



# CyberSec TECH DAY



# Email - Vetor #1 de Ameaças

Como combater com Cisco Secure Email e sua integração com Cisco XDR Threat Response

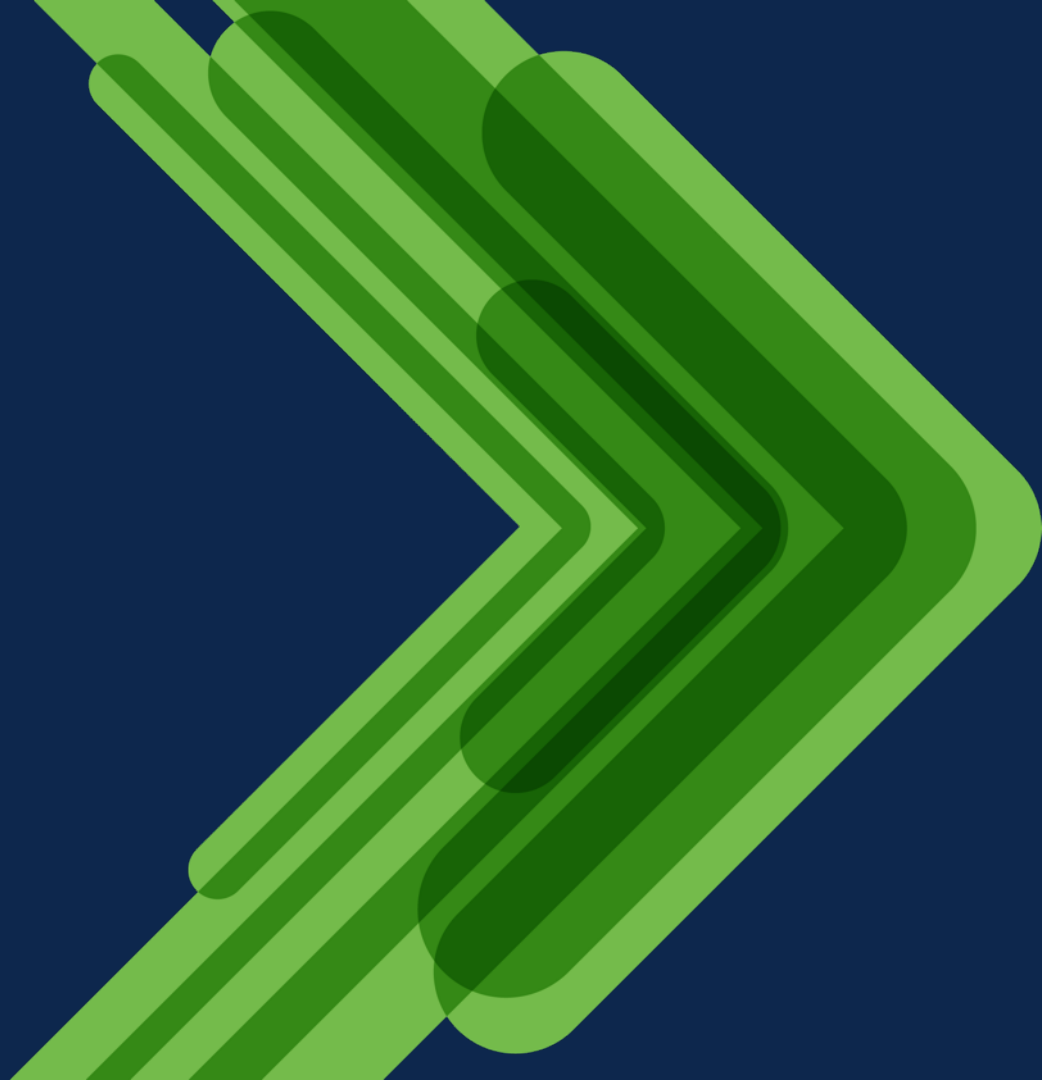
Heitor Silva - [heisilva@cisco.com](mailto:heisilva@cisco.com)  
Technical Solutions Architect

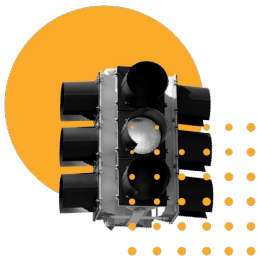


# Agenda

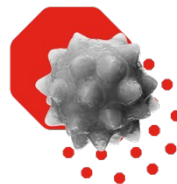
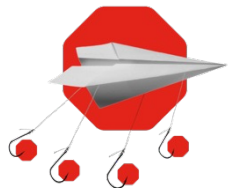
- Importância de Email Security para o mercado
- Relevância Cisco no mercado de Email Security
- Simplicidade Operacional
- Resposta Rápida e Integrada
- Cisco Secure Email & XDR Threat Response
- Q&A

Por que Email Security?

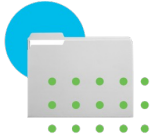




# Email vetor #1 de ameaças



# 10 Principais Tipos de Ameaças



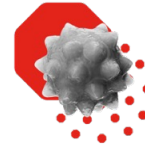
Business Email  
Compromise



Ransomware



Accounts  
Compromise



Malware



Phishing



Spam



Data breach



Advanced  
Persistent  
Threats



Insider threat



0-day Exploit

# Algumas estatísticas do field ...

91%

Ataques

tem início através de um email com um anexo, URL ou conjunto de instruções.

