
cisco Live!
Let's go

The bridge to possible

How to Detect, Protect and Remediate against Email-based Threats

With ETD and XDR

Matt Robertson, Distinguished Engineer
Abdalla Taha, Technical Solutions Architect

About This Session

Email: The Number One Threat Vector







Hey man, click this link:
http://badthingshappenwhenyouclickhere.com

Absolutely! Thanks for forwarding!

Detection and Response to Email Based Threats

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

About This Session

Sergio Pinto



Email: The Number One Threat Vector







Hey guys, sadly I'm not going to make it to Cisco Live; click here: http://presentmysession.com

No worries buddy, we got you!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

About Us



Matt Robertson:
- Distinguished Engineer
- Threat Detection and Analytics
- Cisco Live Distinguished Speaker
- 15.5 years at Cisco
- Canadian eh



Abdalla Taha:
- Technical Solutions Architect
- Cisco Secure Email Specialist
- 8.5 Years at Cisco
- Palestinian-Moroccan living in Finland

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

Detection and Response to Email Based Threats

Agenda:

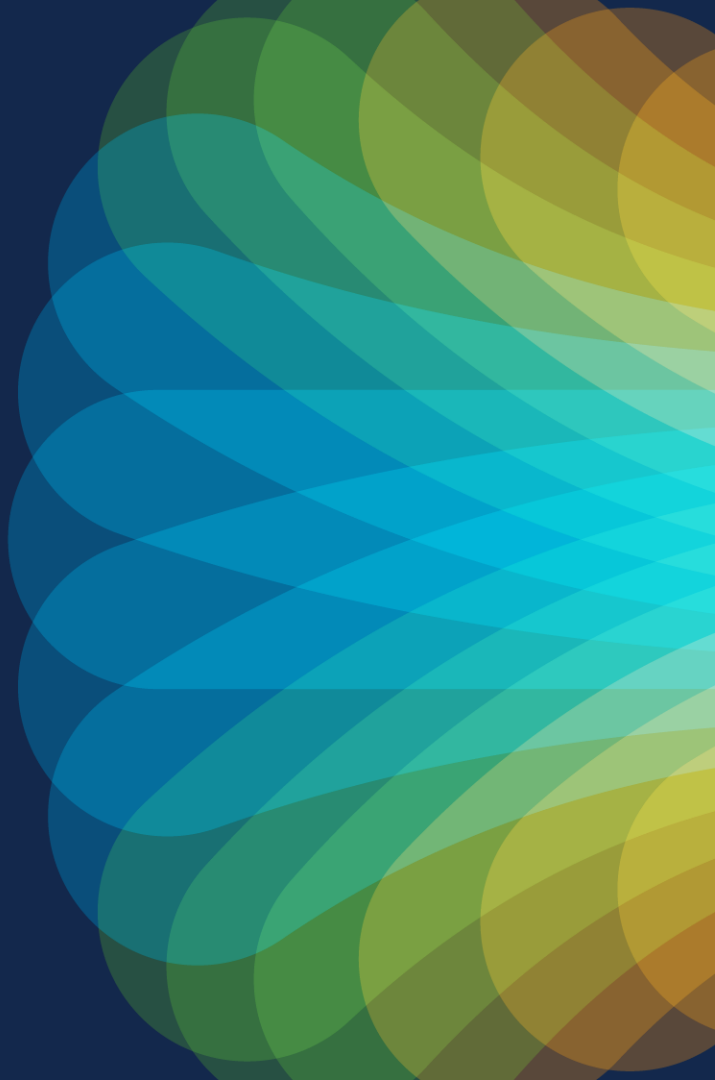
- Introduction
- Why is Email so Vulnerable?
- Cisco Secure Email Threat Defense
- Advanced Detection Techniques
- Extended Detection and Response with XDR
- Summary





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why is Email so vulnerable?



Simple Mail Transfer Protocol



From: 11.12.13.14
$ telnet alln-mx-01.cisco.com 25
Trying 173.37.147.230...
Connected to alln-mx-01.cisco.com.
Escape character is '^]'.
220 alln-inbound-e.cisco.com ESMTP
helo mail.sender.com
250 alln-inbound-e.cisco.com
MAIL FROM:<admin@sender.com>
250 sender <admin@sender.com> ok
RCPT TO:<user1@cisco.com>
250 recipient <user1@cisco.com> ok
DATA
354 go ahead
Subject: TEST MESSAGE
From: Email Admin <admin@sender.com>
To: User One(user1) user1@cisco.com

Here is the email, hope you receive it.
.
250 ok: Message 143004492 accepted
quit
221 alln-inbound-e.cisco.com
Connection closed by foreign host

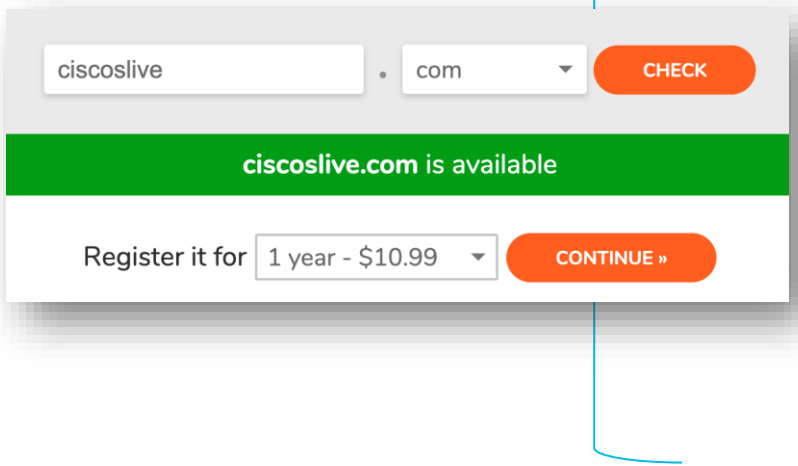
Envelope

Header

Body

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security?




```
Connected to alln-mx-01.cisco.com.
Escape character is '^]'.
220 alln-inbound-e.cisco.com ESMTP
helo notMandatory.lol
250 alln-inbound-e.cisco.com
MAIL FROM:<any.domain@withNOspf.com>
250 sender <any.domain@withNOspf.com> ok
RCPT TO:<victim@cisco.com>
250 recipient <victim@cisco.com> ok
DATA
354 go ahead
Subject: You are a Cisco Live Winner!
From: Cisco Live <winner@ciscoslive.com>
To: Luckiest Man on Earth <is.me@cisco.com>

Congratulations... you won an Apple Vision Pro!
Claim you prize by clicking here:
applevisionprociscolive.xyz/claim/my/price

<pictures of Apple Vision Pro>
.
250 ok:  Message 143004493 accepted
quit
221 alln-inbound-e.cisco.com
Connection closed by foreign host
```

