Elevando a Cibersegurança ao Próximo Nível

HUB SECURITY

Descubra as Ameaças Ocultas

20 24 WTR WORKSHOP TECNOLOGIAS DE REDE PoPBA

Antonio Fernandes

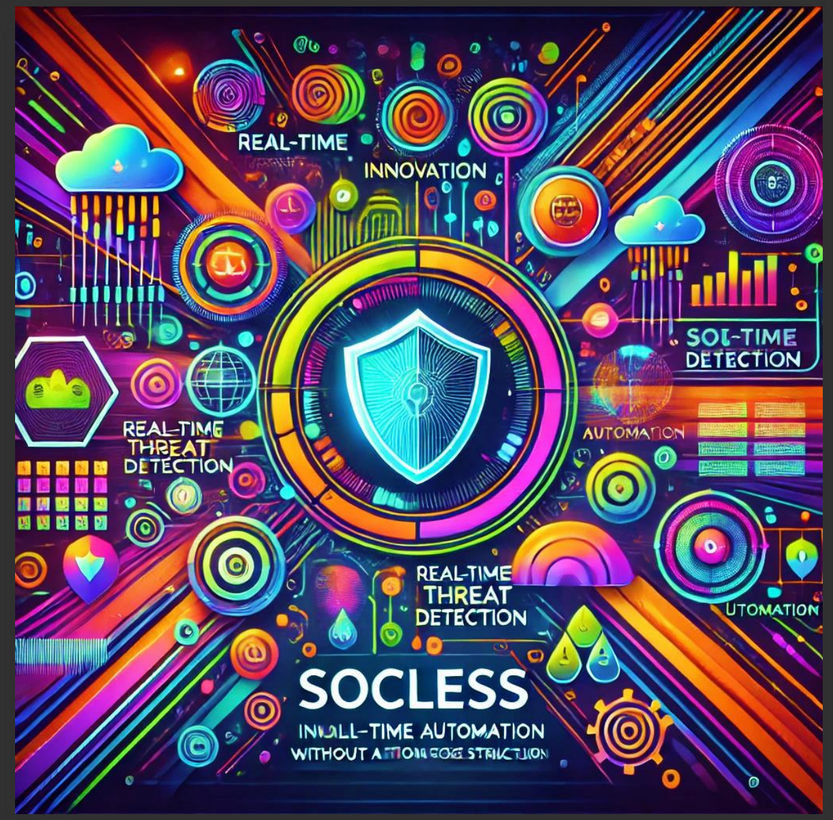
E-Mail: Antonio.Fernandes@HUBSecurity.com.br
Av. Paulista, 1636 - Sala 1504 - Cerqueira César
São Paulo - SP - CEP 01310-200
https://www.hubsecurity.com.br

E-Mail: Antonio.Fernandes@HUBSecurity.com.br
Av. Paulista, 1636 - Sala 1504 - Cerqueira César
São Paulo - SP - CEP 01310-200
https://www.hubsecurity.com.br

HUB SECURITY
Descubra as Ameaças Ocultas

Sobre o HUB Security:

O **HUB Security** é uma empresa inovadora que nasce trazendo ao mercado o conceito **SOCless,** que permite as organizações monitorem e protejam seus ativos digitais de forma contínua, proativa e em tempo real.



Missão e Objetivo:

A missão do **HUB Security** é expandir e implementar soluções robustas de cibersegurança no Brasil e na América Latina, que proporcionem uma **proteção contra ameaças cibernéticas ocultas.**

Os Desafios de Segurança segundo o Gartner

HUB SECURITY
Descubra as Ameaças Ocultas

Gartner

Crescimento das Ameaças Cibernéticas:

O **Gartner** relata que, **com a evolução do 5G, IA (Inteligência Artificial) e IoT (Internet das Coisas), a superfície de ataque das empresas está se expandindo rapidamente**, tornando-as mais vulneráveis a ameaças cibernéticas sofisticadas.

Desafios Crescentes para Organizações:

O **Gartner** relata que, as empresas estão enfrentando um volume maior de ataques e ameaças mais complexas, com métodos de invasão cada vez mais difíceis de detectar e mitigar.

Evolução para Soluções Automatizadas:

O **Gartner** aponta para a necessidade de adoção de soluções mais automatizadas e inteligentes, que **permitam a detecção contínua de ameaças e uma resposta eficiente, em tempo real**.

O Cenário Atual da Cibersegurança

HUB SECURITY
Descubra as Ameaças Ocultas

Os Desafios de Segurança para Provedores de Internet (ISPs)

HUB SECURITY
Descubra as Ameaças Ocultas

Superfície de Ataque Ampliada:

O **crescimento de dispositivos conectados (IoT), redes 5G, e a demanda por serviços mais rápidos** e acessíveis aumentam os riscos.

Gestão de Grandes Volumes de Dados:

ISPs são responsáveis por gerenciar **grandes volumes de tráfego de dados, o que os torna alvos prioritários para ataques cibernéticos,** como DDoS e tentativas de invasão de redes de clientes.

Conformidade com Regulamentações:

ISPs precisam garantir a conformidade com regulamentações de cibersegurança, como **a Resolução nº 740 da ANATEL, que estabelece diretrizes rigorosas para a proteção da infraestrutura** e dos dados dos consumidores.

Escalabilidade e Eficiência:

Os ISPs também enfrentam **o desafio de implementar soluções de segurança que sejam escaláveis e que possam acompanhar o crescimento constante da infraestrutura**, sem comprometer a eficiência dos serviços.

NADA DE
BOM ACONTECE
QUANDO VOCÊ
ESTÁ EM CONTATO
COM O ADVERSÁRIO

O Cenário Atual da Cibersegurança

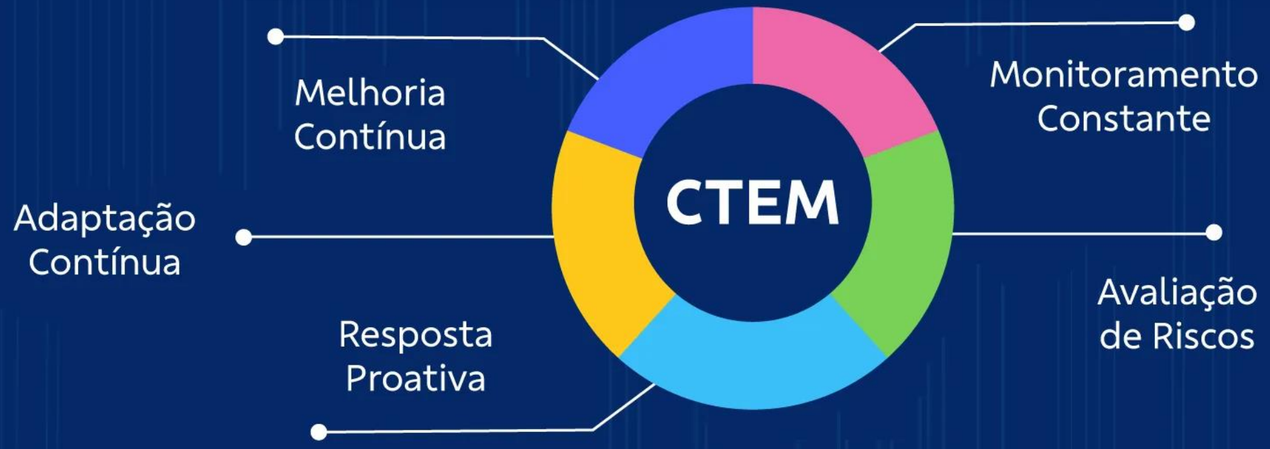
HUB SECURITY
Descubra as Ameaças Ocultas

Gartner

"Até 2026, as organizações que priorizarem seus investimentos em segurança com base em um programa de gerenciamento de exposição contínua terão 3 vezes menos probabilidade de sofrer uma violação."

O que é Gestão Contínua de Exposição a Ameaças (CTEM)

A CTEM é uma abordagem de gerenciamento de riscos que envolve a avaliação contínua e a gestão proativa das ameaças cibernéticas que uma organização enfrenta ao longo do tempo, identificando e corrigindo ameaças antes mesmo que causem danos.



Com o CTEM, equipes de segurança recebem alertas em tempo real sobre possíveis ameaças, permitindo uma ação rápida e decisiva para proteger os sistemas da organização.