\$2.8

Bilhões

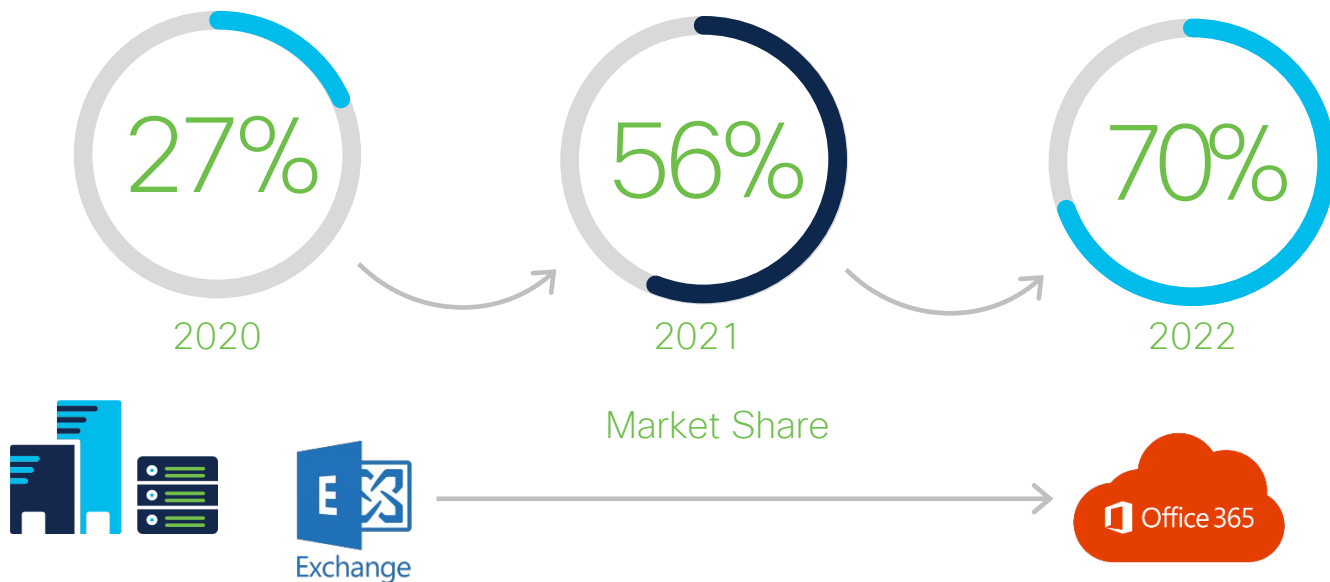
de perdas por phishing, bussiness email compromise, contas comprometidas e spoofing em 2022.

300K  
Reclamações

sobre ataques de phishing contabilizados somente em 2022

# A grande onda de migração para nuvem !!!

Adoção em massa de serviços de correio eletrônico em nuvem por empresas públicas e privadas



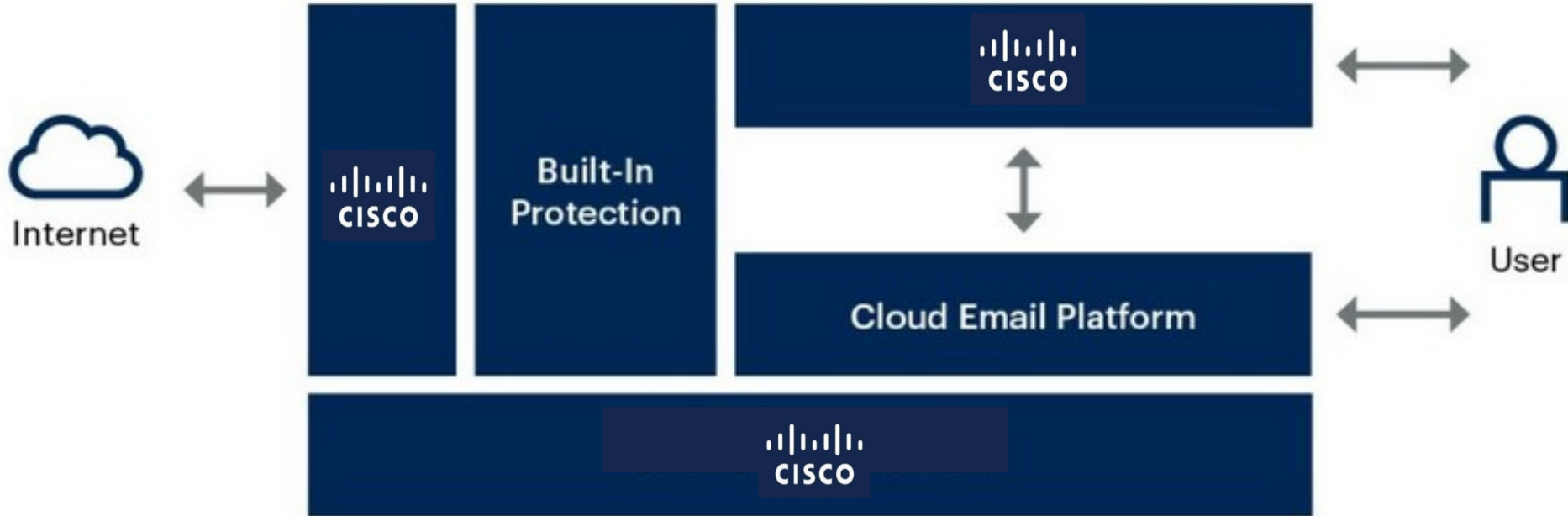




## A postura de utilizar camada única de proteção é inerentemente insegura!

Os invasores visam burlar as proteções de segurança do Microsoft 365, é muito importante que se tenha uma camada adicional de proteção. Gartner recomenda adoção de um “ICES – Integrated Cloud Email Security“, que vai além das proteções tradicionais da plataforma de correio em nuvem e complementa o SEG- Secure Email Gateway com visibilidade das mensagens internas e capacidades de remediação.