Envelope

Header

Add a DKIM key with d=ciscoslive.com and DMARC will pass

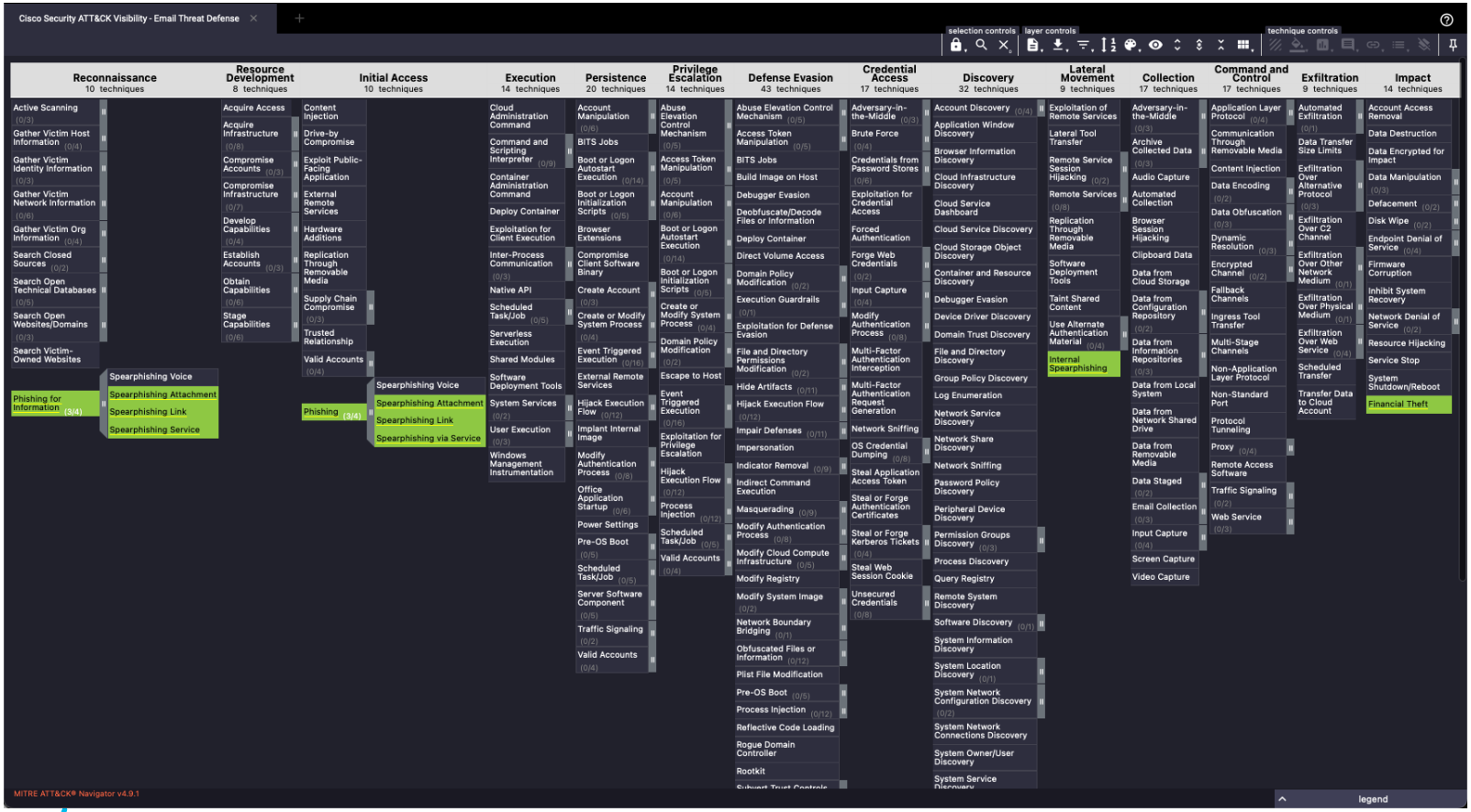
Body

Domain that has been neutral for a long time

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Email as a threat vector

https://attack.mitre.org



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Email as a threat vector



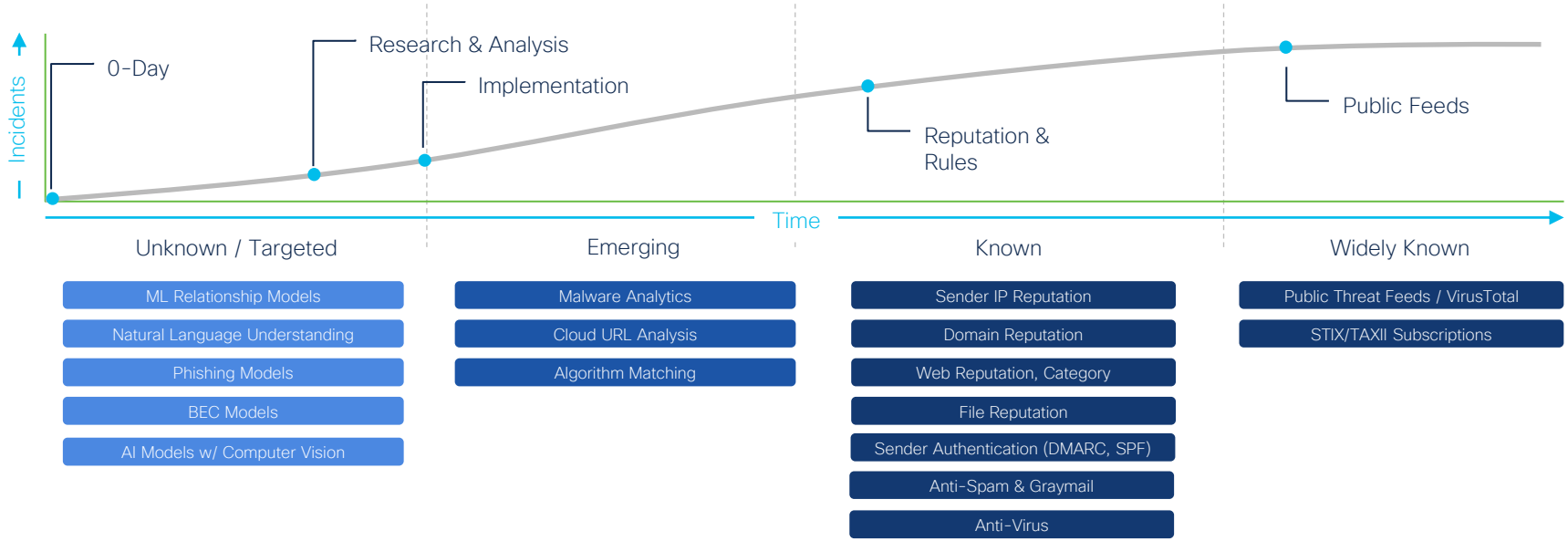
Email serves as a primary entry point



And can be a means of success

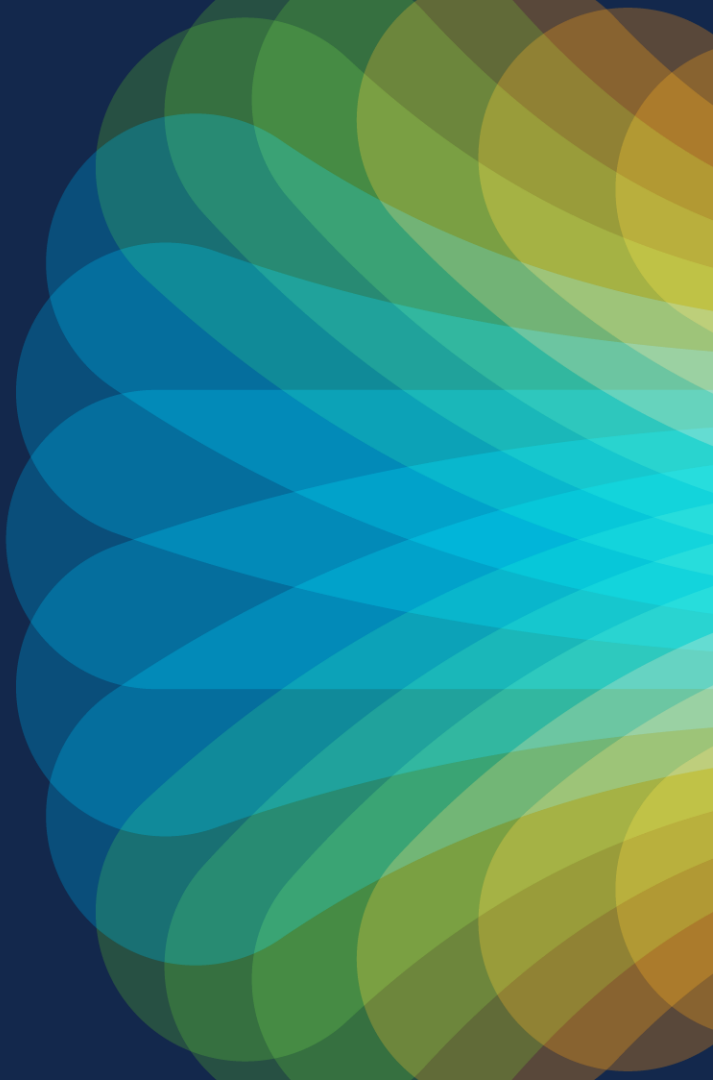
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Advanced Threats Life Cycle



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Email Threat Defense



cisco Live!