Além de identificar ameaças, o CTEM também ajuda a priorizar quais problemas devem ser resolvidos primeiro. Isso torna mais fácil para as equipes de segurança saberem onde concentrar seus esforços para manter os sistemas seguros.

Benefícios da Gestão Contínua de Exposição a Ameaças (CTEM):

HUB SECURITY
Descubra as Ameaças Ocultas

1 **Proatividade:** Permite identificar e mitigar ameaças cibernéticas antes que causem danos significativos.

2 **Adaptabilidade:** Proporciona uma abordagem dinâmica para lidar com ameaças em constante evolução.

3 **Eficiência:** Ajuda a priorizar ações de segurança com base na gravidade e no impacto dos riscos.

4 **Melhoria Contínua:** Facilita a aprendizagem e aprimoramento contínuos das práticas de segurança cibernética.

5 **Redução de Riscos:** Contribui para a redução de violações e prejuízos financeiros associados a ataques cibernéticos.

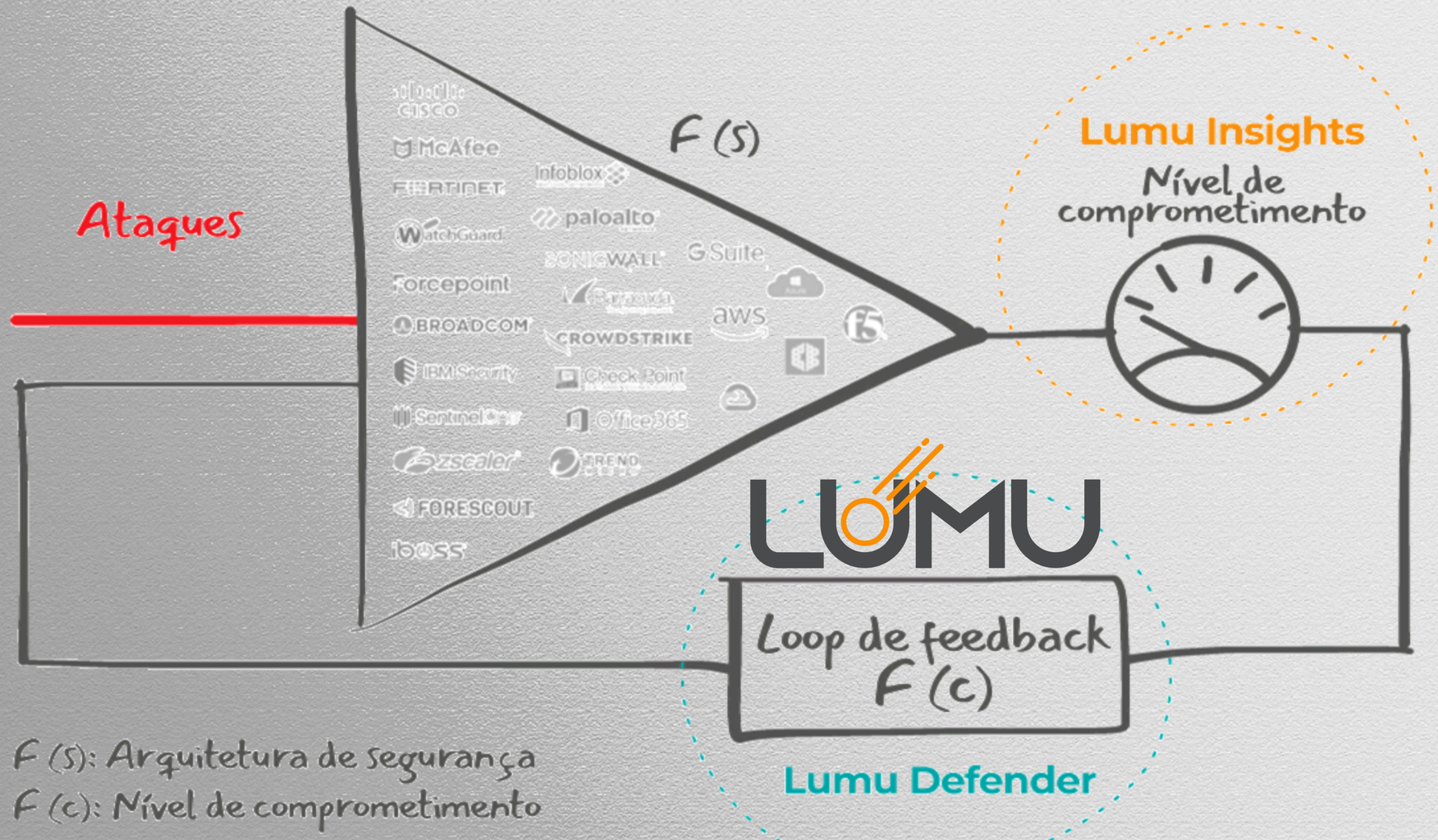
6 **Proteção da Reputação:** Ajuda a proteger a reputação da organização no mercado ao demonstrar comprometimento com a segurança dos dados.

7 **Conformidade:** Auxilia na conformidade com regulamentos e padrões de segurança cibernética.

A SOLUÇÃO PARA ISPs

Como a Tecnologia LUMU Endereça o Modelo CTEM

Continuous Compromise Assessment™:



A **LUMU** aplica a **Avaliação Contínua De Comprometimentos**, que é a base do *Modelo CTEM*, *monitorando o tráfego de rede em tempo real e identificando ameaças ocultas, antes que causem danos.*

A **fonte da verdade** está nos **METADADOS** da rede.

LUMU

HUB SECURITY

Descubra as Ameaças Ocultas

A SOLUÇÃO PARA ISPs

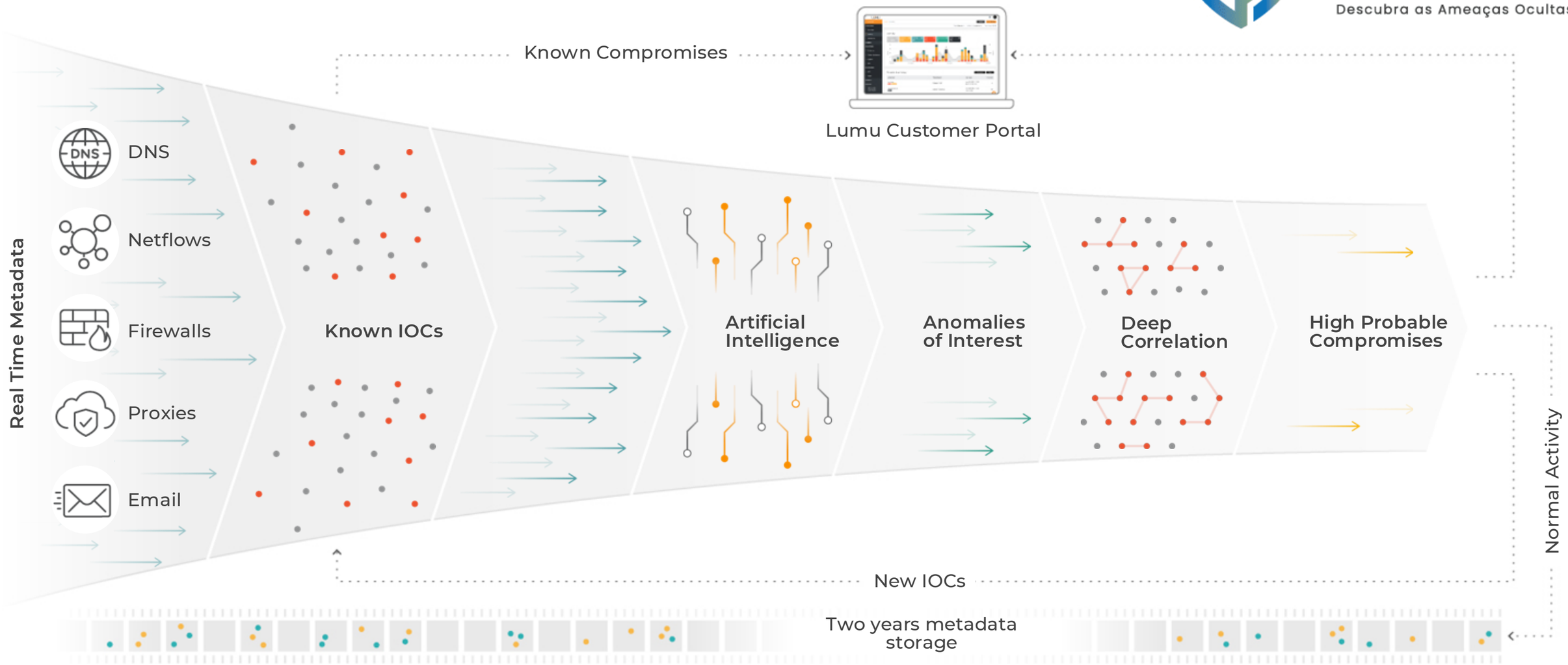
Como a Tecnologia LUMU Endereça o Modelo CTEM