# Recomendação Email Security - Gartner





# Relevância Cisco no mercado de Email Security

# Cisco Secure Email – Entre os líderes nas últimas 6 avaliações do Radicati Group

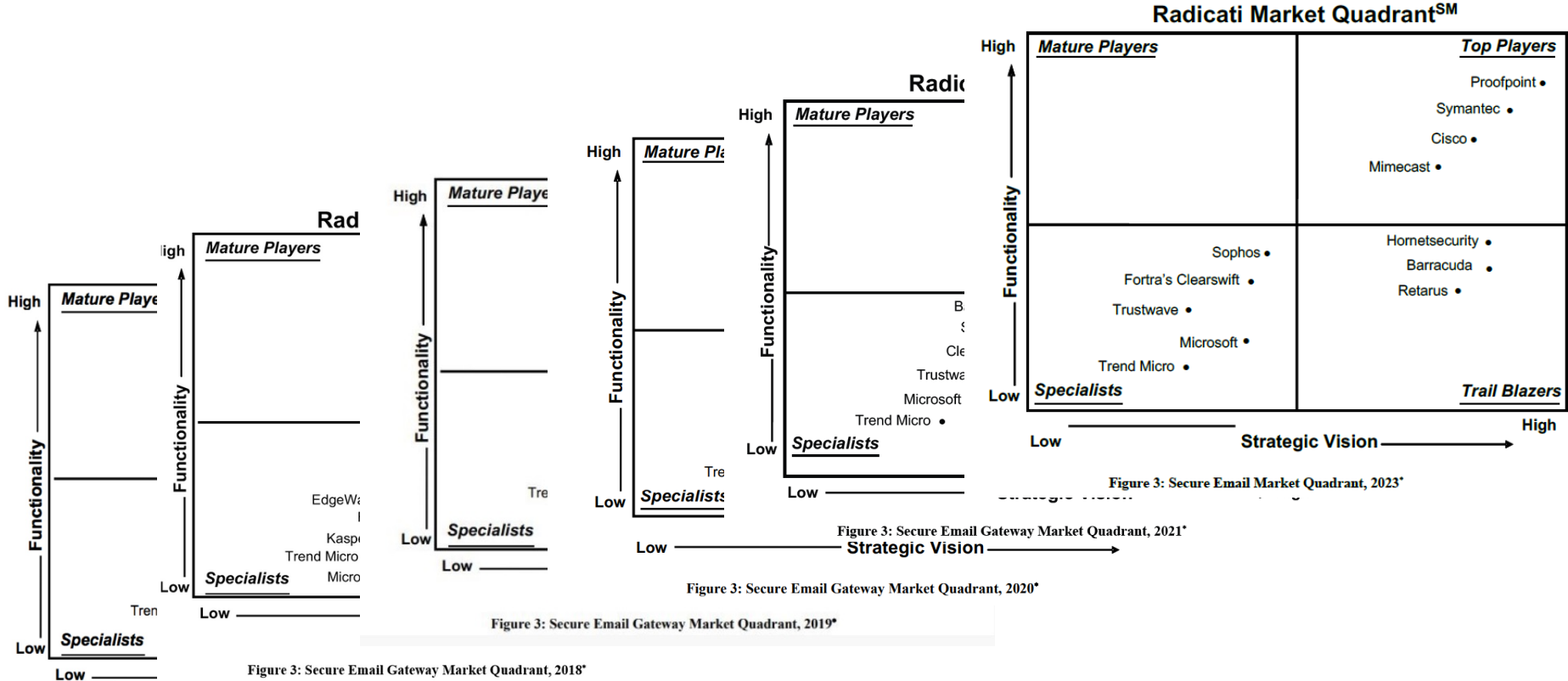


Figure 3: Secure Email Gateway Market Quadrant, 2017\*

Figure 3: Secure Email Gateway Market Quadrant, 2018\*

Figure 3: Secure Email Gateway Market Quadrant, 2019\*

Figure 3: Secure Email Gateway Market Quadrant, 2020\*

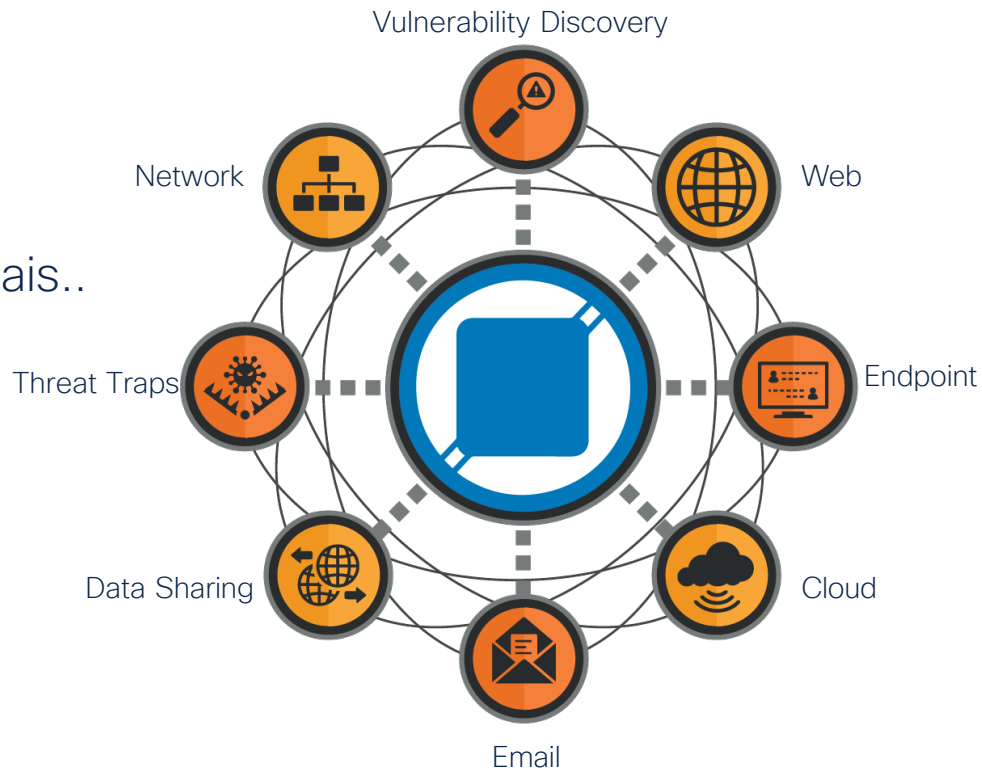
Figure 3: Secure Email Gateway Market Quadrant, 2021\*