Cisco Secure Email Portfolio

On premise



CISCO SECURE Email Gateway

Email Security Appliance (ESA, IronPort)



CISCO SECURE Email and Web Manager

Security Management Appliance (SMA)

Cloud

CISCO SECURE Email Threat Defense

Cloud Mailbox (CM, CMD)

CISCO SECURE Email Cloud Gateway

Cloud Email Security (CES)

& more

CISCO SECURE Awareness Training

CISCO SECURE Domain Protection

RED SIFT

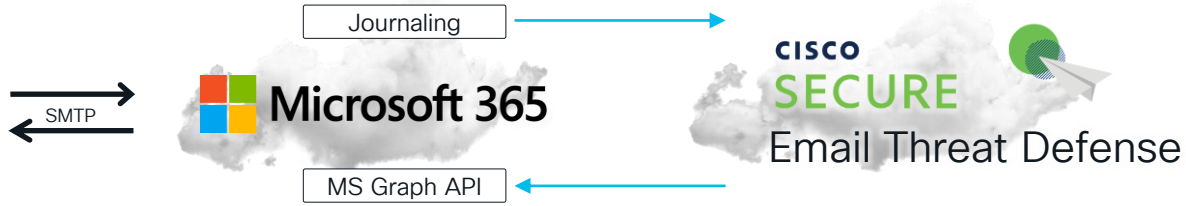
CISCO SECURE Email Archiving

THETALAKE

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Email Threat Defense

Improve Microsoft 365 email security



- Setup takes 5 minutes!
- Scan emails in parallel with Microsoft 365
- No changing of MX records or redirecting traffic
- Mitigate malicious emails automatically and on-demand via API access
- Closes security gaps that Microsoft has by scanning emails also with Behavioural Analytics (AI/ML) and by detecting internal threats

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Email Threat Defense

Improve your gateway



- Works as an add-on to your gateway by adding Behavioural Analytics
- Detects internal threats
- Mitigate malicious emails automatically and on-demand

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Email Threat Defense

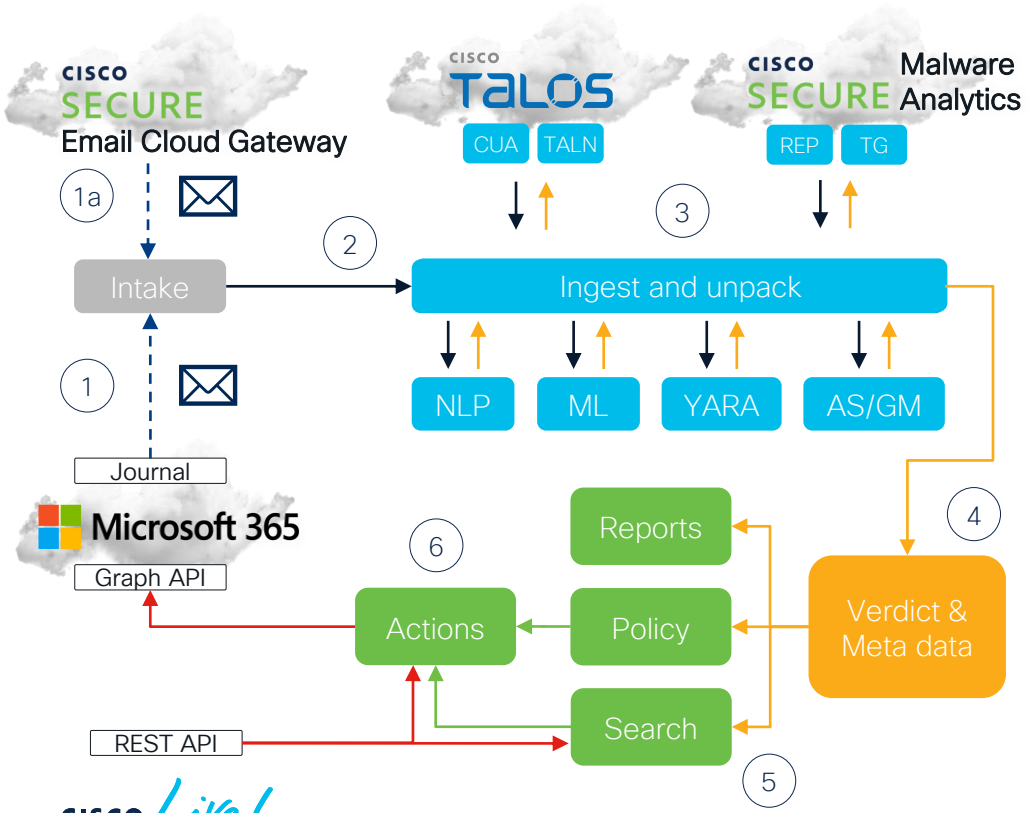
Improve your gateway



- Works as an add-on to your gateway by adding Behavioural Analytics
- For mitigation, custom workaround needed with APIs

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

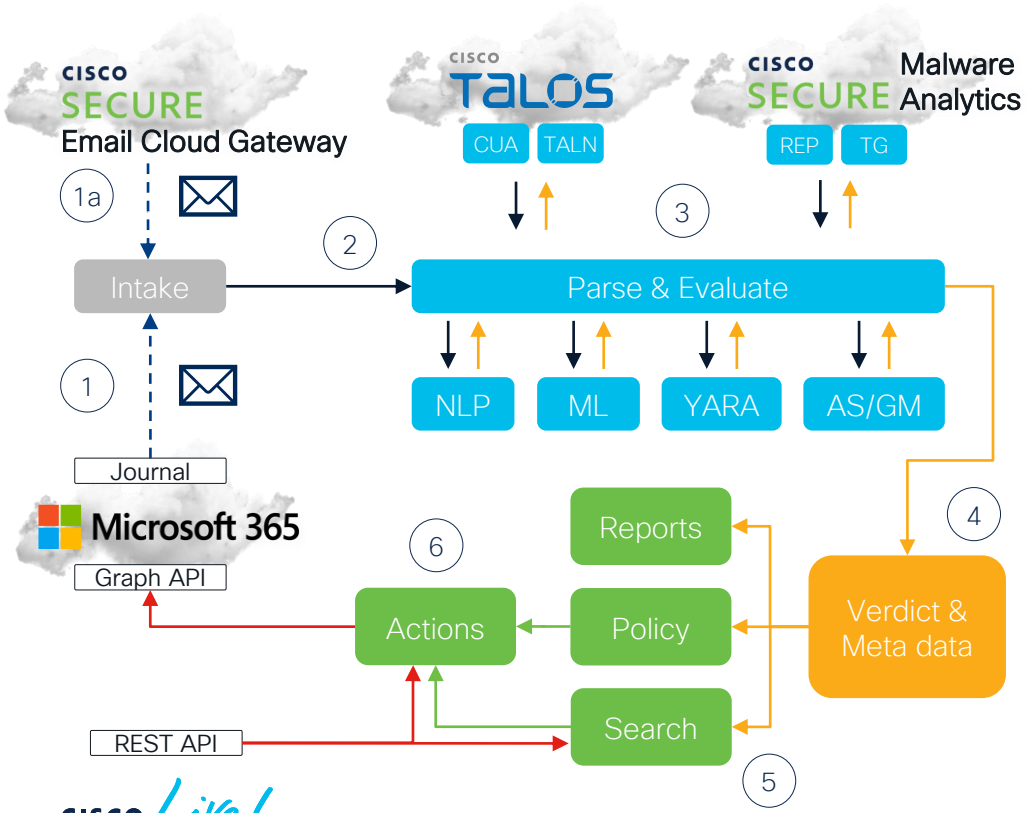
Inside Email Threat Defense



1. Microsoft 365 Journal copy of inbound, outbound and internal messages is received
   1a. ETD connector on Secure Email Gateway sends copies of inbound emails to ETD
2. The intake service ingests the message and unpacks the journal / email copy for parsing and evaluation
3. The message is parsed and evaluated in parallel against all the engines
4. Based on a confidence and weighting algorithm, a verdict is returned along with the metadata
5. Metadata is indexed to use for searches, reports and for policy evaluation
6. Automatic and on-demand actions associated with verdicts are acted upon via the Graph API