HUB SECURITY
Descubra as Ameaças Ocultas

Coleta de Metadados

O Processo de Iluminação

HUB SECURITY
Descubra as Ameaças Ocultas



LUMU

A SOLUÇÃO PARA ISPs

Como a Tecnologia LUMU Endereça o Modelo CTEM

Continuous Compromise Assessment™:

HUB SECURITY
Descubra as Ameaças Ocultas

LUMU

Busca constante em tempo real das ameaças

Implanta detecção contínua de comprometimento e bloqueia os adversários em milissegundos

Mede a efetividade, faz as correções e atualizações automáticas de toda pilha de segurança e oferece feedback

Elevando a Cibersegurança para (ISPs) ao Próximo Nível

HUB SECURITY
Descubra as Ameaças Ocultas

Solução Inovadora e Automatizada:
A **LUMU** representa o próximo nível em cibersegurança para ISPs, oferecendo automação avançada, monitoramento contínuo e detecção proativa de ameaças.

Capacidades Avançadas de Detecção e Resposta:
A combinação do Modelo CTEM e da plataforma **LUMU** permite que os ISPs detectem e respondam rapidamente a ameaças, antes que causem interrupções ou danos aos serviços.

LUMU

Escalabilidade e Eficiência:
Com a **LUMU**, os ISPs podem escalar suas soluções de cibersegurança sem comprometer a eficiência operacional, garantindo a proteção contínua das redes e a integridade dos dados dos clientes.

Preparação para o Futuro:
Ao adotar a tecnologia **LUMU**, os ISPs estarão prontos para enfrentar os desafios emergentes da cibersegurança no ambiente 5G, IoT e além, mantendo-se à frente das ameaças e regulamentos.

Dashboard Completo e Detalhado

Elevando a Cibersegurança para (ISPs) ao Próximo Nível

HUB SECURITY
Descubra as Ameaças Ocultas

Modelo de Maturidade SecOps

LUMU

0

1
Visibilidade inicial nos firewalls e IDS/IPS

2
Maior visibilidade, Resposta interna um pouco madura, porém manual contra as ameaças.

3
Visibilidade completa, mas com automação ade resposta a ameaças limitadas.

4
Totalmente Automatizado, pronto para ser um SOCless.

VAMOS TRAZER LUZ AO SEU AMBIENTE DE CIBER SEGURANÇA?

HUB SECURITY

Descubra as Ameaças Ocultas

Antonio Fernandes

E-Mail: Antonio.Fernandes@HUBSecurity.com.br
Av. Paulista, 1636 - Sala 1504 - Cerqueira César
São Paulo - SP - CEP 01310-200
https://www.hubsecurity.com.br

LUMU

Sobre a Lumu

HUB SECURITY
Descubra as Ameaças Ocultas

1,270
Clientes

4.8 trillion+
Registros de Metadados Analisados

736 million+
Contatos Maliciosos Detectados

ESG
Enterprise Strategy Group

"CISOs looking for security analytics and operations help may want to seek out Lumu and evaluate how Lumu can help them with continuous compromise assessment."
– ESG Showcase: Continuous Compromise Assessment, A Missing Link in Cybersecurity

Gartner

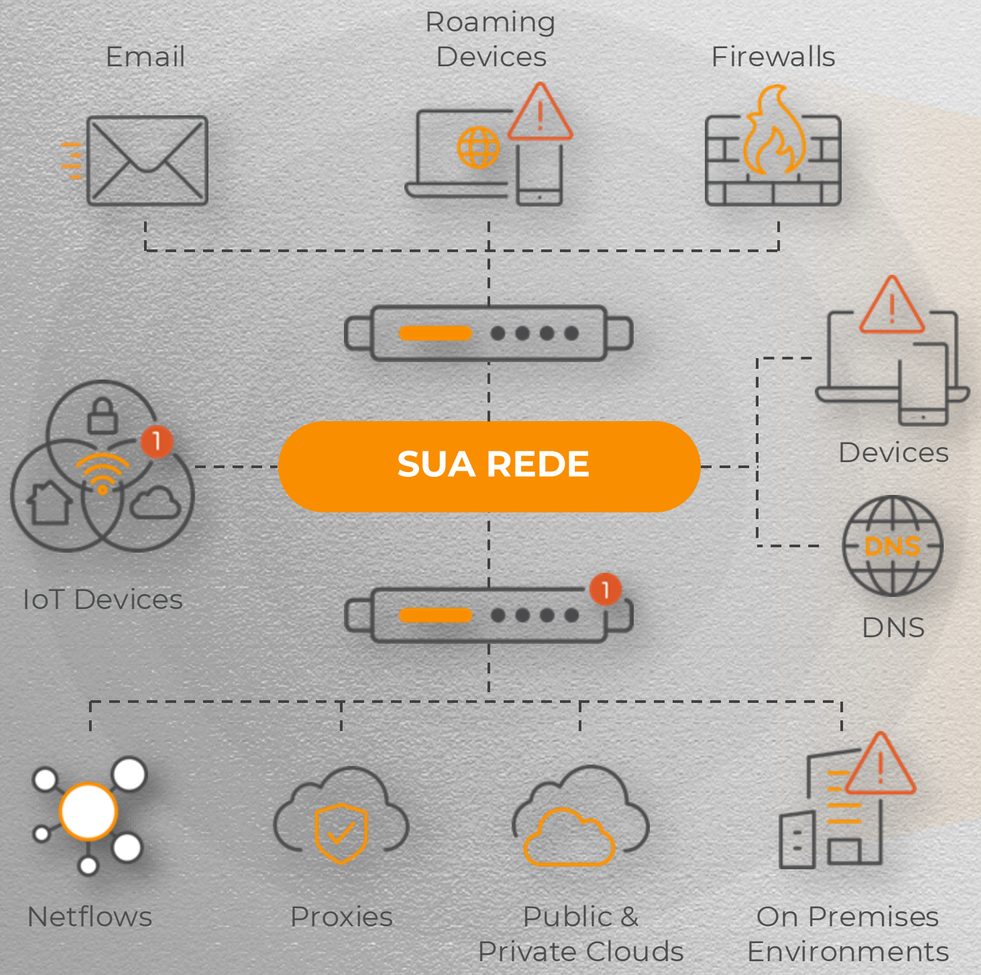
"Many Gartner clients reported that NDR tools have detected suspicious network traffic that other perimeter security tools have missed."
– GARTNER 2020 Network Detection and Response Market Guide

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

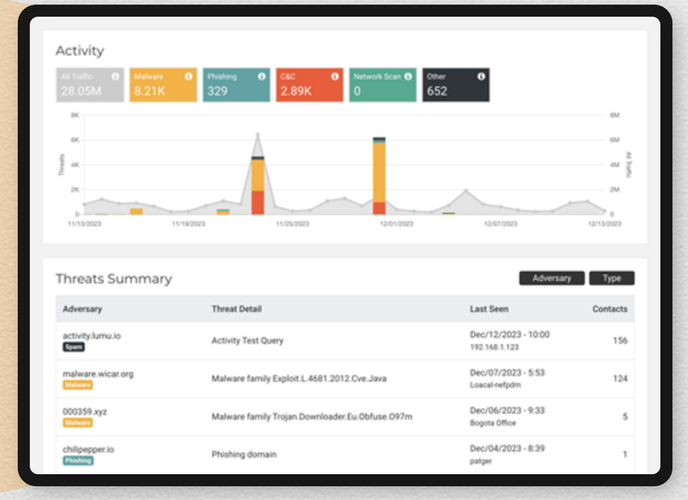
FORGEPOINT | BIP CAPITAL | Opportunity Fund | Exceptional Capital | LUMU