Figure 3: Secure Email Market Quadrant, 2023\*

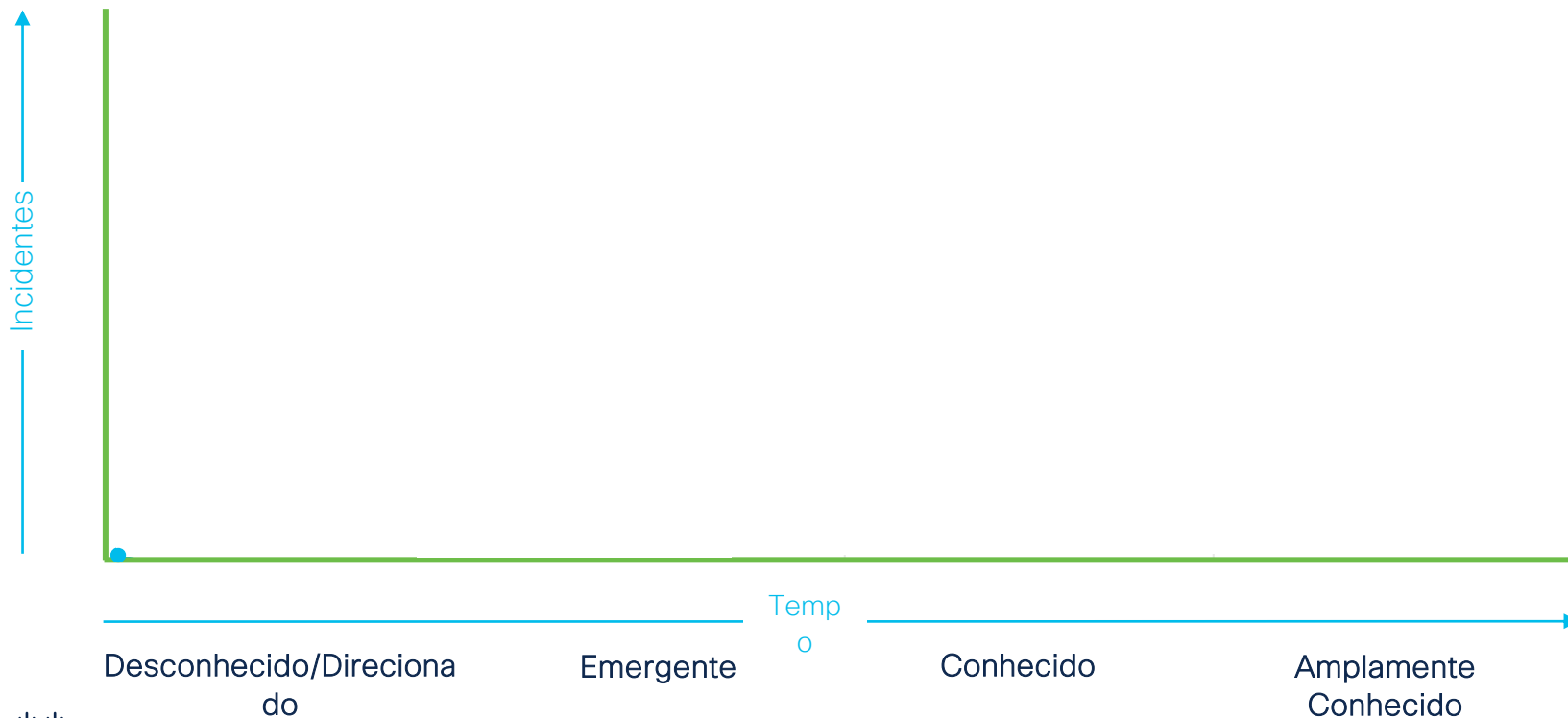
# Visibilidade inigualável

Para proteger mais, você necessita ver mais..

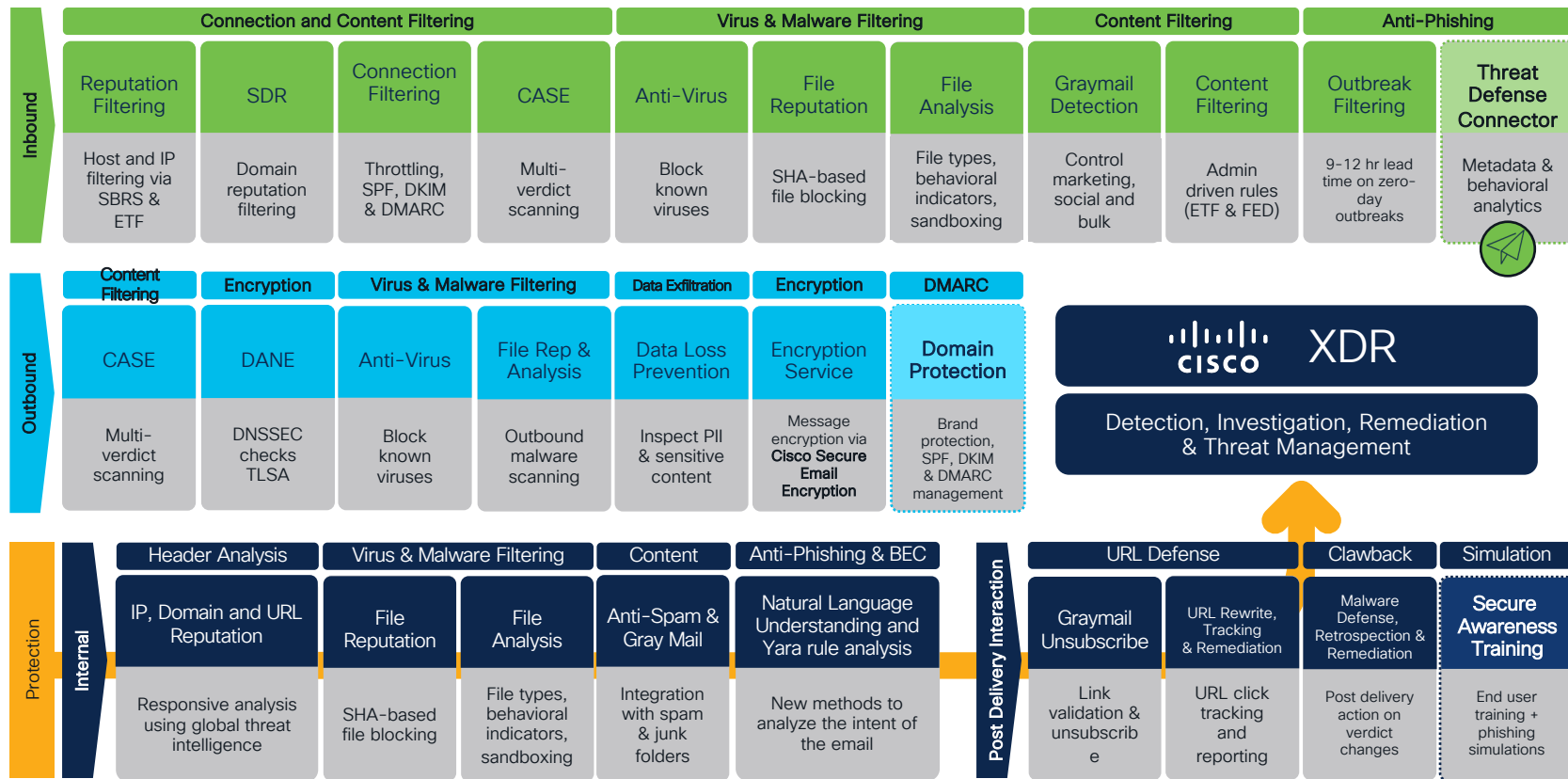
- O conjunto de dados mais diversificado
- Parcerias estratégicas
- Identificação pró-ativa de problemas