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Email Threat Defense

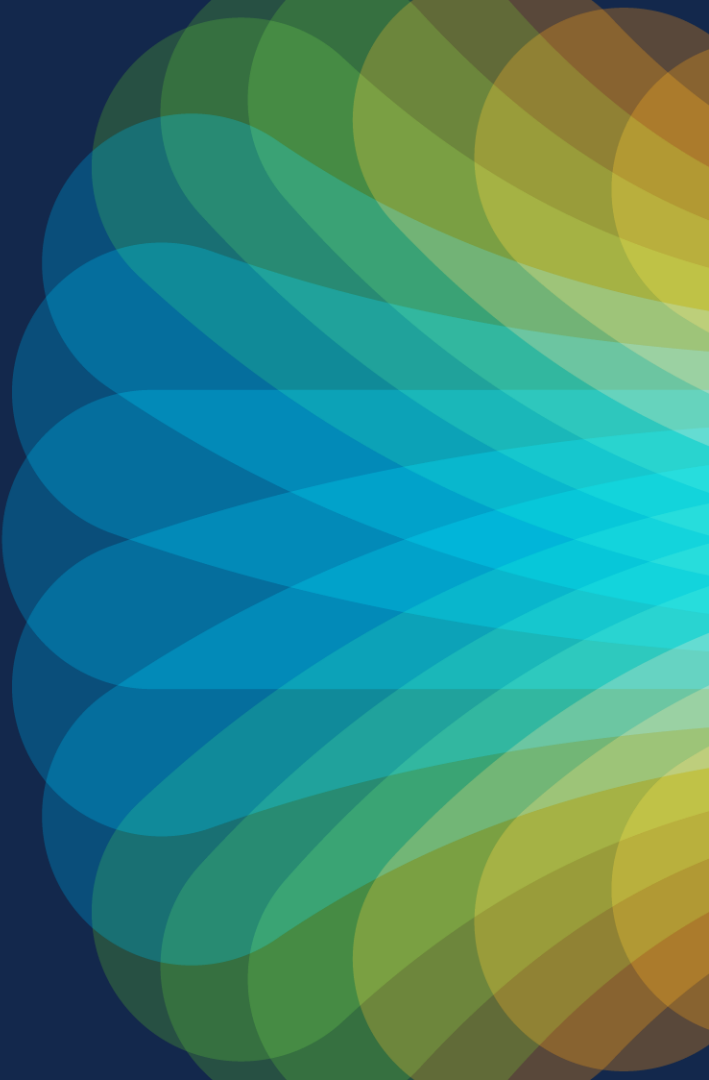


Acronyms

- CUA = Cloud URL Analysis, URL sandboxing to detect zero-day phishing and malware URLs
- TALN = Talos Anti-spam Logical eNgine
- REP = File reputation, based on SHA256
- TG = Threat Grid, file sandboxing to detect zero-day malware from email attachments
- NLP = Natural Language Processing
- ML = Machine Learning
- YARA = Yet Another Ridiculous Acronym link
- AS = Antispam
- GM = Graymail

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Advanced Detection Techniques



Email: The Number One Threat Vector

Exploiting the weakness of people





Hey man, click this link:
http://badthingshappenwhenyouclickhere.com



Absolutely! Thanks for forwarding!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Exploiting People



- Desire to help
- Trust
- Relationships
- Laziness
- Knowledge
- etc.

Example Exploit Techniques (Verdicts)

- Scam
- Phishing
  - Spear Phishing
- Business Email Compromise
- SPAM
- Graymail

Absolutely! Thanks for forwarding!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Email Scams back in the day







Hey man, I'm a Nigerian prince and need some money, can you help me out? It will be worth your while.

Absolutely! Here's some money!

https://en.wikipedia.org/wiki/Advance-fee_scam

- Basic con-job
- Promise large amount of return for small up-front payment
- Con artist disappears with money

'Nigerian prince' email scams still rake in over $700,000 a year—here's how to protect yourself

Published Thu, Apr 18 2019·2:38 PM EDT

https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protecting People/Business from People







Innovative criminal:

Evolving techniques and tools

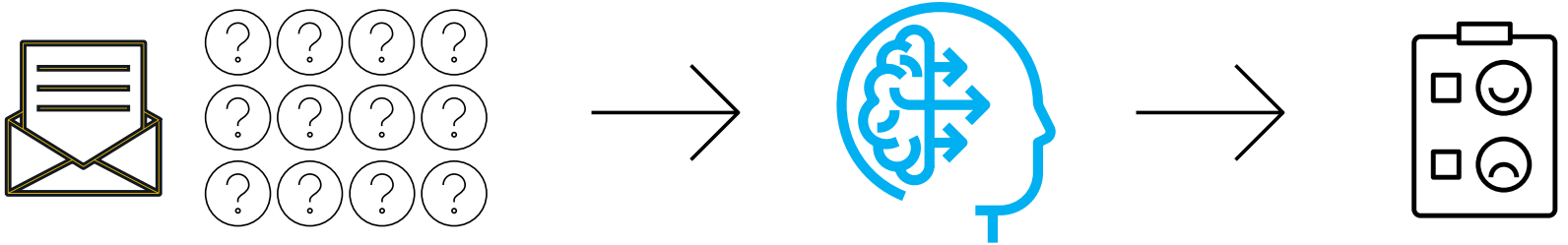
Exploitable Person

Trusted by the business

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

AI/ML can Help Here!

AI/ML can be extremely useful in modelling domains that are not well understood and constantly evolving



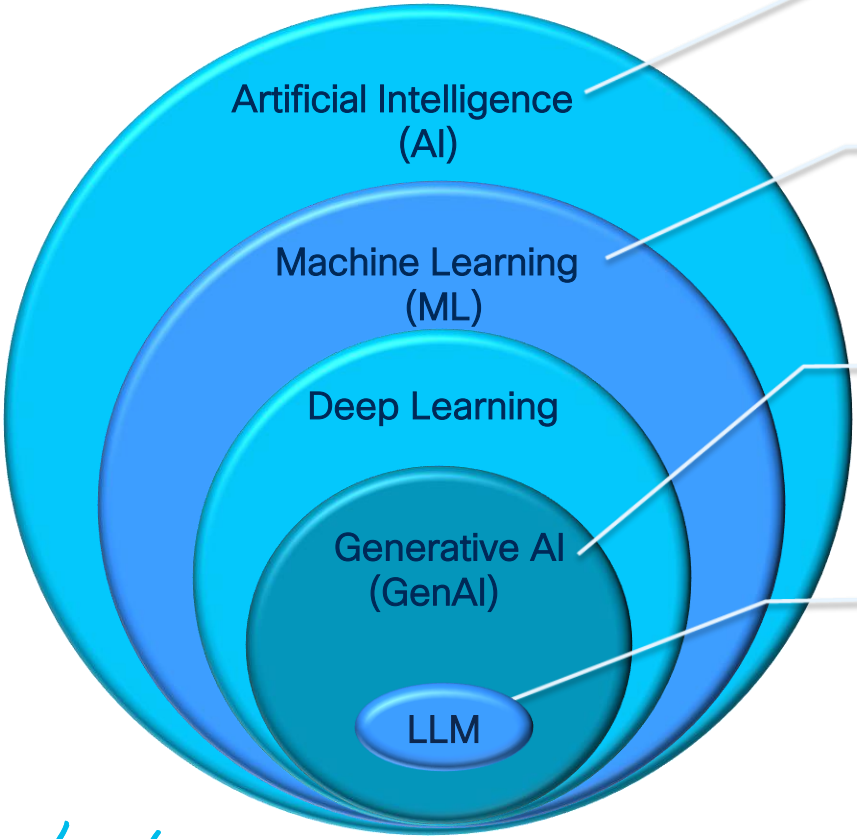
Signals

ML Classifier

Decision

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Aside: Artificial Intelligence Technology



