CyberSec
TECH DAY

cisco

Mais que tecnologia

LOGICALIS
Architects of Change

NTT

teletex

Email – Vetor #1 de Ameaças

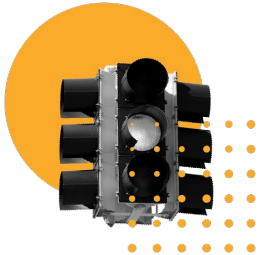
Como combater com Cisco Secure Email e sua integração com Cisco XDR Threat Response

Heitor Silva – heisilva@cisco.com
Technical Solutions Architect

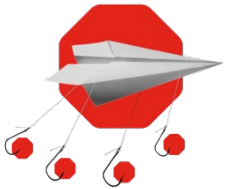
Agenda

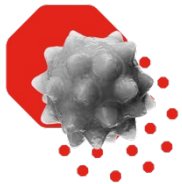
- Importância de Email Security para o mercado
- Relevância Cisco no mercado de Email Security
- Simplicidade Operacional
- Resposta Rápida e Integrada
- Cisco Secure Email & XDR Threat Response
- Q&A

Por que Email Security?

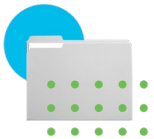


Email vetor #1 de ameaças





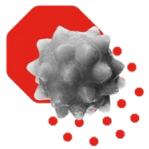
10 Principais Tipos de Ameaças



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.

* industry phishing report

$2.8

Bilhões

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

* FBI 2022 IC3 Report

300K

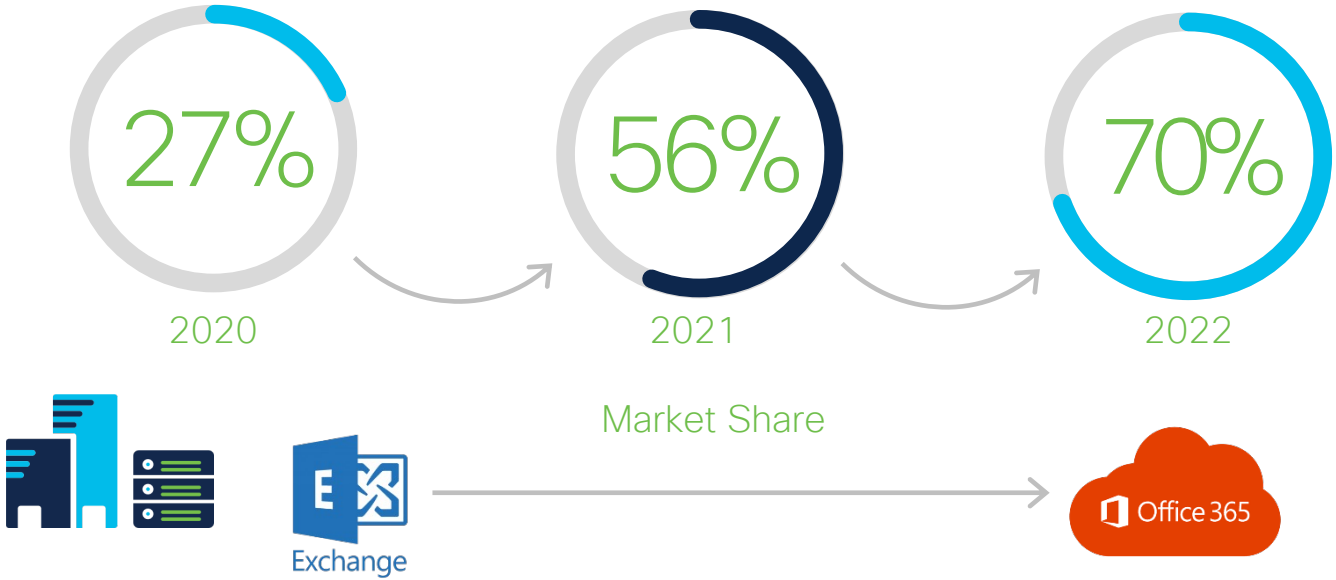
Reclamações

sobre ataques de phishing contabilizados somente em 2022

* FBI 2022 IC3 Report

A grande onda de migração para nuvem !!!