# Cobertura completa ao ciclo de vida de uma ameaça



# Cisco Secure Email - Proteção em camadas para o vetor #1



Simplicidade Operacional





# Cisco Secure Email agrega valor as organizações



Simplicidade  
de

Simplicidade Operacional



Visibilidade  
de

Visibilidade e Proteção Completa



Rapidez

Agilidade para identificar e remediar



Proteção de correio eletrônico integrada ao Cisco Talos

- Implantação Simplificada
  - ✓ Ativação
  - ✓ Configuração
  - ✓ Administração
- **Todas Mensagens**
  - ✓ Análise Avançada
  - ✓ Pesquisa Detalhada
  - ✓ Todos os Fluxos
- Rapidez na Identificação e Remediação
  - ✓ Identifica contas sob ataque
  - ✓ Remediação simples
  - ✓ XDR Threat Response



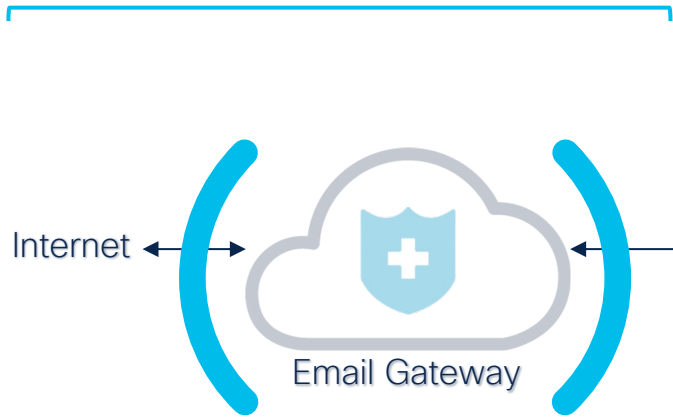
SECURE

© 2023 Cisco and/or its affiliates. All rights reserved.

# Visibilidade completa e proteção para todos os fluxos

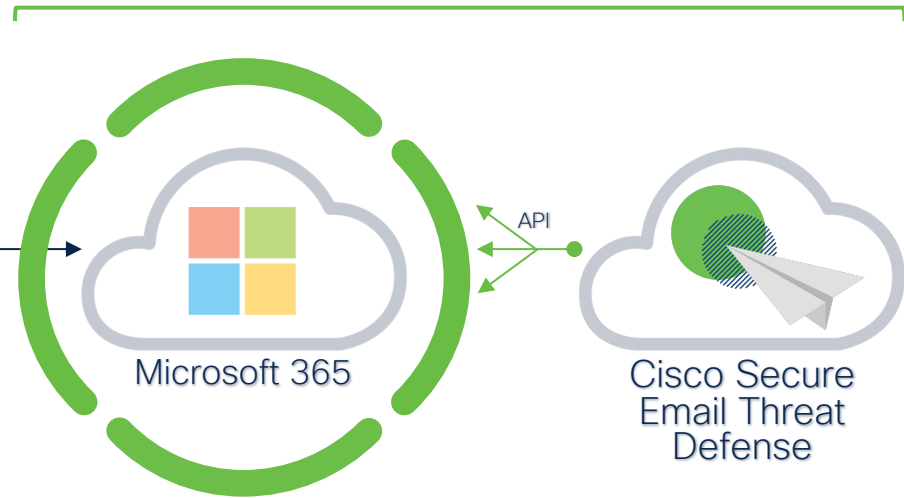
## Secure Email Gateway

Modifica e filtra mensagens de **entrada** e **saída** que atravessam o perímetro



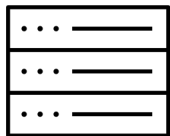
## Cisco Secure Email Threat Defense

Visibilidade completa para mensagens de **entrada, saída e internas**.



# Cisco Secure Email modelos de adoção

Flexível para se adequar ao seu ambiente



On-Premise

Appliances Virtuais



Hybrid

Appliances Virtuais

+


Cloud (SaaS)




Cloud

100% Cloud (SaaS)

# Ativação simples em 2 etapas para Microsoft 365



Autorizar API

 Microsoft

## Permissions requested Review for your organization

**This application is not published by Microsoft or your organization.**

This app would like to:


- ✓ Read mail in all mailboxes
- ✓ Read organization information
- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Etapa  
1



Criar  
Regra de  
Journal

## new journal rule

Apply this rule...

\*Send journal reports to:

Name:

\*If the message is sent to or received from...

\*Journal the following messages...

Etapa  
2

### Message Source

- Microsoft 365
  - Incoming
  - Internal
  - Outgoing
- Gateway
  - Incoming

#### Journal Address

Configure Microsoft 365 to send journals to Secure Email Threat Defense. For details, see the [Cisco Secure Email Threat Defense User Guide](#).

Journal Address:  
03a309df-7565-4a27-af11-a48a6ceabedd@mail.cmd.cisco.com

#### Secure Email Gateway (SEG)

No SEG is present

- Use Cisco SEG default header X-IronPort-RemotelP
- Use Custom SEG header

#### Messages Analysis

Direction of Messages  Incoming

Select direction(s) of messages to be dynamically analyzed. Analyzing an internal message will also include any external recipients that are included.  Outgoing

Internal

Direction of Attachments  Incoming

Select direction(s) of attachments to be dynamically analyzed. Attachments will be sent to Cisco Secure Malware Analytics for analysis.  Outgoing

Internal

Spam and Graymail  On

Analyze or remediate Spam and Graymail.

### Visibility & Remediation

#### Microsoft 365 Authentication

- Read/Write
  - Visibility
  - On-demand remediation
  - Automated remediation (optional)
  - EML Download
- Read
  - Visibility
  - No remediation
  - EML Download

Imported Domains (1 auto-remediated, 2 total) Update List

Domains are imported to help determine message directions. Domains can be excluded from Automated Remediation Policy.

Apply Auto-Remediation to all domains

- cybersectechday.com.br
- cybersectechday.onmicrosoft.com

Apply auto-remediation to domains not in the domain list above.

Automated Remediation Policy  On

These actions apply to all selected domains.