Aims to mimic human behavior

Focuses on learning from data

Aims to generate new data or text that mirrors the input

Large Language Models (LLM) include GPT and ChatGPT specializing in understanding and generating human-like test

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Machine and Deep Learning

Current



Primary LLM used for relationship mapping, BEC, and Phishing detectors



BERT is used for call-to-action, Credential Phishing, and Lang filters



Primary NLP Detector for language, sentiment, urgency, and tone of emails



ChatGPT is used for translation and multi-lang models (out of band)



OCR detection that leverages LSTM neural networks for content extraction

Under Development



Leverage BERT to detect BEC patterns and language with sender/recipient relationships



Generative AI for summarization of threat descriptions

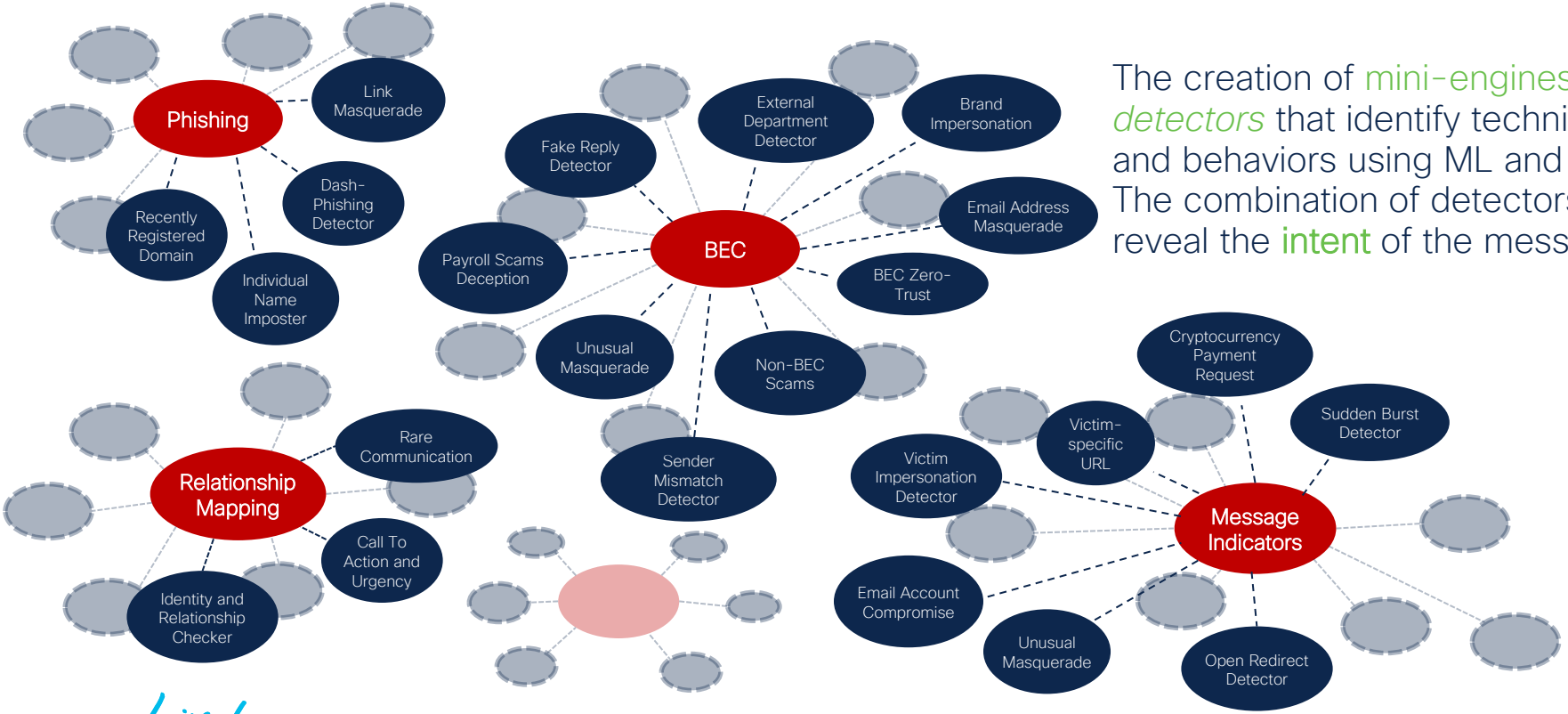


AI Automation (Cisco Assistant) for rule and configuration across security products – LLM selection/testing in progress

Supported languages currently: English, French, Spanish, Catalan, Portuguese, German, Italian, Dutch, Danish, Swedish, Norwegian, Polish, Czech, Slovak, Turkish, and Mandarin Chinese. And the list is growing...

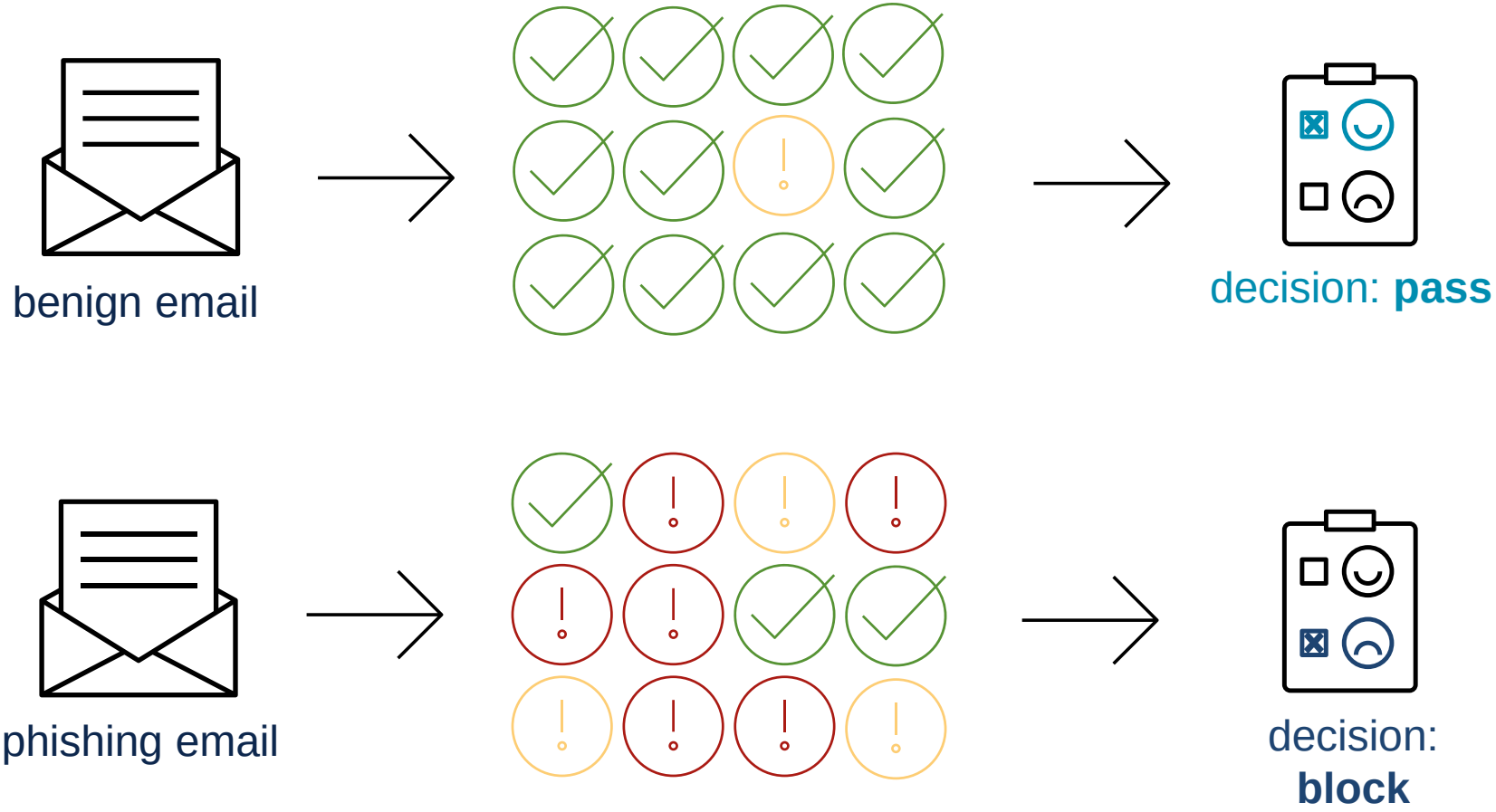
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Layering Detections using Machine Learning