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

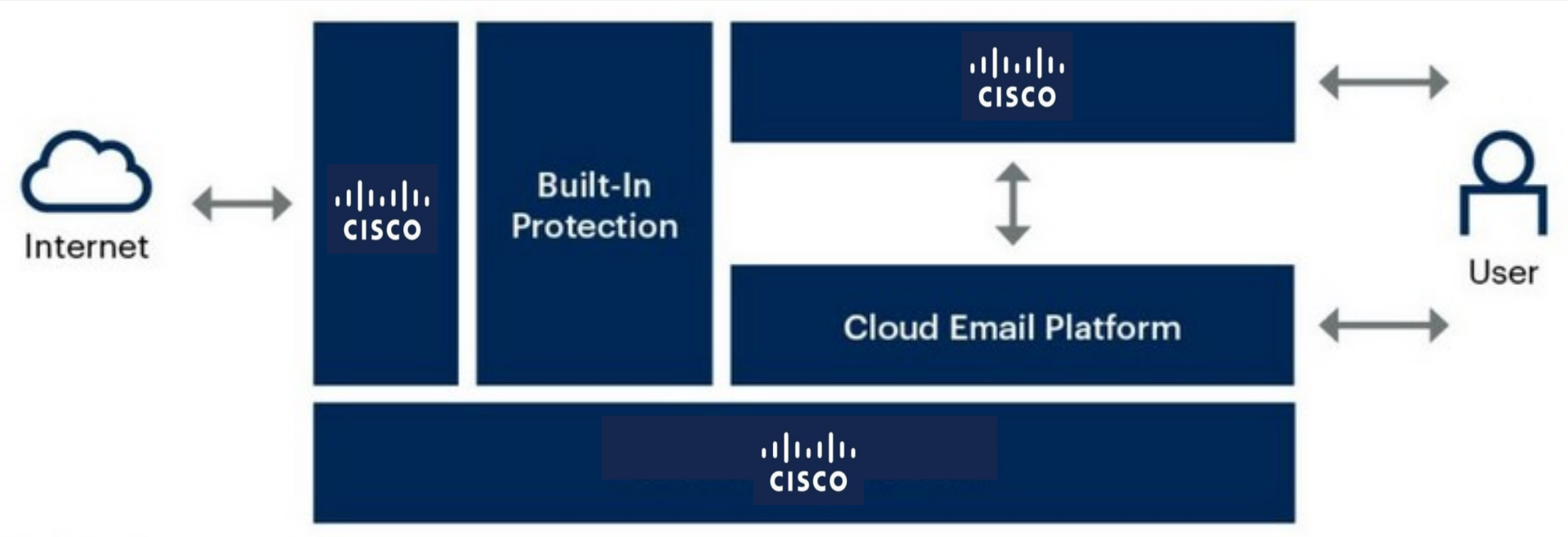


[1] Gartner, Survey Analysis: Google and Microsoft Battle It Out in a Growing Cloud Email Market
[2] Gartner, Market Guide for Email Security

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

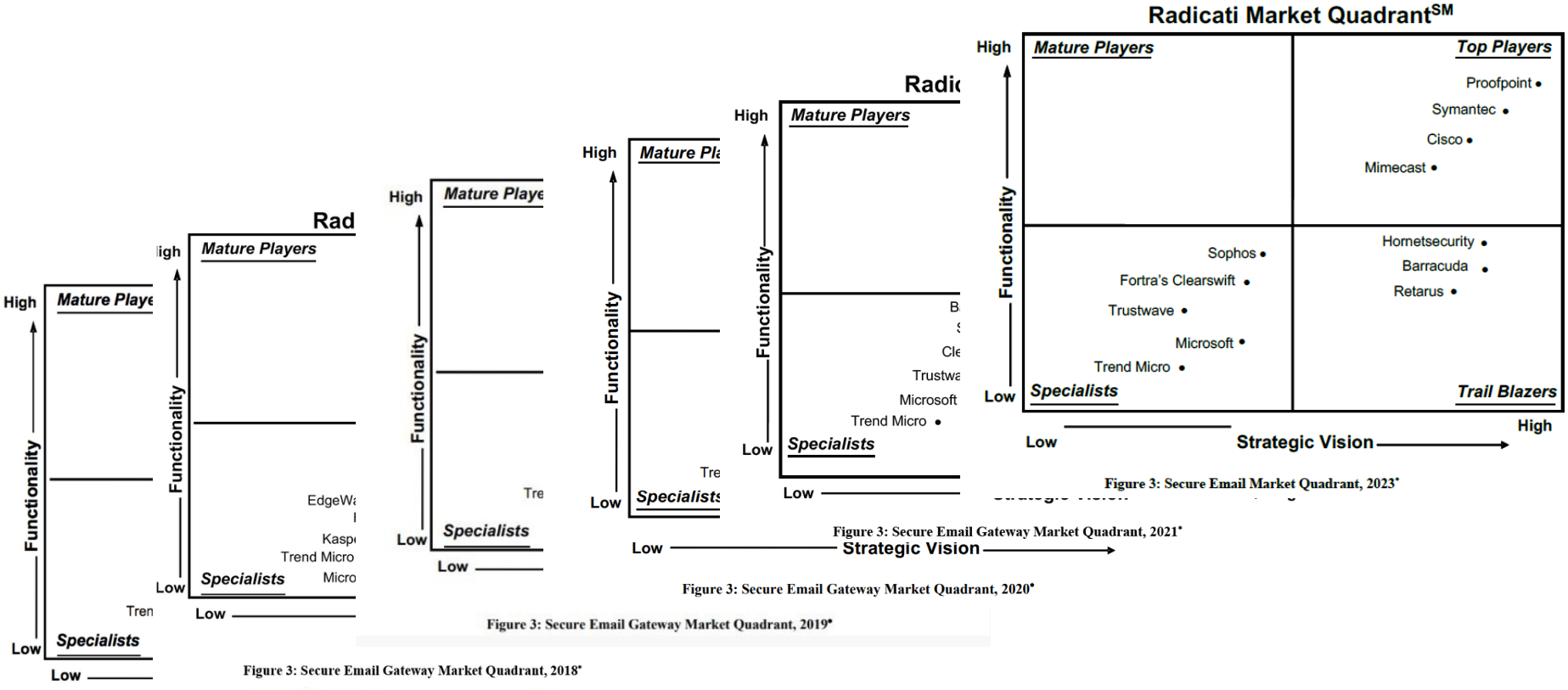
Os invasores visam burlar as proteções de segurança do Microsoft 365, é muito importante que se tenha uma camada adicional de proteção. Gartner recomenda adoção de um “ICES – Integrated Cloud Email Security“, que vai além das proteções tradicionais da plataforma de correio em nuvem e complementa o SEG-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