A Sua Rede Está Enviando Sinais

A Lumu Interpreta e Processa os Dados Para Você



NETWORK DATA



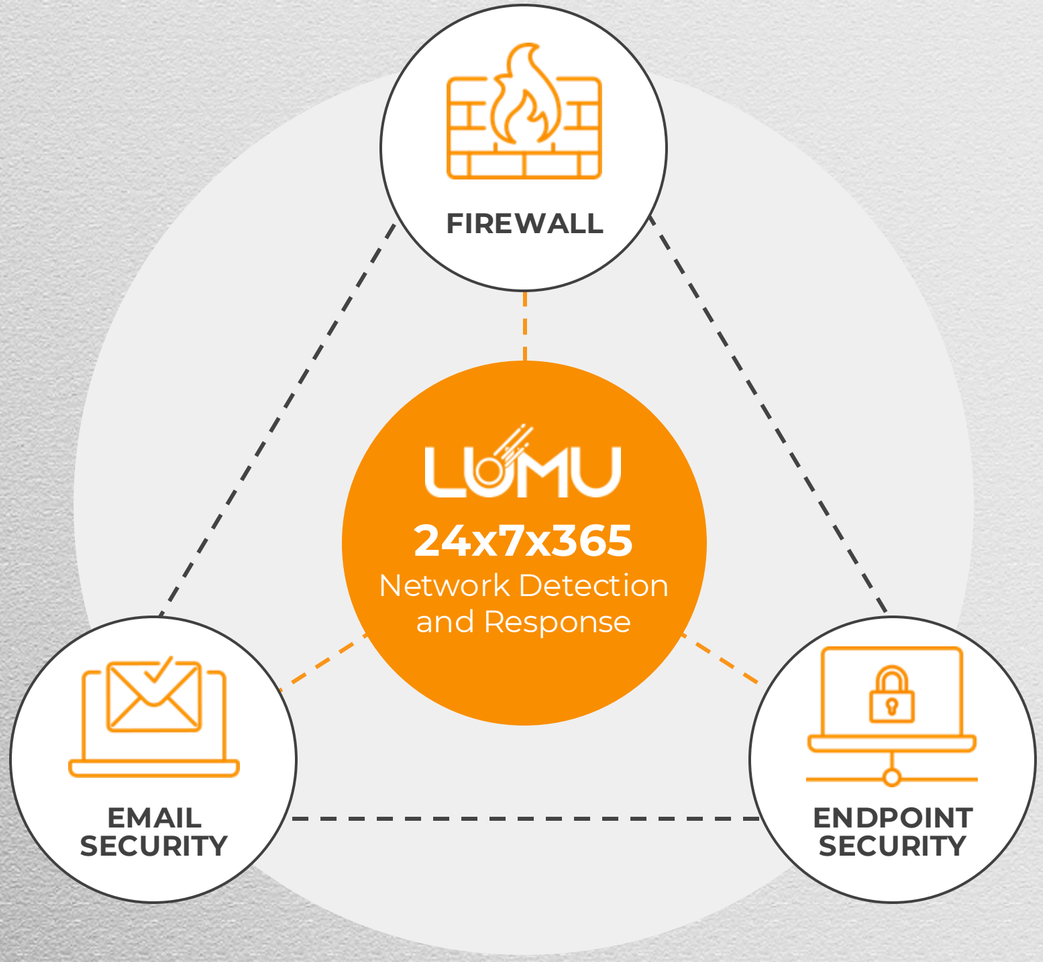
HUB SECURITY
Descubra as Ameaças Ocultas

LUMU

Detecte e Responda a Ameaças em Tempo Real

Coloque a Sua Pilha de Segurança Para Trabalhar

HUB SECURITY
Descubra as Ameaças Ocultas



LUMU

Coleta de Metadados

AMBIENTES LOCAIS

Virtual Appliance

DNS • Fluxos de rede • Logs

Custom Collector API

Soluções de terceiros

SIEM • EDR • CLM

NUVENS PÚBLICAS E PRIVADAS

Cloud Collectors

DISPOSITIVOS REMOTOS

Agentes Nativos Cyber

macOS / Windows

Integração de VPN/SDP

Eficácia Comprovada

HUB SECURITY
Descubra as Ameaças Ocultas

Detecções da rede

- Escaneamento de portas
- Varredura de portas
- Escaneamento interno reverso de lookup de DNS
- Escaneamento de porta UDP
- Escaneamento de porta TCP
- Phishing
- Adware
- Download de malware ligado ao website
- Download drive-by
- Downloaders de malwares baseados em macros, atividades anormais na web ou em anúncios
- Mineração de criptomoedas
- Cryptojacking
- Spam de saída
- Acesso remoto externo
- Atividade de domínio suspeito
- Atualização de malware
- Peer-to-peer
- Recebendo instruções
- HTTP suspeita
- HTTP furtiva (stealth)
- Atividade de TOR
- SSH reverso
- DGA (Algoritmo de Geração de Domínios)
- Precursores de ransomware
- Spambots

Táticas adversárias

- Reconhecimento
- Desenvolvimento de recursos
- Acesso inicial
- Execução
- Persistência
- Escalonamento de privilégios
- Evasão de defesas
- Acesso com credenciais
- Descoberta
- Movimento lateral
- Coleção
- Comando e Controle
- Exfiltração
- Impacto

Grupos

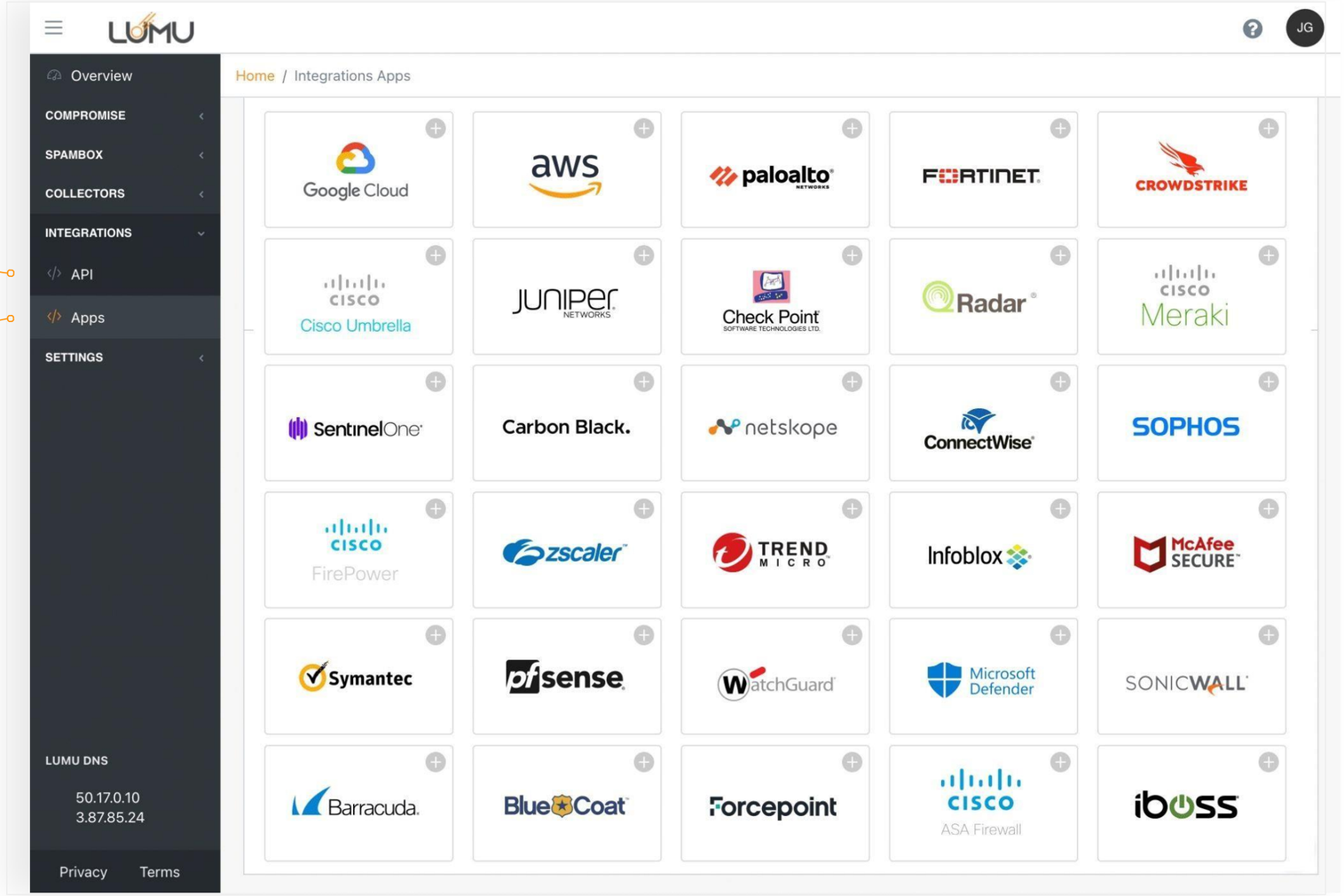
- admin@338
- Ajax Security Team
- Andariel
- APT-C-36
- APT1 ~41
- Axiom
- BackdoorDiplomacy
- BlackOasis
- Blacktech
- Blue Mockingbird
- Carbanak
- Chimera
- Cobalt Group
- Dark Caracal
- Darkhotel
- DarkPanda
- Dragonfly
- Fox Kitten
- Frankenstein
- Gallmaker
- Group5
- HoneyBee
- Lazarus Group
- Machete
- Night Dragon
- Promethium
- Windshift
- Zirconium

LUMU

Sua Arquitetura de Segurança na Mesma Página

Nossa **API aberta** permite a integração com todo o seu ecossistema de cibersegurança.