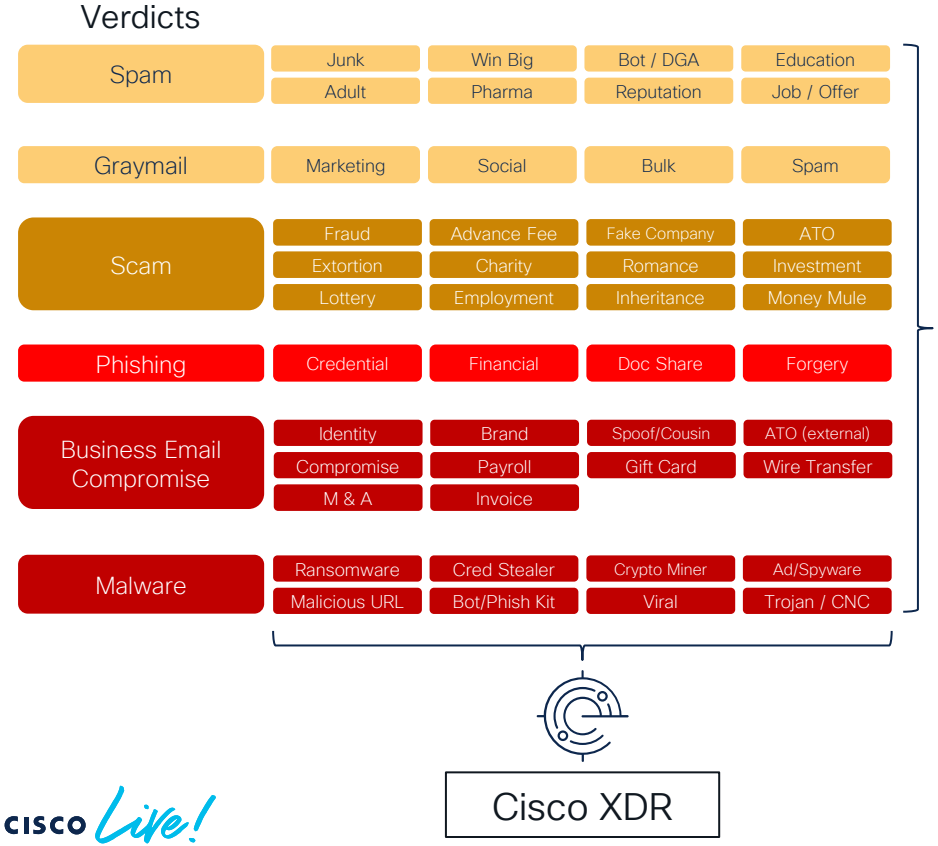
The creation of mini-engines or *detectors* that identify techniques and behaviors using ML and NLP. The combination of detectors reveal the intent of the message.

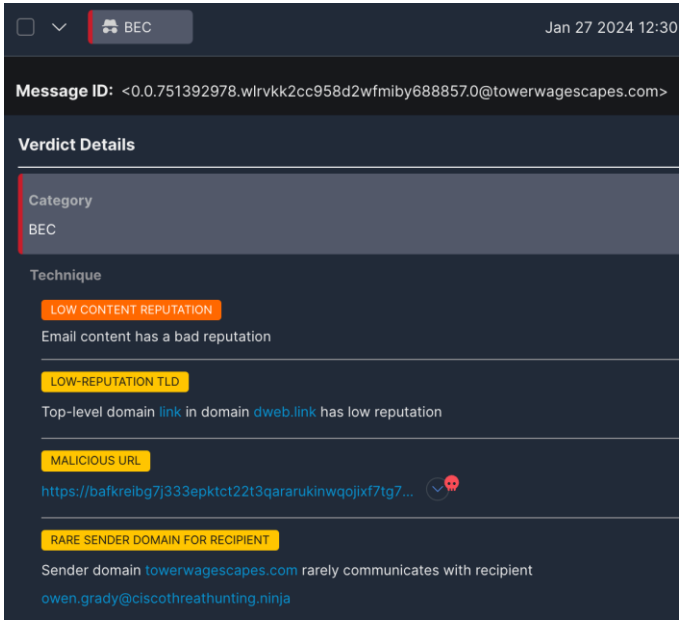
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

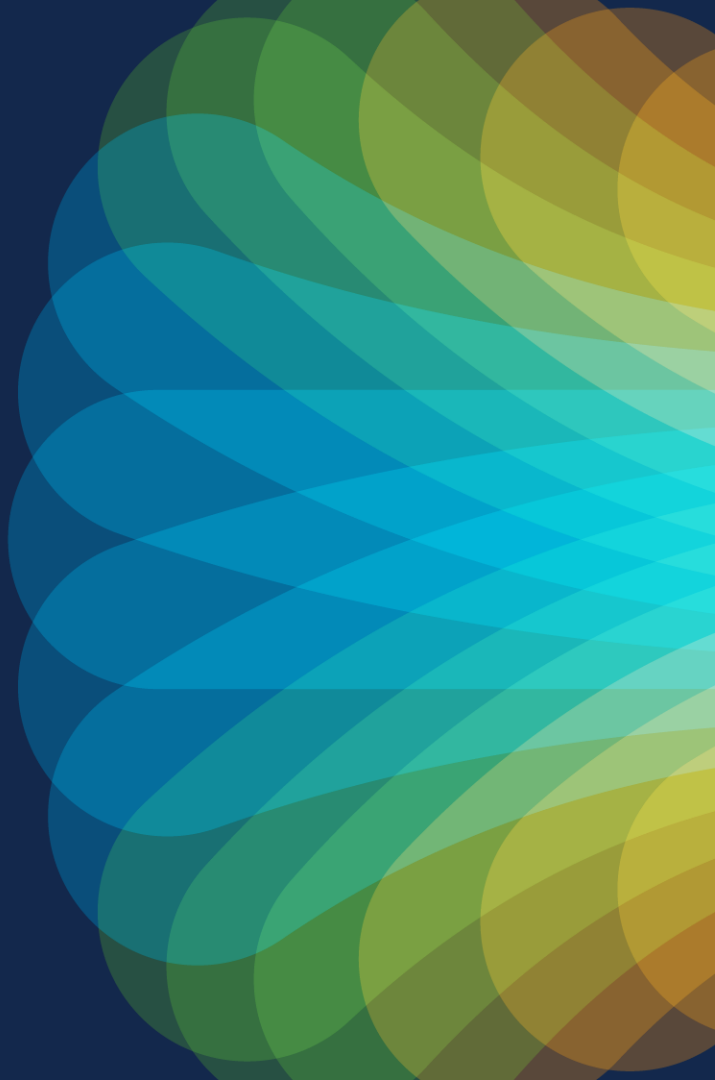
Threat Categorization, Risks and Techniques





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Examples



Phishing and Spear Phishing





Hey man, click this link:
http://badthingshappenwhenyouclickhere.com



Absolutely!