Recomendação Email Security – Gartner



Relevância Cisco no mercado de Email Security

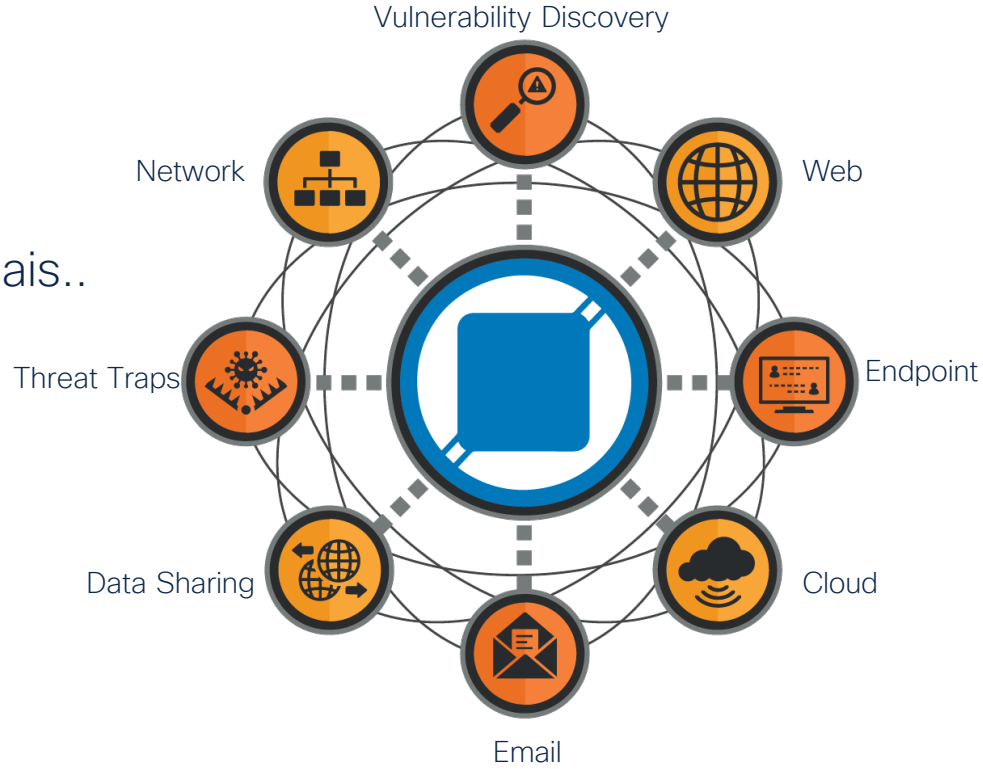
Cisco Secure Email – Entre os líderes nas últimas 6 avaliações do Radicati Group



Visibilidade inigualável

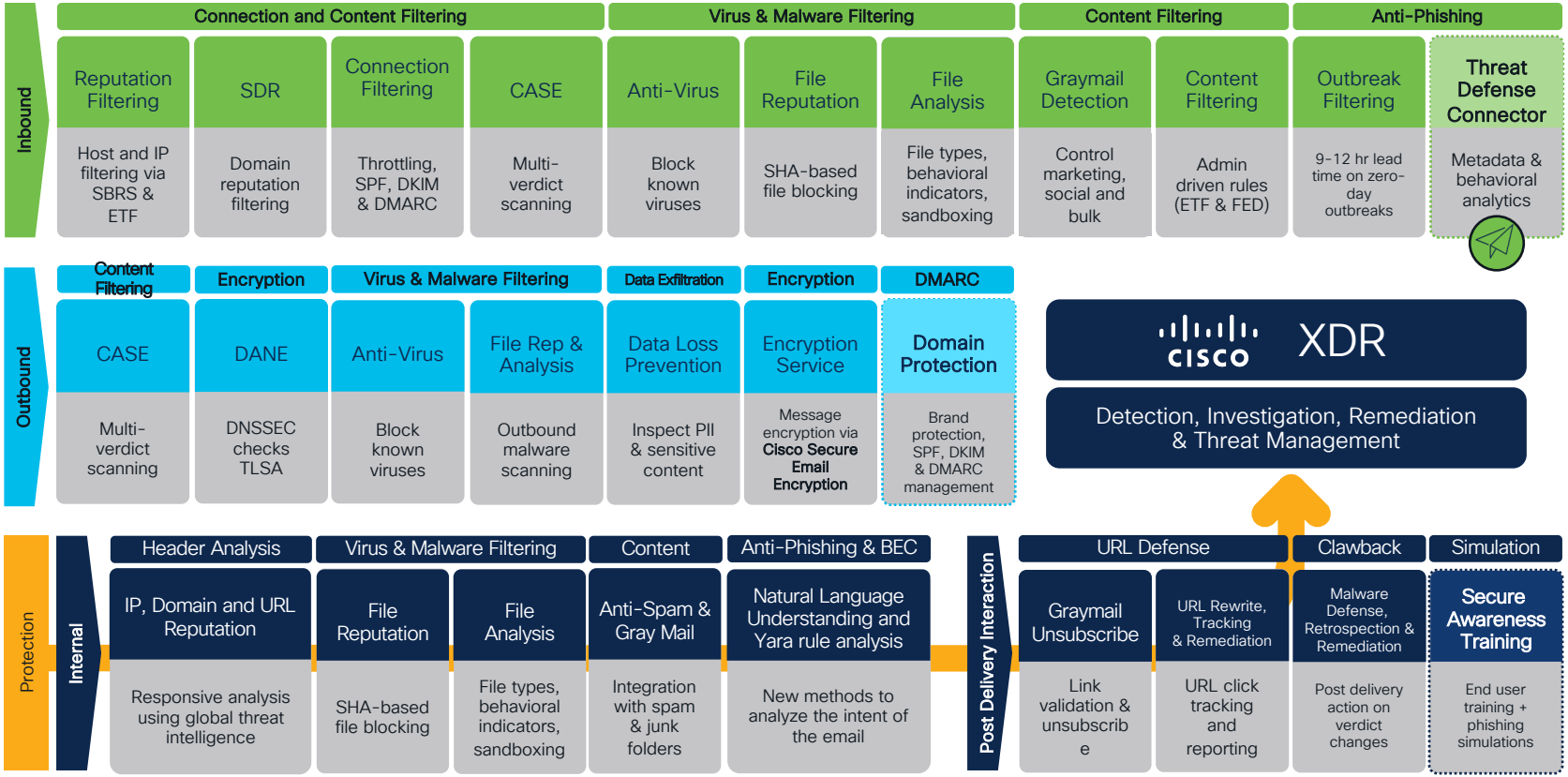
Para proteger mais, você necessita ver mais..