Apps prontas para usar que conectam sua arquitetura num par de cliques.



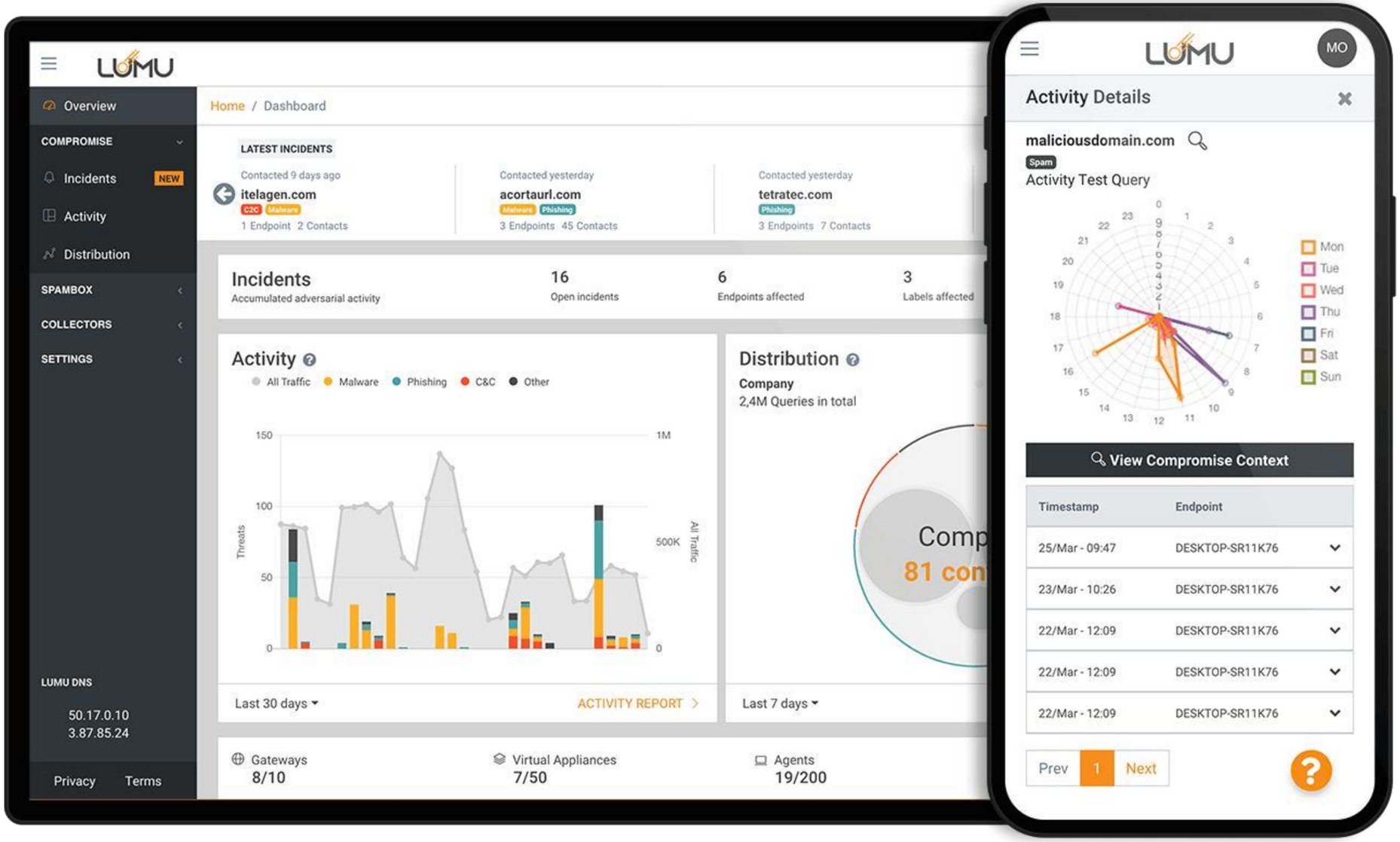
A Lumu faz o Trabalho Duro para Você

	1 Coleta de Metadados da Rede	2 Identificação de Atividade Maliciosa	3 Criação de incidente	4 Resposta a Ameaça
Sem a Lumu	Multiplas ferramentas necessárias	Utilização do corpo técnico limitado ao horário CLT	Triagem complexa	Manual e com propensão à erros
Com a Lumu	✓ **Coleta automática de metadados**	✓ **Identificação contínua de atividade maliciosa, trabalhando 24x7x365**	✓ **Criação automática e com contexto**	✓ **Automática com uso das ferramentas existentes**

LUMU

HUB SECURITY
Descubra as Ameaças Ocultas

Demo ao Vivo



LUMU

HUB SECURITY
Descubra as Ameaças Ocultas

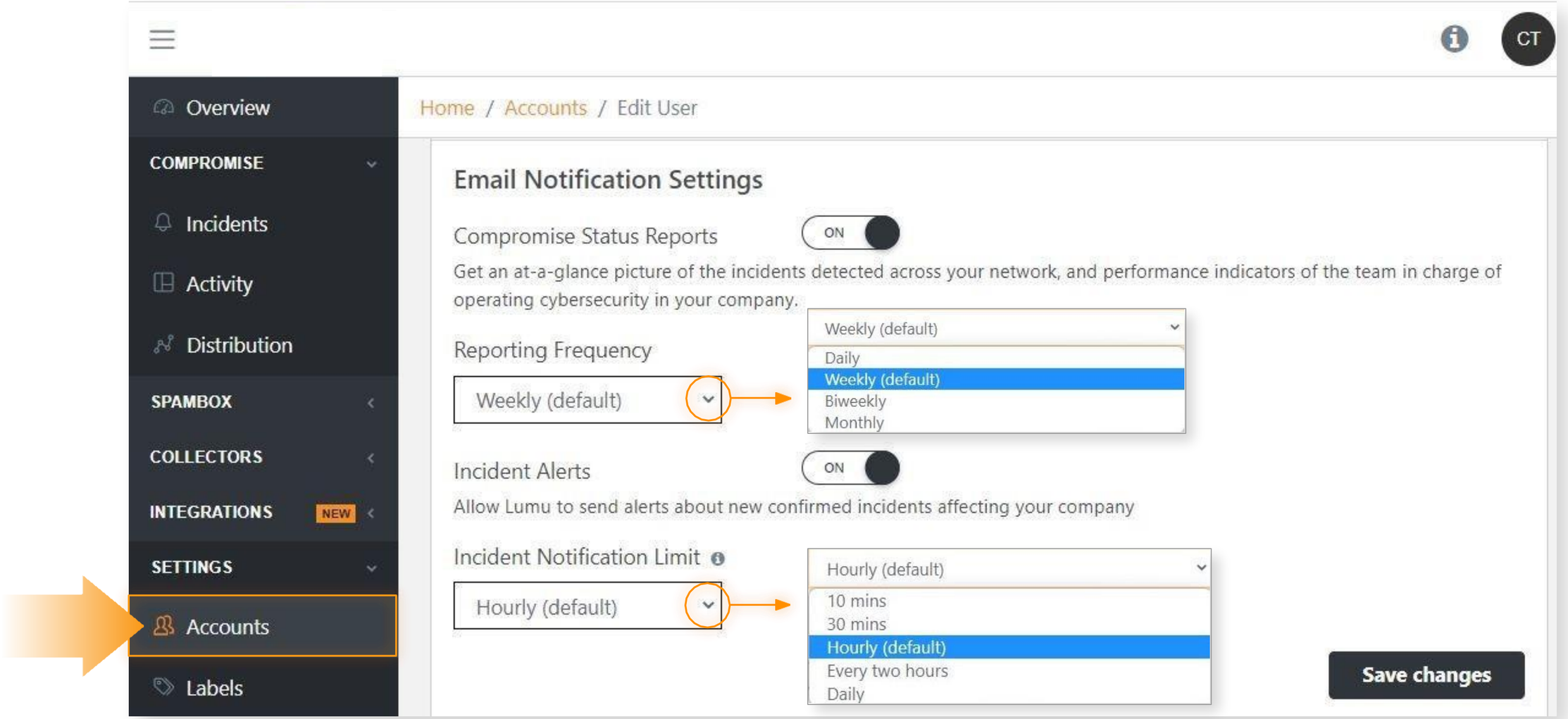
Relatórios Periódicos Automatizados

Detecte e identifique com precisão os ativos de TI que demandam ação imediata para eliminar o comprometimento

