-la eficazmente.

LIVRO

## Habilidades e treinamento

**"The cybersecurity talent gap: addressing skills shortages and meeting future demand"**

**Autores: Heather Adkins, Betsy Bevilacqua e Megan Ruthven**
Descrição: este livro aborda a lacuna de talentos em cibersegurança, oferecendo estratégias para treinamento, desenvolvimento e retenção de talentos na área de segurança cibernética.

## Contato com a Clavis

A Clavis está sempre à disposição para agendar reuniões sobre suas soluções. Entre em contato conosco por qualquer um dos nossos canais disponíveis: formulário no site, e-mail ou telefone, incluindo atendimento por voz e WhatsApp.

**E-mail:** contato@clavis.com.br
**Telefone:** (21) 2210-6061 | (21) 2561-0867
**Whatsapp:** (21) 97915-9602 | (21) 96551-2568