- 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

Visibilidade de

Rapidez

Simplicidade Operacional

Visibilidade e Proteção Completa

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

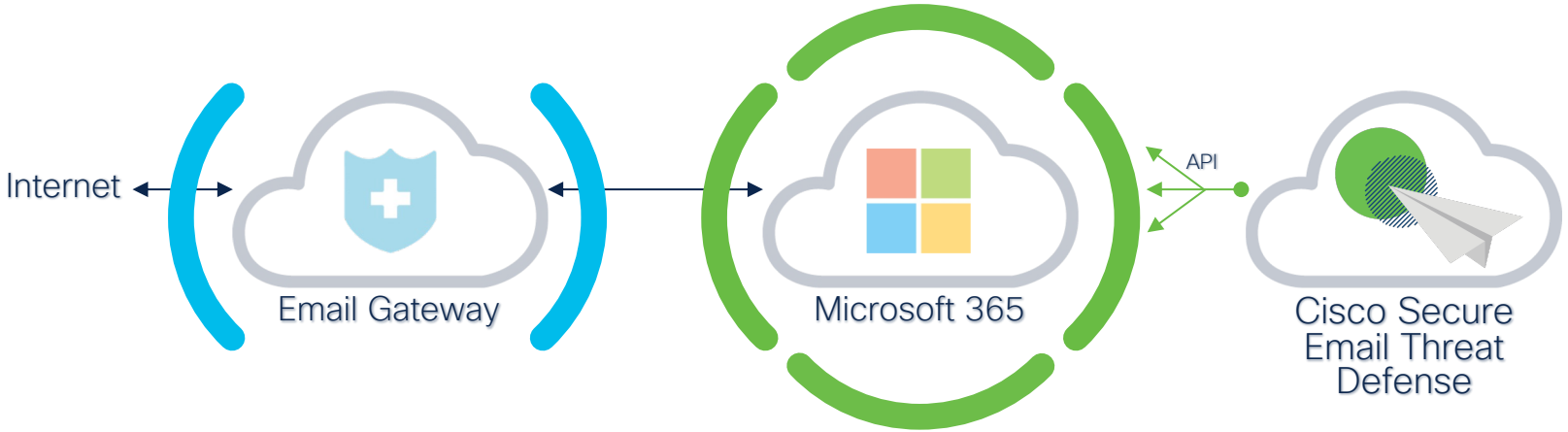
Visibilidade completa e proteção para todos os fluxos

Secure Email Gateway

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

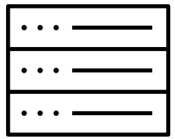
Cisco Secure Email Threat Defense

Visibilidade completa para mensagens de entrada, saída e internas.



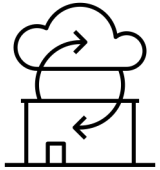
Cisco Secure Email modelos de adoção

Flexível para se adequar ao seu ambiente



On-Premise

Appliances Virtuais



Hybrid

Appliances Virtuais
+
Cloud (SaaS)