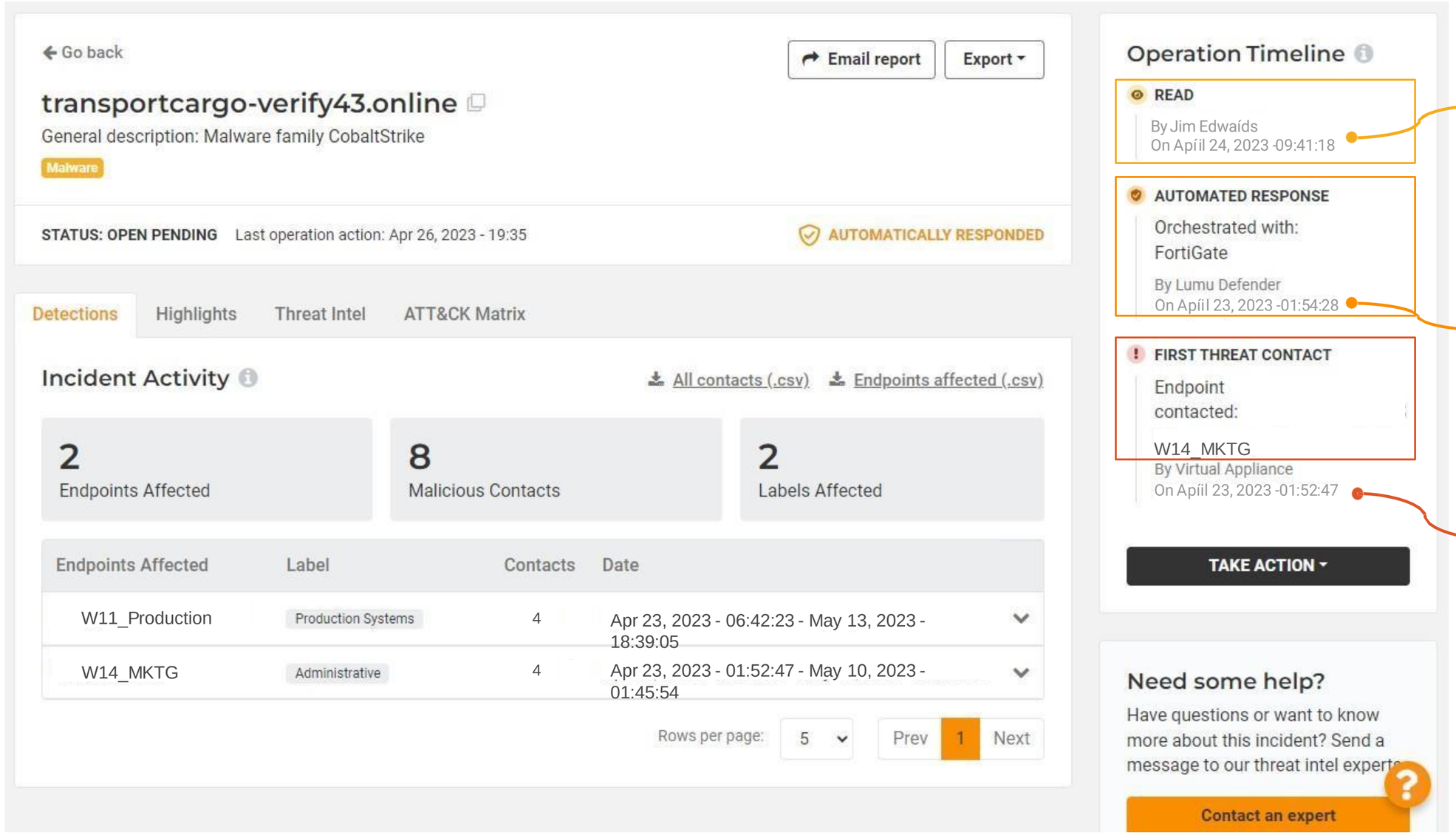
Meça a efetividade da sua estratégia de resposta a incidentes

Acompanhe o seu progresso no caminho para o estado de comprometimento zero

Habilite Relatórios nos e-mails



Automação em ação



3

Incidente visto pelo operador de cibersegurança na segunda-feira, 24 de abril (32 horas depois)

2

Ameaça bloqueada pela plataforma Defender 2 minutos após o contato inicial.

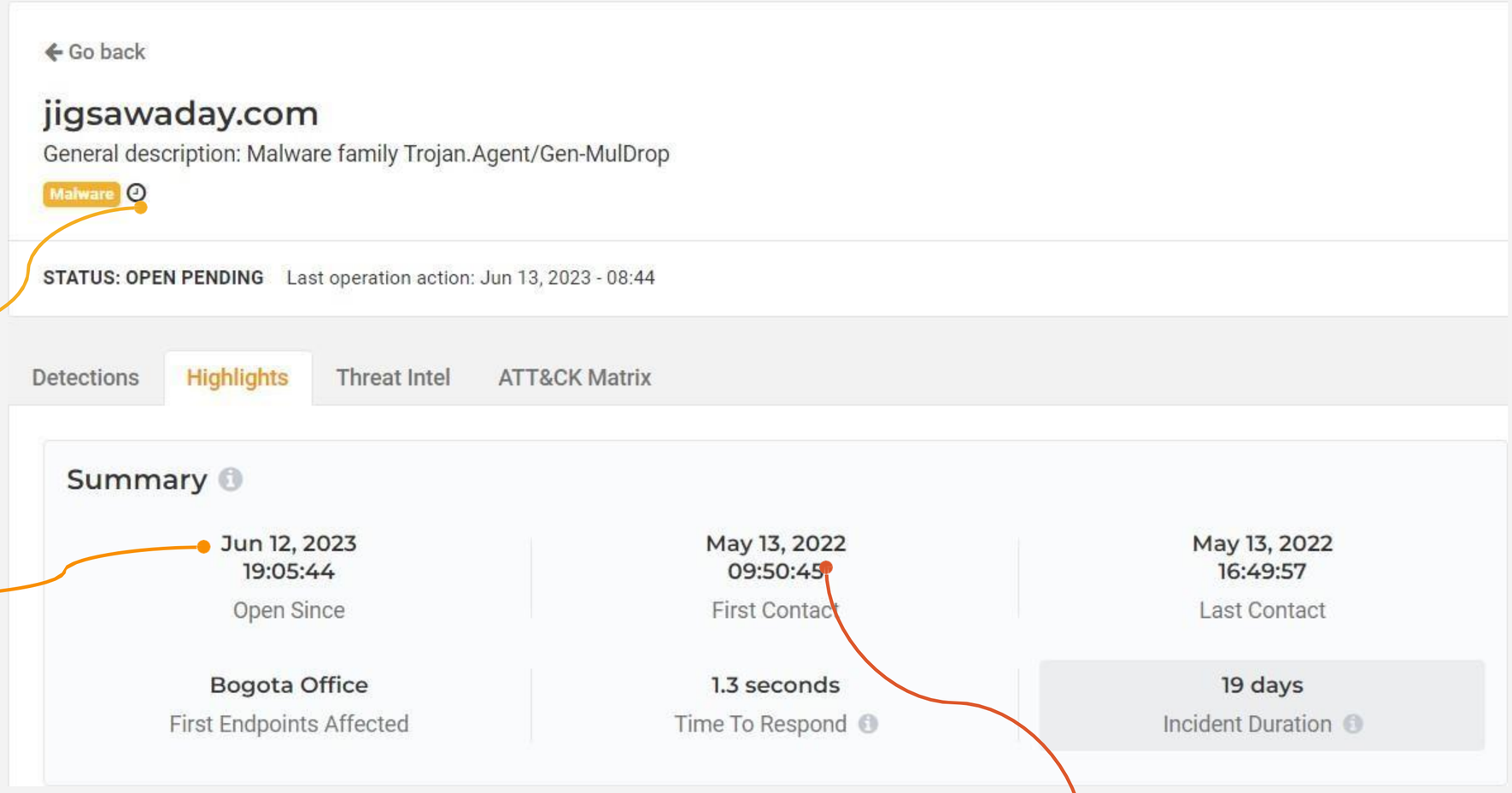
1

Ameaça inicialmente detectada na rede às 01h52 do dia 23 de abril (domingo)