Threat Category	Description	Action
<b>Threats</b>	Threats include messages flagged as Business Email Compromise (BEC), Scam, Malicious, or Phishing.	<span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">Move to Quarantine</span>
<b>Spam</b>	Spam includes messages with unwanted content, including undesirable URLs.	<span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">No Action</span>
<b>Graymail</b>	Graymail is mail that has been determined to be marketing, social, or junk.	<span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">No Action</span>

Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts.

Resposta Rápida e  
Integrada



# Categorização, identificação de Riscos e Técnicas

Graymail	Marketing	Social	Bulk	Spam
Spam	Junk	Win Big	Bot / DGA	Education
	Adult	Pharma	Reputation	Job / Offer
Scam	Fraud	Advance Fee	Fake Company	ATO
	Extortion	Charity	Romance	Investment
	Lottery	Employment	Inheritance	Money Mule
Phishing	Credential	Financial	Doc Share	Forgery
	Identity	Brand	Spoof/Cousin	ATO (external)
Business Email Compromise	Compromise	Payroll	Gift Card	wire Transfer
	M & A	Invoice		
Malware	Ransomware	Cred Stealer	Crypto Miner	Ad/Spyware
	Malicious URL	Bot/Phish Kit	Viral	Trojan / CNC

Phishing
Quarantine
Aug 29 2022 6:54 AM EST

---

**Message ID:** <DBAP192MB0922B7E041EE132AB799B689CFF39@ingencorporation.com>

**Verdict Details**

Category  
Phishing

Business Risk  
Credential

Technique  
**REQUEST FOR CREDENTIALS**

Message segment 'Please login to avoid account deletion' contains a request for credentials

**SUBJECT TOPIC: ACCOUNTS**

Subject text is often associated with business email compromise (BEC).

**MALICIOUS FILE**

note.html (SHA256: 1daa049e1da5292f...)

**UNICODE MASQUERADE**

Email contains 3 words with confusable unicode usage. Words: alert, message, password

**Sender**

From  
dnedry@ingencorporation.com

Name  
Don Nedry

Reply To

Return Path

SMTP Server IP  
::1

SMTP Client IP  
76.97.162.228

X-Originating IP  
76.97.162.228

# Redução de risco: **Remediação**

Detectamos uma URL suspeita o que fazer?

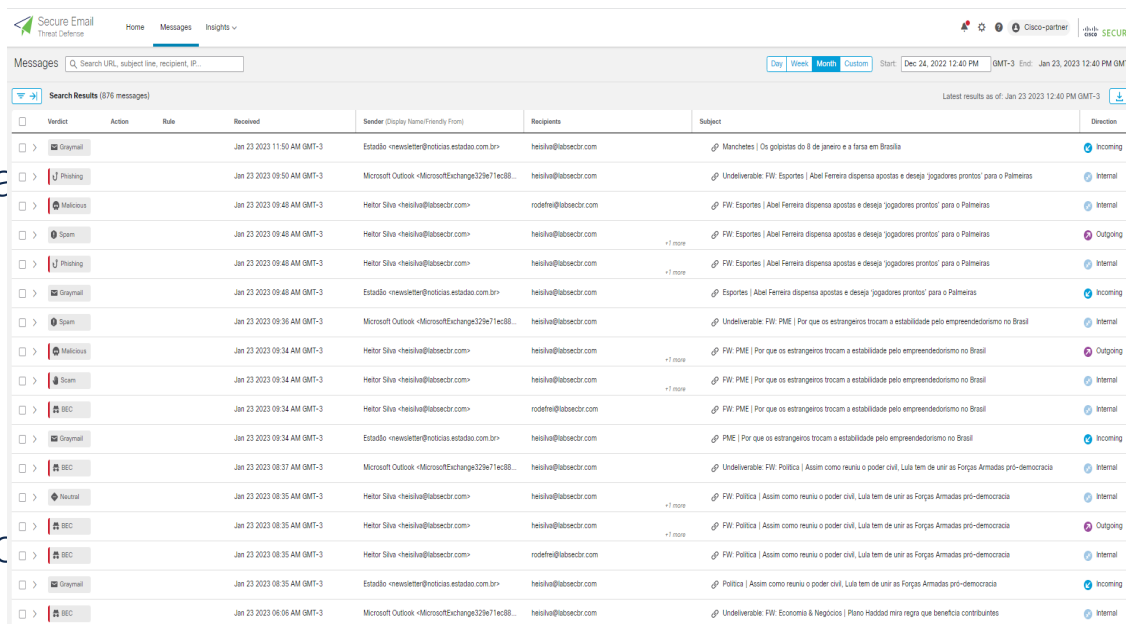
- Quem mais recebeu esta mesma URL?
- Quais ferramentas estão disponíveis se eu utilizo Microsoft 365?
- O que fazer se a mensagem foi movida?
- O que fazer se esta mensagem foi encaminhada?





# Economize tempo: pesquisa, classificação e remediação

- Pesquise instantaneamente por observáveis relevantes
- Sintaxe de pesquisa simples
- Sem usar ferramentas complexas
  - Message Trace
  - Power Shell
  - Compliance Search
- Sem envolver especialistas
- Visibilidade dos usuários afetados



The screenshot displays the 'Secure Email Threat Defense' interface. At the top, there are navigation tabs for 'Home', 'Messages', and 'Insights'. Below this is a search bar with the text 'Search Results (376 messages)'. The main area is a table of messages with the following columns: Verdict, Action, Date, Received, Sender (Display Name/Friendly From), Recipients, Subject, and Direction. The messages are sorted by date, showing a list of emails received and sent on January 23, 2023. The subjects of the messages include topics like 'Manchetes | Os golpistas do 8 de janeiro e a farsa em Brasília', 'Undeliverable: FW: Esportes | Abel Ferreira dispensa apostas e deseja 'jogadores prontos' para o Palmeiras', and 'FW: Esportes | Abel Ferreira dispensa apostas e deseja 'jogadores prontos' para o Palmeiras'.