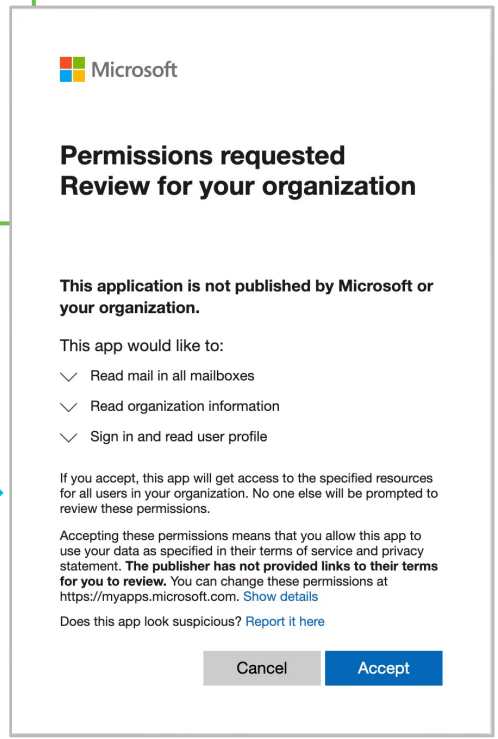
Cloud

100% Cloud (SaaS)

Ativação simples em 2 etapas para Microsoft 365

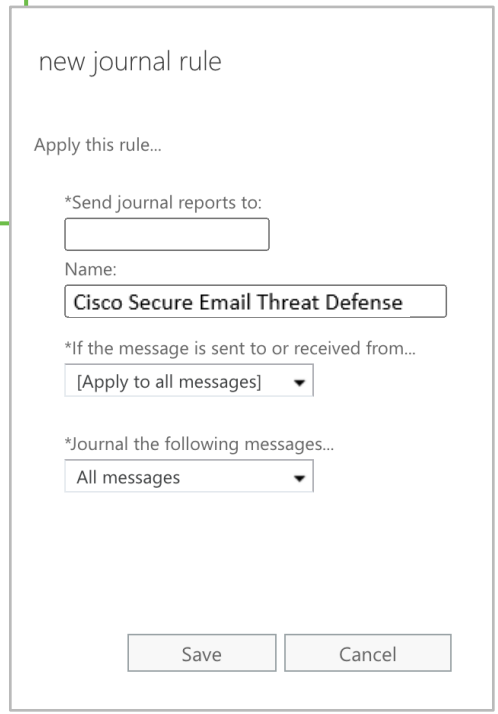
Autorizar API

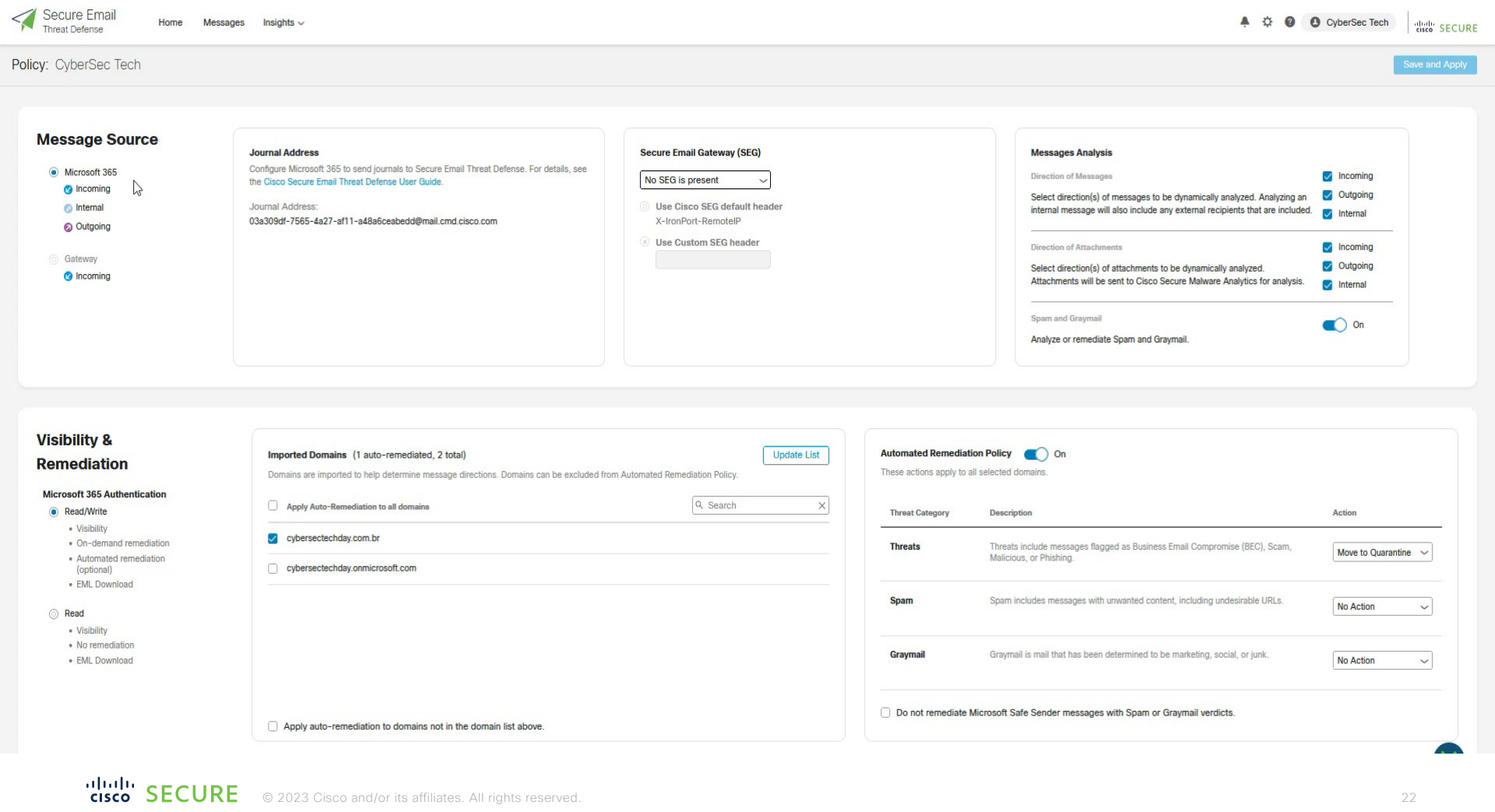
Etapa 1



Criar Regra de Journal

Etapa 2

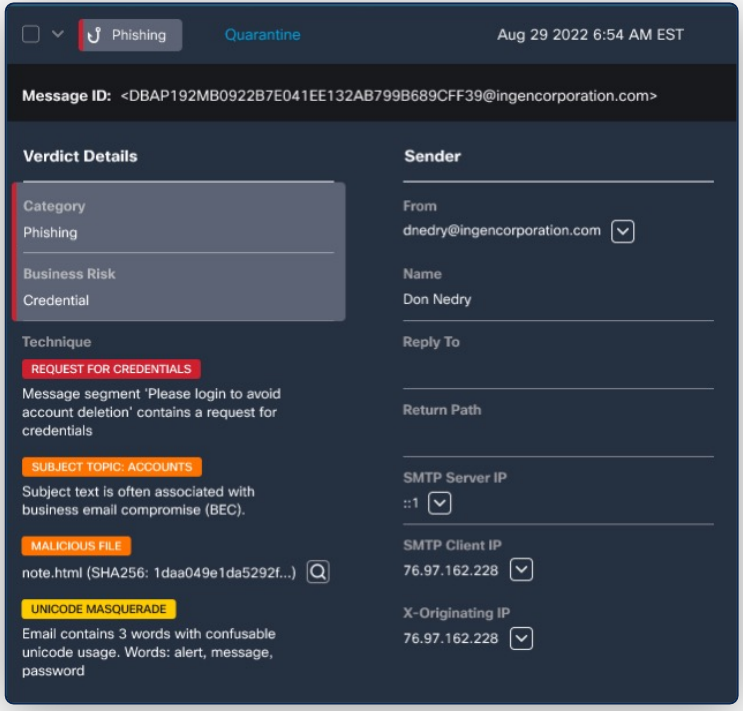




Resposta Rápida e Integrada

Categorização, identificação de Riscos e Técnicas

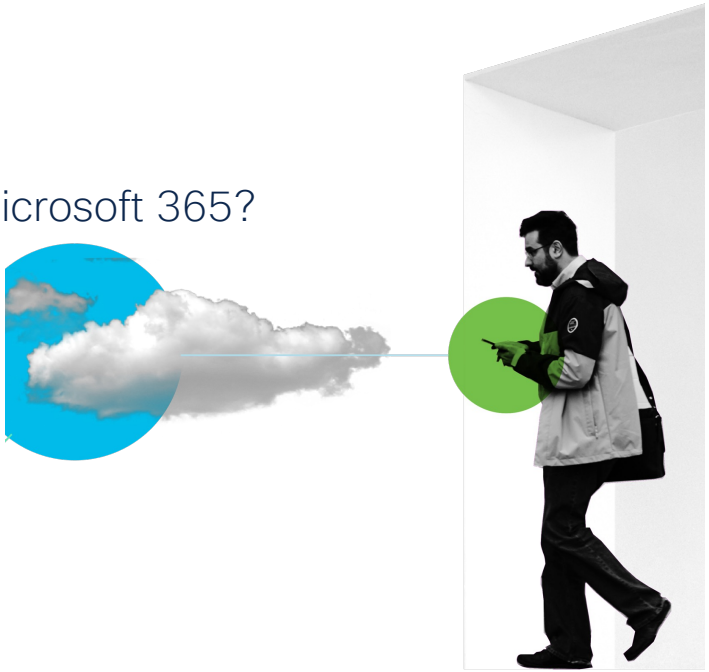
Graymail	Marketing	Social	Bulk	Spam
Spam	Junk	Win Big	Bot / DGA	Education
	Adult	Pharma	Reputation	Job / Offer
Scam	Fraud	Advance Fee	Fake Company	ATO
	Extortion	Charity	Romance	Investment
	Lottery	Employment	Inheritance	Money Mule
Phishing	Credential	Financial	Doc Share	Forgery
Business Email Compromise	Identity	Brand	Spoof/Cousin	ATO (external)
	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