Automação em ação - Detecção (MTTD)

1 Detecção registrada através da playback

2 Timestamp de abertura do incidente



Timestamp do primeiro contato. **+11 meses antes**

3

Alinhamento Total com o Framework do NIST

Reduzindo o excesso de alertas

Eficiência operacional > **Decisões baseadas em fatos e ameaças reais** > **Tranquilidade em saber o seu estado de comprometimento**

PERÍODO DE 20 DIAS

Taxa de alertas: **0.00000009%**

LUMU É o Seu Analista De Cibersegurança 24X7 Personalizado, somos um SOCless.

- Identifica e resolve **ameaças em tempo real**
- **Bloqueia o adversário** em sua jornada
- **Maximiza** a sua pilha de segurança existente
- **Te ajuda a ganhar tempo** no seu dia-a-dia

LUMU

Estudos e Pesquisas

INFOR CHANNEL SEÇÕES OPINIÃO ENVIE SEU TEXTO REVISTA DIGITAL VÍDEOS

Estudo da Lumu Technologies revela preocupação de líderes com Segurança no trabalho remoto

O Ciso Priorities Flashcard revela que 70% dos profissionais de Segurança Cibernética brasileiros consideram a medição de comprometimento uma prioridade, enquanto 60% entendem que a implementação de uma estratégia de Zero Trust é urgente

O recorte nacional do *CISO Priorities Flashcard* foi feito por meio de respostas voluntárias de 30 profissionais de segurança cibernética no Brasil – diretores de Segurança, Cisos ou similares – entre 18 de dezembro de 2021 e 20 de janeiro de 2022.

Outras conclusões do levantamento apontam que entre os CISOs entrevistados:

73% listam como prioridade o aprimoramento dos testes de segurança cibernética, além dos testes de penetração;
70% consideraram urgente medir a eficácia do ecossistema de segurança cibernética;
67% devem priorizar a adoção ou expansão da caça a ameaças;
63% percebem a necessidade de unificar a visibilidade das ameaças em todos os ativos;
63% planejam diminuir o tempo de detecção e resposta a ameaças;
60% têm como objetivo otimizar o gerenciamento de alertas do SOC;
57% declararam a avaliação de risco da cadeia de suprimentos urgente;
43% incluíram a aquisição de um seguro cibernético em sua lista de pendências;
40% consideraram terceirizar operações de segurança cibernética.

LUMU

HUB SECURITY Descubra as Ameaças Ocultas

Clientes

Bancos e Financeiras

Banco Falabella · Banco Ficohsa · TECVAL · Fidelity · Banco Pichincha · FLAR · CAFSA · Comédica · "Pablo Muñoz Vega" · Bladex · Banco de Loja · ach Colombia · Davivienda · paymentez · Diners Club International · Banco del Pacífico · BGR · San Francisco · Intercredit · Primerica · CreditOne Bank · Ocean Bank · Banco BMG · Puntos Colombia · Banco8op · Horizon Bank · Banco Austro · Silver Spoon

Varejo

Soriana · Cravioto Ferreterías · FIFCO · Titan · Ley · Grupo Monge · Abcdin · Dijon · Grupo Distelsa · AD Retail · Riba Smith · Zionsville Antique Mall · Nordic · GMT

Cia Elétricas

EDERSA · Biomax · AguasNuevas · Mexoil · terpel · cAp · aysa · Cammesa · Edesal · COPEC · Celsia

Mídia

SENTIDOS Comunicaciones Estratégicas · RCN Television · El Cronista

Turismo

Grupo Puntacana · Pontes Hotéis & Resorts

Governo e Entidades

Gobierno de Guatemala · Ministerio de Finanzas Públicas · El conocimiento es de todos · Minciencias · El futuro es de todos · Presidencia de la República · Agencia de Regulación y Control de las Telecomunicaciones · Superintendencia de Bancos de Panamá · OAB Pernambuco

Agronegócio

Empresas Polar · Toks · Wayne · Usina Cruangi · unibon · Grupo Calesa · Usina Serra Grande

Educação

childroots · MD Uniminuto · ESPE · Fundación Bolívar Davivienda · Christopher Columbus

Academias

MHS Labs · Falck · UTM · emi · Bodytech

Industria Textil

lintex · Aceros Arequipa

MSPs

Technology Group · Goldbeartech · Kemper Technology Consulting · Touchstone Security

Seguradoras

USIC · Seguros Bolívar · Mercantil Seguros · Colmena · Peña Verde · Kensington · Mercantil Andina

IT & Consulting

Accionplus · summa+ Consultores · Netuno · BGP · minsait · Apic · E-Crobar · Inverfas S.A. · Cintech · Fimpe · Smart Network Solutions · Soluciones Seguras · Teliko · International Consulting Group · Teleinformática · e-Safer

Logistica & Transportes

TPA · rentingcarz.com · Puerto Angamos · Grupo Parvi · Grupo LAAR

LUMU

HUB Security — Descubra as Ameaças Ocultas

Prêmios & Reconhecimentos

Fastest Growing Company of 2022

RSA Conference 2022 Products for MSPs/MSSPs

Winner - Continuous Compromise Assessment Category

NEW MOST INTERESTING Infosec Products June 2022

2021 GLOBEE AWARDS GRAND WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

CIO Bulletin

A RisiThg CompaThyto Watch 2021

Continuous Compromise Detection: "Robust Compromise Detection Products Offered"

CRN

10 Hottest Cybersecurity Startups Of 2021

CSO

Hottest new cybersecurity products at RSA Conference

EMA TECHNOLOGIES VENDOR TO WATCH MAY 2020

Avaliação da Plataforma

ESG
Enterprise Strategy Group

"Os CISOs que procuram análises de segurança e ajuda operacional podem querer procurar a Lumu e avaliar como eles podem ajudá-los com a avaliação contínua de comprometimento.."

–ESG Showcase: Continuous Compromise Assessment, A Missing Link in Cybersecurity

Gartner

"Muitos clientes do Gartner relataram que as ferramentas NDR detectaram tráfego de rede suspeito que outras ferramentas de segurança de perímetro não conseguiram detectar."

–GARTNER 2020 Network Detection and Response Market Guide

AICPA SOC
aicpa.org/soc4so

LUMU

FORGEPOINT | BIP CAPITAL | Opportunity Fund | Exceptional Capital

HUB SECURITY
Descubra as Ameaças Ocultas

Autorização de Distribuição

LUMU

DECLARAÇÃO

A Lumu do Brasil Ltda (Lumu Technologies), sediada na Rua Dom José de Barros, 177 – conj. 602 - Centro, na cidade de São Paulo, inscrita no CNPJ 45.865.366.0001/61, representada por seu Diretor de Canais Brasil, Jorge de Castro Alves, CPF: 443.947.991-04, declara a quem possa interessar, que a empresa HUB SECURITY LTDA, CNPJ 55.198.788/0001-84 localizada na Av. Paulista, 1636 - Sala 1504 - Cerqueira César São Paulo - SP - CEP 01310-200, é um parceiro oficial e registrado da Lumu Technologies, com um acordo firmado em 31/Maio/2024.

Desta forma, a HUB SECURITY está autorizada a comercializar, em todo o território nacional, a solução de Análise Contínua de Comprometimento; solução SaaS que envolve busca, detecção e resposta automática de ameaças, além do gerenciamento de incidentes através de um portal web.

São Paulo, 17 de junho de 2024.