Verdict	Action	Date	Received	Sender (Display Name/Friendly From)	Recipients	Subject	Direction
	Graymail	Jan 23 2023 11:50 AM GMT-3		Estado <newsletter@noticias.estado.com.br>	heisiva@abecbr.com	Manchetes   Os golpistas do 8 de janeiro e a farsa em Brasília	Incoming
	Phishing	Jan 23 2023 09:50 AM GMT-3		Microsoft Outlook <MicrosoftExchange329e71ec88...>	heisiva@abecbr.com	Undeliverable: FW: Esportes   Abel Ferreira dispensa apostas e deseja 'jogadores prontos' para o Palmeiras	Internal
	Malicious	Jan 23 2023 09:48 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	rodefre@abecbr.com	FW: Esportes   Abel Ferreira dispensa apostas e deseja 'jogadores prontos' para o Palmeiras	Internal
	Spam	Jan 23 2023 09:48 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	heisiva@abecbr.com	FW: Esportes   Abel Ferreira dispensa apostas e deseja 'jogadores prontos' para o Palmeiras	Outgoing
	Phishing	Jan 23 2023 09:48 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	heisiva@abecbr.com	FW: Esportes   Abel Ferreira dispensa apostas e deseja 'jogadores prontos' para o Palmeiras	Internal
	Graymail	Jan 23 2023 09:48 AM GMT-3		Estado <newsletter@noticias.estado.com.br>	heisiva@abecbr.com	Esportes   Abel Ferreira dispensa apostas e deseja 'jogadores prontos' para o Palmeiras	Incoming
	Spam	Jan 23 2023 09:36 AM GMT-3		Microsoft Outlook <MicrosoftExchange329e71ec88...>	heisiva@abecbr.com	Undeliverable: FW: PME   Por que os estrangeiros tocam a estabilidade pelo empreendedorismo no Brasil	Internal
	Malicious	Jan 23 2023 09:34 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	heisiva@abecbr.com	FW: PME   Por que os estrangeiros tocam a estabilidade pelo empreendedorismo no Brasil	Outgoing
	Spam	Jan 23 2023 09:34 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	heisiva@abecbr.com	FW: PME   Por que os estrangeiros tocam a estabilidade pelo empreendedorismo no Brasil	Internal
	BEC	Jan 23 2023 09:34 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	rodefre@abecbr.com	FW: PME   Por que os estrangeiros tocam a estabilidade pelo empreendedorismo no Brasil	Internal
	Graymail	Jan 23 2023 09:34 AM GMT-3		Estado <newsletter@noticias.estado.com.br>	heisiva@abecbr.com	PME   Por que os estrangeiros tocam a estabilidade pelo empreendedorismo no Brasil	Incoming
	BEC	Jan 23 2023 08:37 AM GMT-3		Microsoft Outlook <MicrosoftExchange329e71ec88...>	heisiva@abecbr.com	Undeliverable: FW: Política   Assim como reuniu o poder civil, Lula tem de unir as Forças Armadas pré-democracia	Internal
	Neutral	Jan 23 2023 08:35 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	heisiva@abecbr.com	FW: Política   Assim como reuniu o poder civil, Lula tem de unir as Forças Armadas pré-democracia	Internal
	BEC	Jan 23 2023 08:35 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	heisiva@abecbr.com	FW: Política   Assim como reuniu o poder civil, Lula tem de unir as Forças Armadas pré-democracia	Outgoing
	BEC	Jan 23 2023 08:35 AM GMT-3		Heitor Silva <heisiva@abecbr.com>	rodefre@abecbr.com	FW: Política   Assim como reuniu o poder civil, Lula tem de unir as Forças Armadas pré-democracia	Internal
	Graymail	Jan 23 2023 08:35 AM GMT-3		Estado <newsletter@noticias.estado.com.br>	heisiva@abecbr.com	Política   Assim como reuniu o poder civil, Lula tem de unir as Forças Armadas pré-democracia	Incoming
	BEC	Jan 23 2023 06:06 AM GMT-3		Microsoft Outlook <MicrosoftExchange329e71ec88...>	heisiva@abecbr.com	Undeliverable: FW: Economia & Negócios   Plano Haddad mira negra que beneficia contribuintes	Internal

# Pesquisa e remediação rápidas, quando os minutos são valiosos



← Cisco Secure Email Threat Defense < 5 min

Office 365: Message Trace, Compliance Search, PowerShell ~1 hora

<b>12x</b> Redução de tempo	para pesquisa e correção de mensagens em caixas de correio
--------------------------------	--

Messages

Day Week Month Custom Start: Oct 02, 2023 2:47 PM GMT-3 End: Oct 9, 2023 2:47 PM GMT-3

THREATS  
46  
BEC 2  
Scam 11  
Phishing 2  
Malicious 31  
Quarantine 21



MESSAGES  
729  
Outgoing 73  
Mixed 0  
Internal 61  
Incoming 595

Search Results (729 messages)

Latest results as of: Oct 09 2023 02:47 PM GMT-3

Verdict	Action	Rule	Received	Sender (Display Name/Friendly From)	Recipients	Subject	Direction
<input type="checkbox"/>	Graymail		Oct 09 2023 11:54 AM GMT-3	The New York Times <nytdirect@nytimes.com>	nrocha@cybersectechday.com.br	Upshot: Being paid in beer? Try our history quiz	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 11:16 AM GMT-3	The New York Times <nytdirect@nytimes.com>	heilto.silva@cybersectechday.com.br	Extreme Weather: Finish selecting your places	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 11:14 AM GMT-3	The New York Times <nytdirect@nytimes.com>	rcorrea@cybersectechday.com.br	Extreme Weather: Finish selecting your places	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 11:11 AM GMT-3	The New York Times <nytdirect@nytimes.com>	nrocha@cybersectechday.com.br	Extreme Weather: Finish selecting your places	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:53 AM GMT-3	Splash UOL   SplashTV <splashtv@newsletteruol.co...>	rmiranda@cybersectechday.com.br	Leão Lobo: Márcia (se) Fu... em A Fazenda 15	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:53 AM GMT-3	Splash UOL   SplashTV <splashtv@newsletteruol.co...>	hsilva@cybersectechday.com.br	Leão Lobo: Márcia (se) Fu... em A Fazenda 15	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:53 AM GMT-3	PagBank & UOL   Por dentro da Bolsa <uoleconomi...>	mlucia@cybersectechday.com.br	Guerra, feriados e indicadores afetam mercado	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:53 AM GMT-3	PagBank & UOL   Por dentro da Bolsa <uoleconomi...>	hsilva@cybersectechday.com.br	Guerra, feriados e indicadores afetam mercado	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:32 AM GMT-3	PagBank & UOL   Por dentro da Bolsa <uoleconomi...>	rcorrea@cybersectechday.com.br	Guerra, feriados e indicadores afetam mercado	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:32 AM GMT-3	PagBank & UOL   Por dentro da Bolsa <uoleconomi...>	heilto.silva@cybersectechday.com.br	Guerra, feriados e indicadores afetam mercado	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:14 AM GMT-3	VivaBem UOL <vivabem@newsletteruol.com.br>	rmiranda@cybersectechday.com.br	Fruta engorda? Veja como consumi-las do jeito certo!	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:14 AM GMT-3	VivaBem UOL <vivabem@newsletteruol.com.br>	mlucia@cybersectechday.com.br	Fruta engorda? Veja como consumi-las do jeito certo!	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 10:14 AM GMT-3	VivaBem UOL <vivabem@newsletteruol.com.br>	hsilva@cybersectechday.com.br	Fruta engorda? Veja como consumi-las do jeito certo!	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 09:56 AM GMT-3	VivaBem UOL <vivabem@newsletteruol.com.br>	heilto.silva@cybersectechday.com.br	Fruta engorda? Veja como consumi-las do jeito certo!	Incoming
<input type="checkbox"/>	Graymail		Oct 09 2023 09:32 AM GMT-3	Stu Sjouwerman <ssjouwerman@knowbe4.com>	rcorrea@cybersectechday.com.br	Open-Source Intelligence (OSINT): Learn the Methods Bad Actors Use to Hack Your Organization	Incoming