Redução de risco: Remediacão

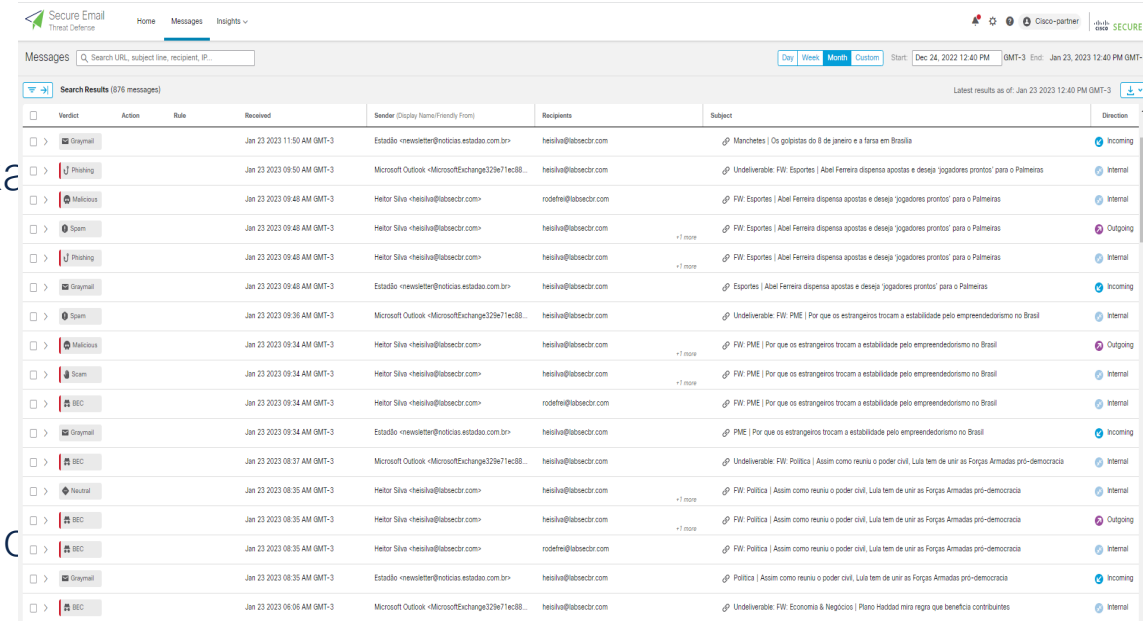
Detectamos uma URL suspeita o que fazer?

- 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

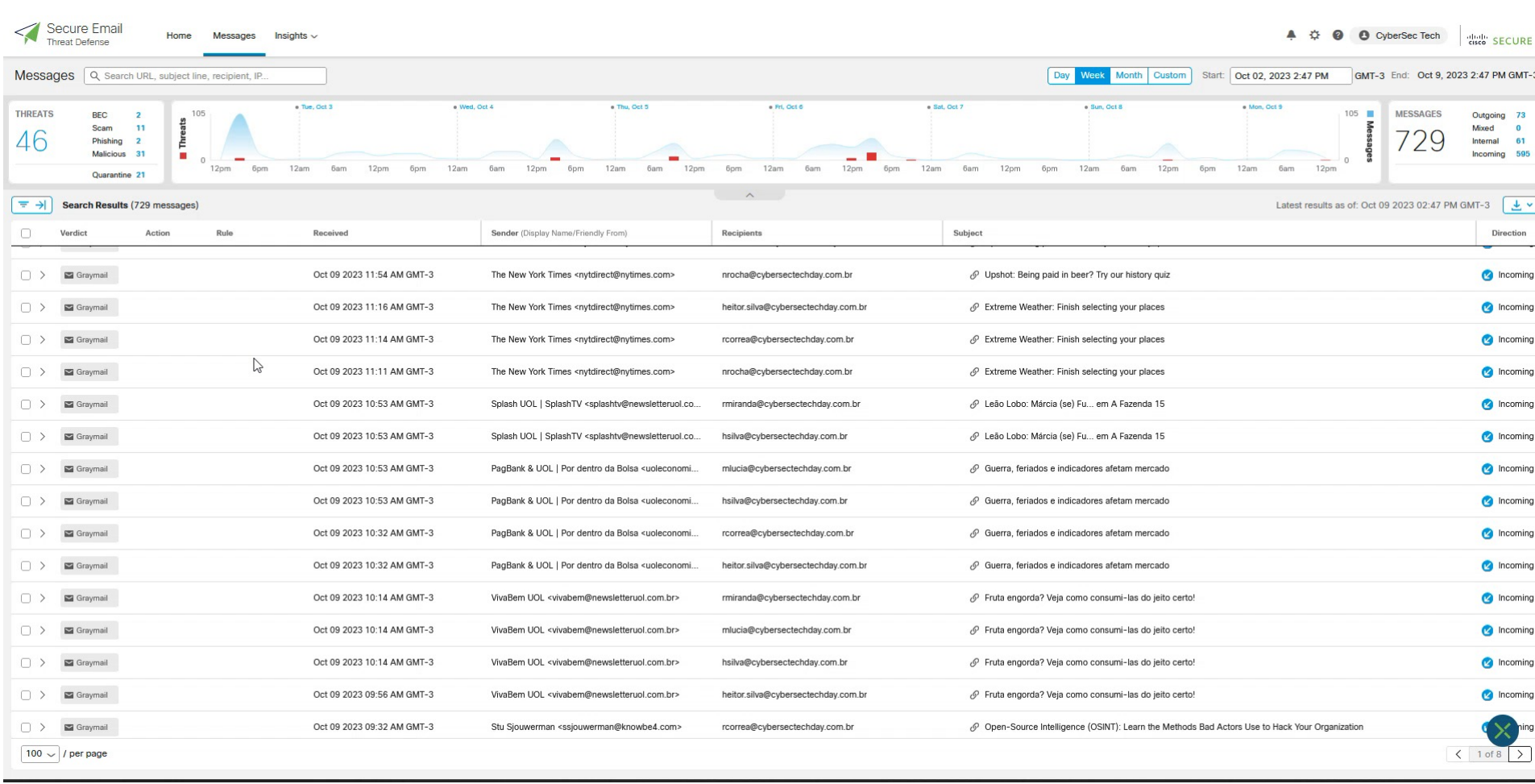
- Pesquise instantaneamente por observáveis relevantes
- Sintaxe de pesquisa simples
- Sem usar ferramentas complexa
  - Message Trace
  - Power Shell
  - Compliance Search
- Sem envolver especialistas
- Visibilidade dos usuários afetado