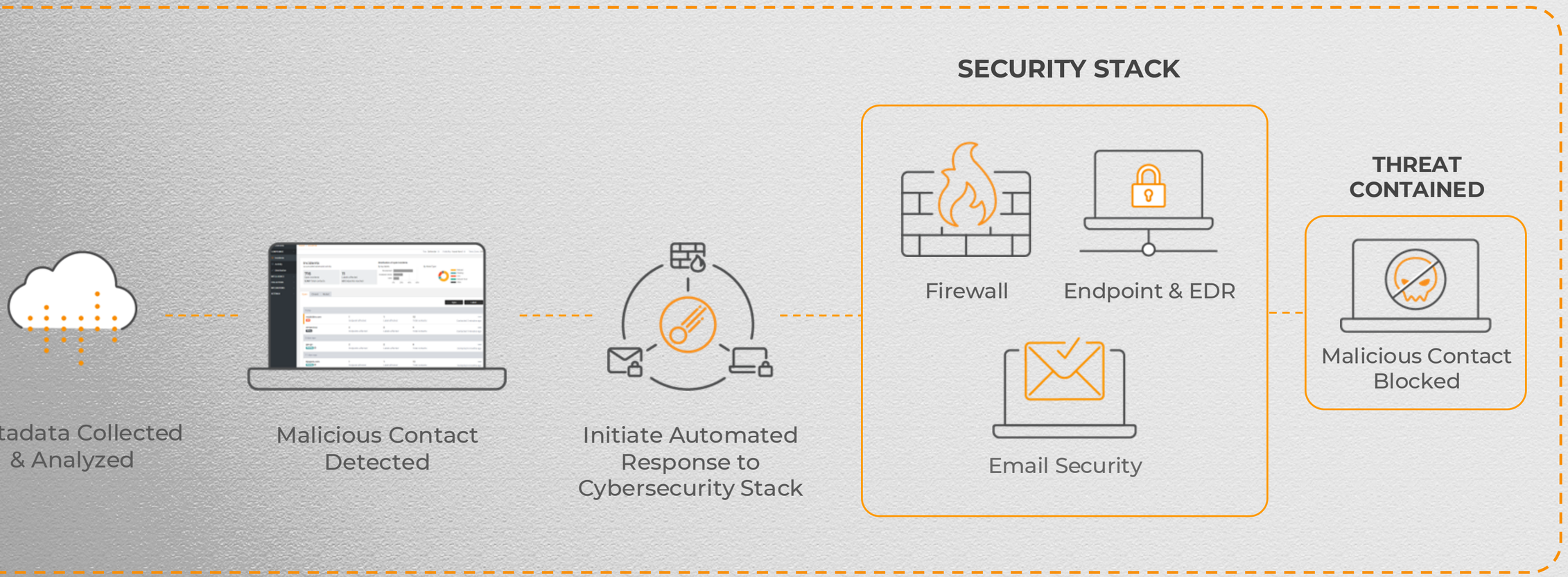
Jorge Alves

Jorge C. Alves
Diretor de Canais – Brasil
Lumu Technologies

HUB SECURITY
Descubra as Ameaças Ocultas

Lumu em Ação

HUB SECURITY
Descubra as Ameaças Ocultas

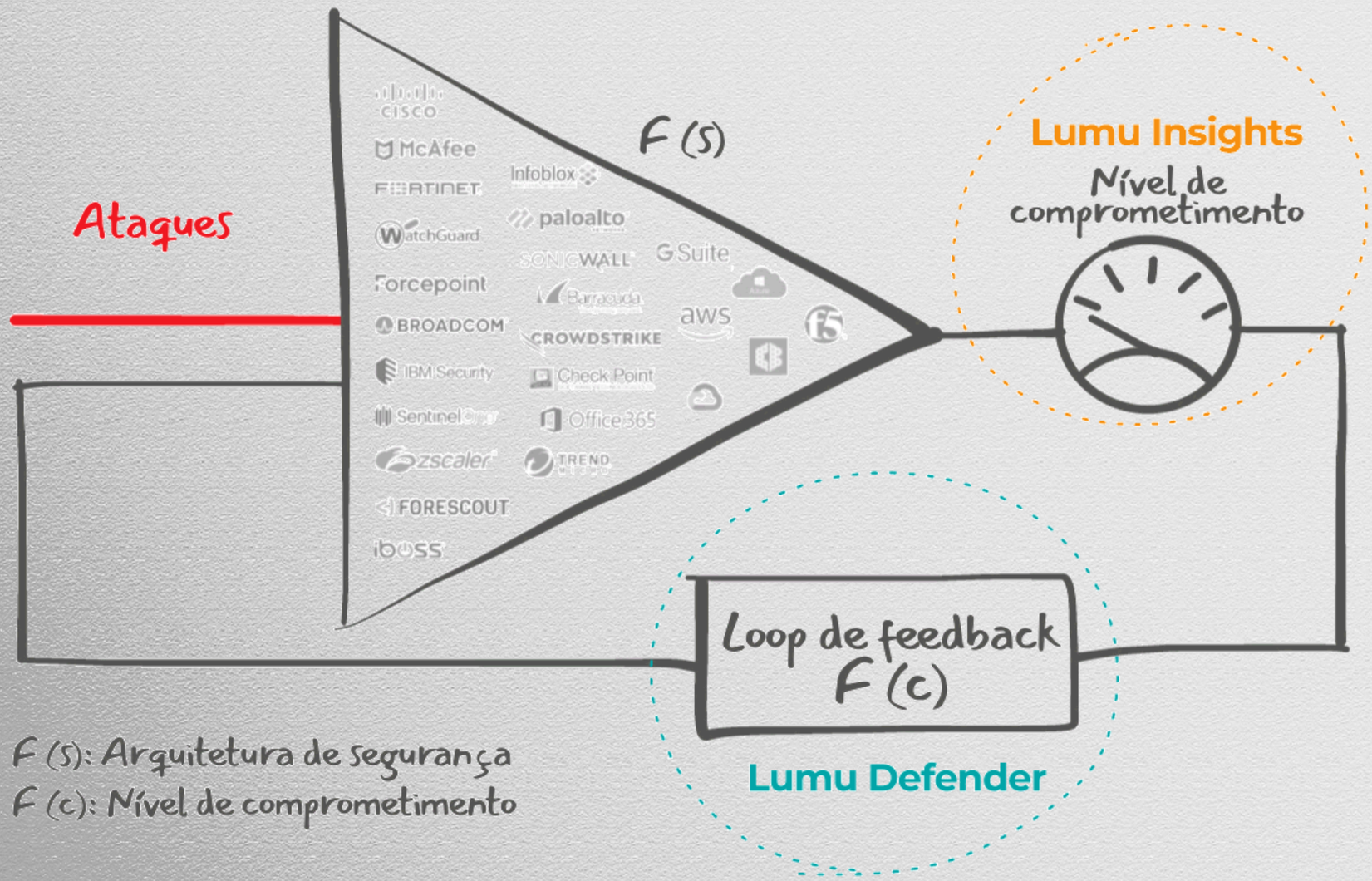


Toda a atividade é mostrada no Portal Lumu

LUMU

Melhorias contínuas permitem obter melhor ROI das suas estruturas de cibersegurança

HUB SECURITY
Descubra as Ameaças Ocultas



LUMU

A Lumu faz o Trabalho Duro para Você

HUB SECURITY
Descubra as Ameaças Ocultas

	1 Coleta de Metadados da Rede	2 Identificação de Atividade Maliciosa	3 Criação de incidente	4 Resposta a Ameaça
Sem a Lumu	Multiplas ferramentas necessárias	24x7 talento técnico	Triagem complexa	Manual e com propensão a erros
Com a Lumu	✓ Coleta automática de metadados	✓ Identificação contínua de atividade maliciosa	✓ Criação automática e com contexto	✓ Automática com uso das ferramentas existentes

LUMU

Alinhamento Total com o Framework do NIST

Faz referência a atividades anteriores para ajudar nos esforços de recuperação e resposta

Descubra ativos que estão em contato com adversários

Responda às ameaças em tempo real, fechando a janela de oportunidade do invasor

Bloqueie adversários em tempo real, descubra seus padrões e comportamentos para ajustar sua pilha de segurança

Automatize a busca de ameaças para obter visibilidade em tempo real das ameaças ativas

LUMU

HUB SECURITY
Descubra as Ameaças Ocultas


LUMU
Obrigado!
www.lumu.io
Abra a sua conta gratuita hoje
/lumutech
/lumutech
/lumutech
/lumutech
/lumutechnologies