100 / per page

1 of 8

# Cisco Secure Email & XDR Threat Response



# Cisco XDR Threat Response & Secure Email



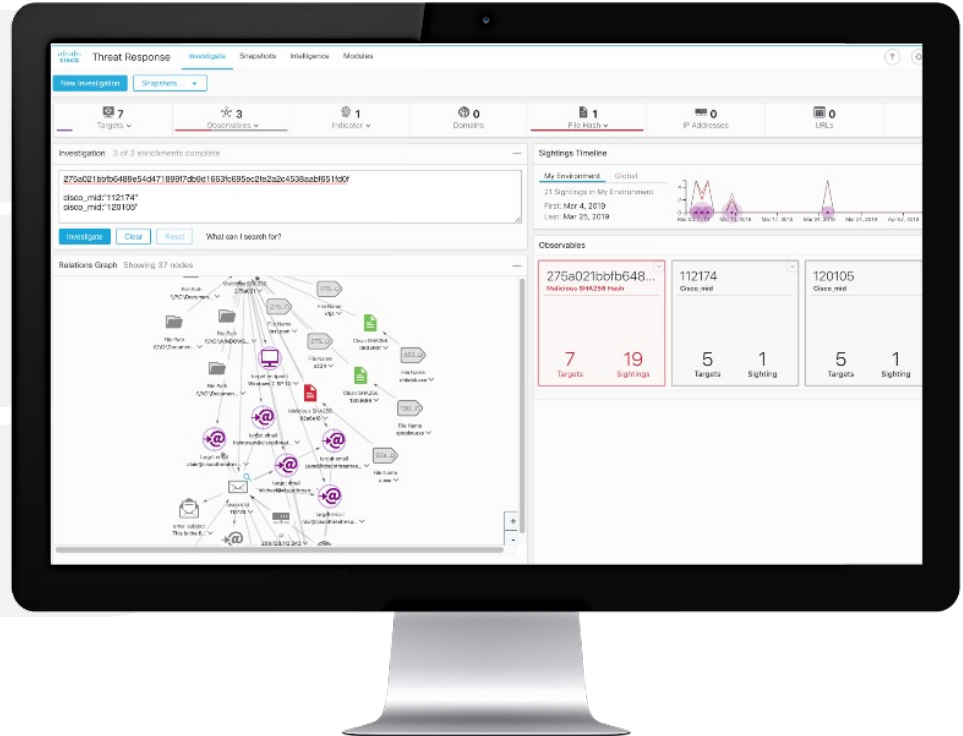
Entenda o e-mail como um vetor de ameaça, visualizando os relacionamentos de mensagem, remetente e alvo no contexto de uma ameaça



Pesquise vários endereços de e-mail, assuntos e anexos de uma só vez para entender como uma ameaça se espalhou entre os elementos da rede

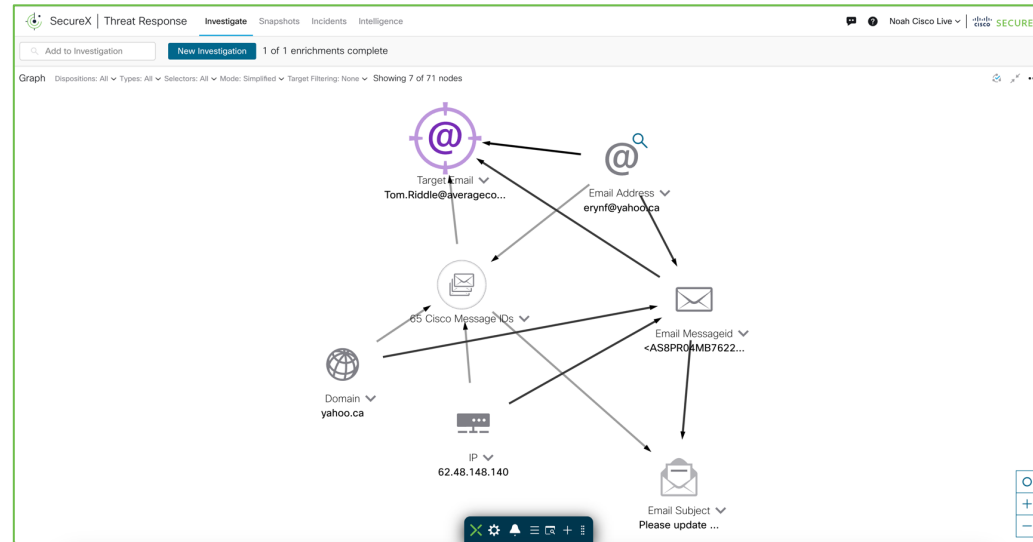


Expanda a visibilidade das suas operações de Cyber Security para e-mails e outros artefatos associados as ameaças



# Integração Cisco Secure Email & XDR

- Agora você pode colocar em quarentena, mover ou apagar mensagens com um observável específico diretamente dos menus dinâmicos XDR em produtos integrados.
- Os observáveis dos quais você utilizar são:
  - Endereço de email
  - ID de mensagem
  - Assunto
  - Nome de arquivo
  - IP do remetente
  - SHA 256
  - URL





CyberSec  
TECH DAY

Obrigado!