Pesquisa e remediação rápidas, quando os minutos são valiosos

12x
Redução de tempo

para pesquisa e correção de mensagens em caixas de correio



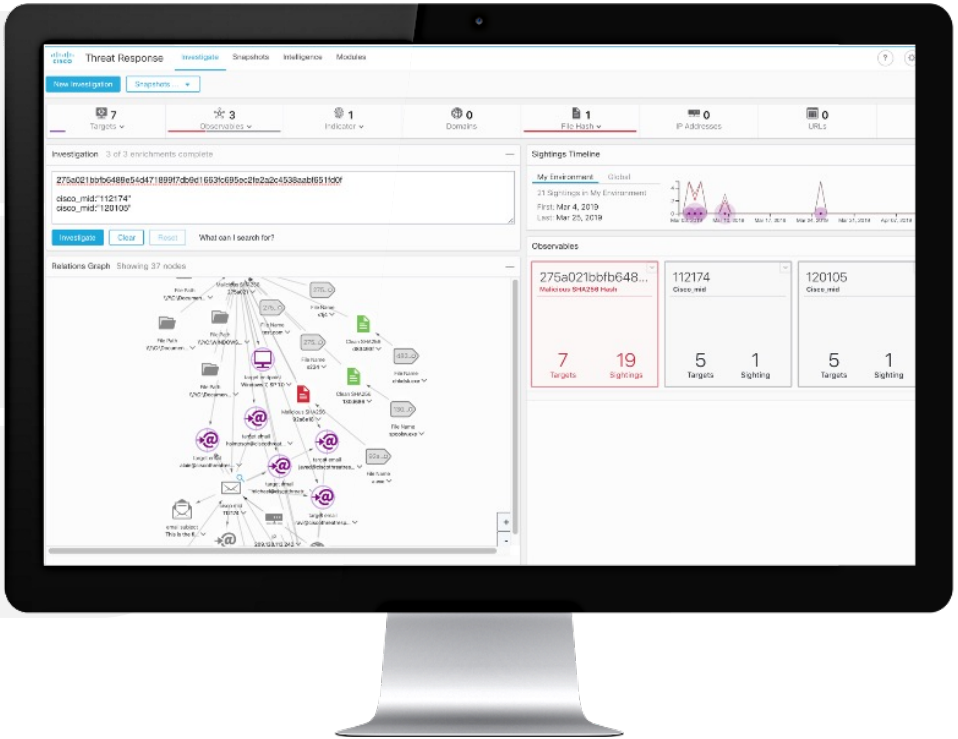
Cisco Secure Email & XDR Threat Response

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

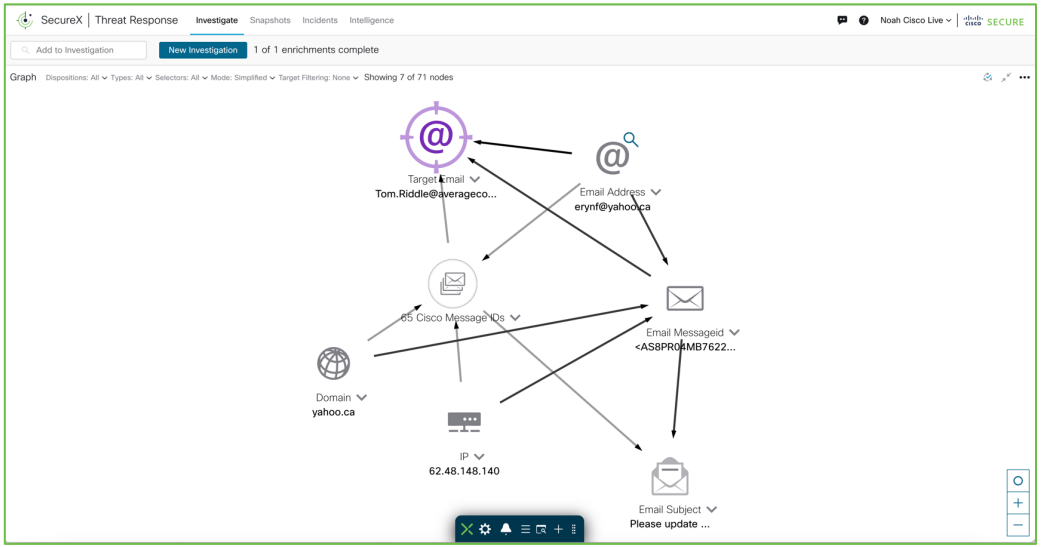
Pesquise vários endereços de e-mail, assuntos e anexos de uma só vez para entender como uma ameaça se espalhou entre os elementos da rede

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!

cisco · Mais que tecnologia · LOGICALIS Architects of Change · NTT · teletex