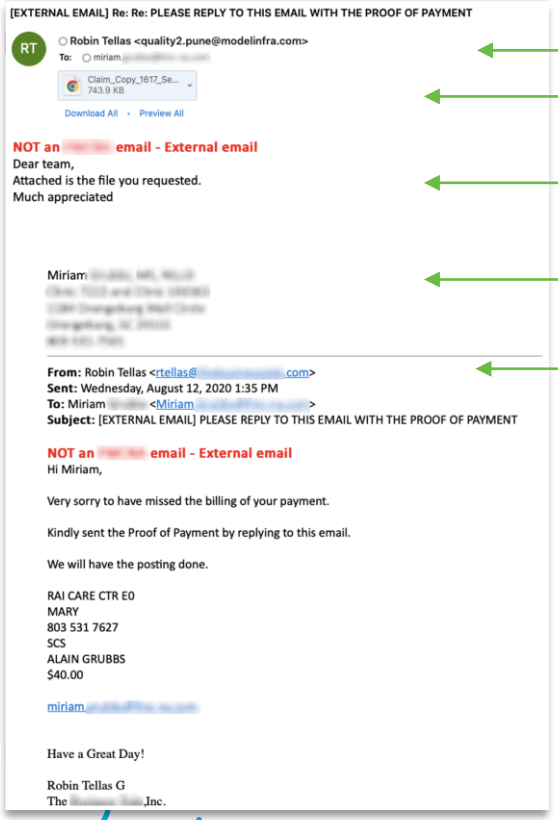
Phishing: Form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malware

Spear Phishing: targeted phishing attack that uses personalised emails

https://en.wikipedia.org/wiki/Phishing

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Anatomy of a Spear Phishing



Spoofed Display Name

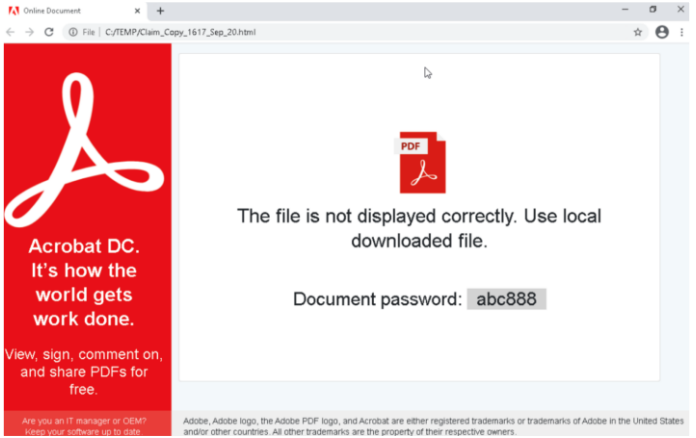
HTML Attachment

Benign Content

Signature of Recipient

Original Sender

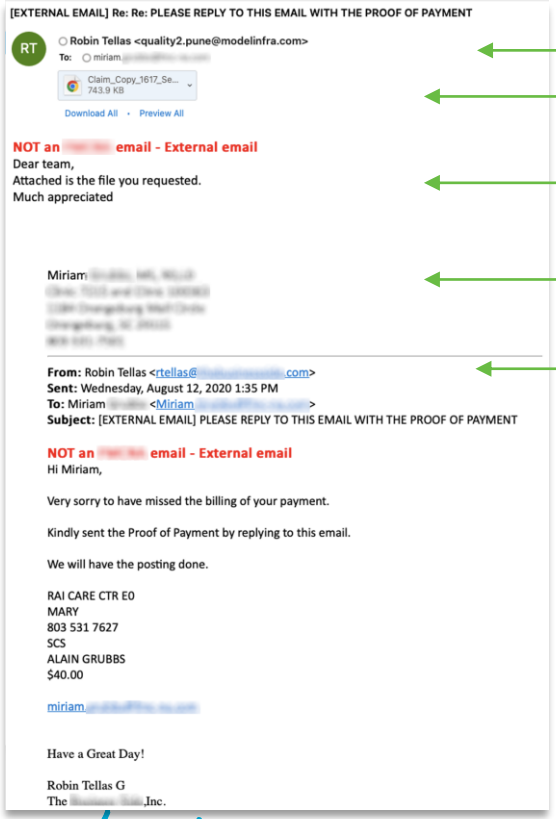
Fake Message History



1. Attachment is an html file
2. When opened it renders a screen that mimics a pdf file that failed to open.
3. It downloads a passworded zip file. The zip file contains a malicious payload

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Anatomy of a Spear Phishing


[EXTERNAL EMAIL] Re: Re: PLEASE REPLY TO THIS EMAIL WITH THE PROOF OF PAYMENT

RT

Robin Tellas <quality2.pune@modelinfra.com>

To: miriam

Claim_Copy_1617_Se... 743.9 KB

Download All · Preview All

NOT an email - External email

Dear team,

Attached is the file you requested.

Much appreciated

Miriam

From: Robin Tellas <rtellas@ .com>

Sent: Wednesday, August 12, 2020 1:35 PM

To: Miriam <Miriam >

Subject: [EXTERNAL EMAIL] PLEASE REPLY TO THIS EMAIL WITH THE PROOF OF PAYMENT

NOT an email - External email

Hi Miriam,

Very sorry to have missed the billing of your payment.

Kindly sent the Proof of Payment by replying to this email.

We will have the posting done.

RAI CARE CTR E0

MARY

803 531 7627

SCS

ALAIN GRUBBS

$40.00

miriam

Have a Great Day!

Robin Tellas G

The Inc.

Spoofed Display Name

HTML Attachment

Benign Content

Signature of Recipient

Original Sender

Fake Message History

RARE SENDER DOMAIN

SENDER NAME MISMATCH

EXTENSION HARMFUL

DECODE MALICIOUS HTML

FAKE REPLY

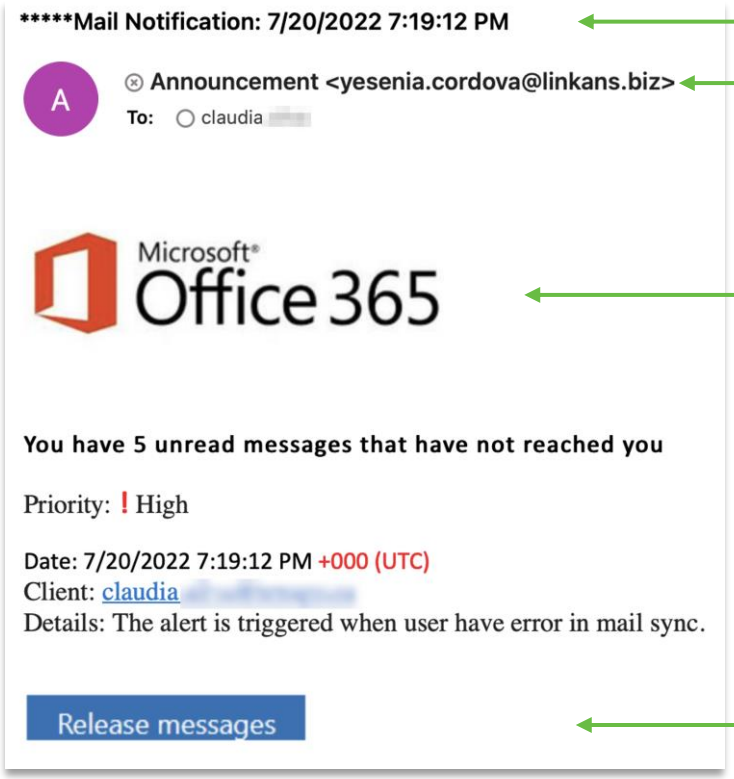
CALL TO ACTION: OPEN ATTACHMENT

VERDICT: THREAT

TYPE: PHISHING

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Credential Phishing



Subject Topic

Sender Display Name Mismatch

Office 365 Logo

Victim-Specific URL, Open Redirect

The entire message is an image and if clicked anywhere it leads to the phishing site. There was also a bunch of random text at the bottom to make it look more legitimate to spam engines. The URL itself was leveraging an open redirect on the American Express site, thus evading most URL detection engines.

Example of open redirect:
http://safe.com/redirect?
url=http://malicious.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Malicious Email





Hey man, check out this attachment:
badthingshappenwhenyouopenthis.pdf

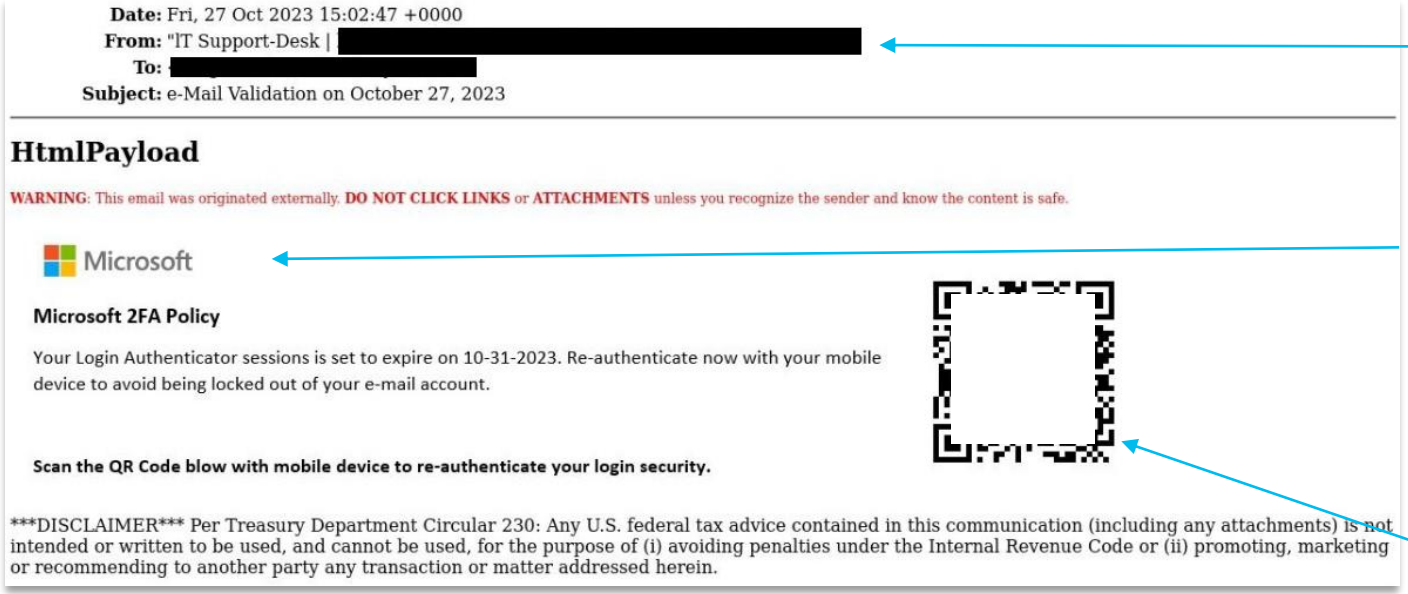


Absolutely!

Email is designed to trick the user into installing malicious software

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Malicious Email



Date: Fri, 27 Oct 2023 15:02:47 +0000
From: "IT Support-Desk | [redacted]
To: [redacted]
Subject: e-Mail Validation on October 27, 2023

HtmlPayload

WARNING: This email was originated externally. **DO NOT CLICK LINKS** or **ATTACHMENTS** unless you recognize the sender and know the content is safe.

Microsoft

Microsoft 2FA Policy

Your Login Authenticator sessions is set to expire on 10-31-2023. Re-authenticate now with your mobile device to avoid being locked out of your e-mail account.

Scan the QR Code blow with mobile device to re-authenticate your login security.

DISCLAIMER Per Treasury Department Circular 230: Any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

Sender Impersonation, Spoofed sender,

Brand Impersonation

Malicious link in QR payload

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Business Email Compromise





Hey man, please pay the attached invoice



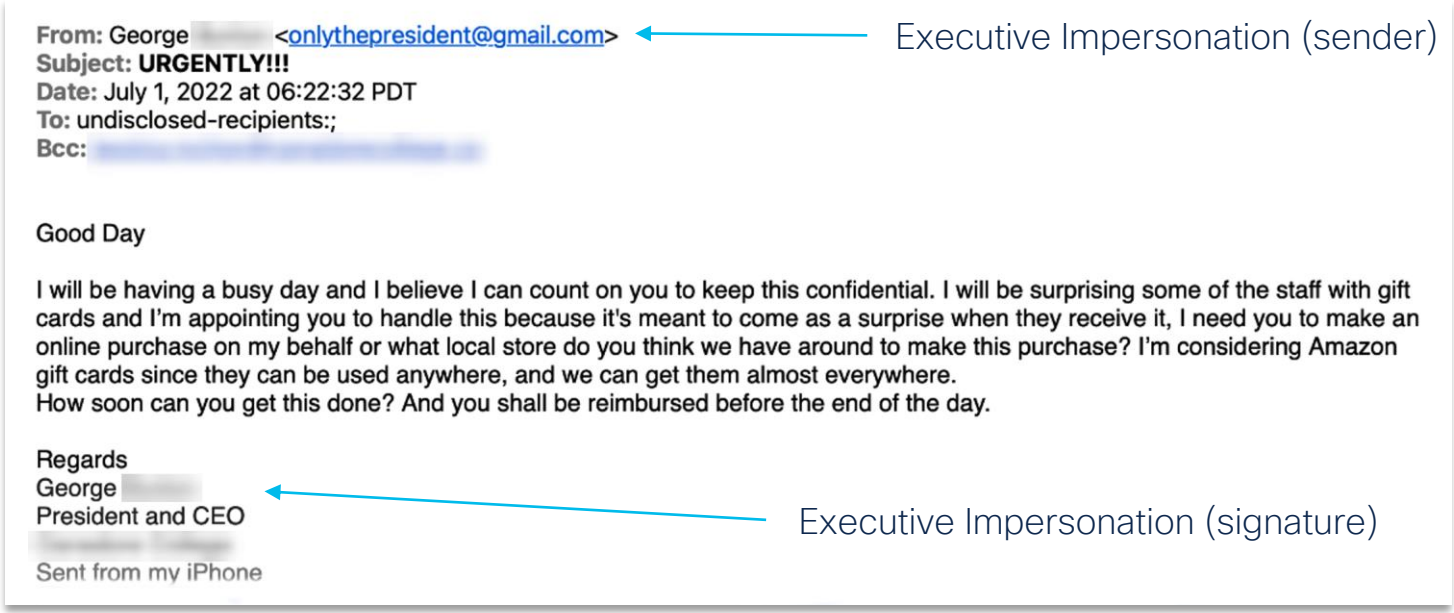
Absolutely!

Leveraging email fraud to attack an organization to achieve a specific outcome which negatively impacts the target organization. For example, an Invoice scam.

https://en.wikipedia.org/wiki/Email_spoofing#Business_email

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

BEC – Gift Card Scam



From: George [redacted] <onlythepresident@gmail.com>
Subject: **URGENTLY!!!**
Date: July 1, 2022 at 06:22:32 PDT
To: undisclosed-recipients:;
Bcc: [redacted]

Good Day

I will be having a busy day and I believe I can count on you to keep this confidential. I will be surprising some of the staff with gift cards and I'm appointing you to handle this because it's meant to come as a surprise when they receive it, I need you to make an online purchase on my behalf or what local store do you think we have around to make this purchase? I'm considering Amazon gift cards since they can be used anywhere, and we can get them almost everywhere.
How soon can you get this done? And you shall be reimbursed before the end of the day.

Regards
George [redacted]
President and CEO
[redacted]
Sent from my iPhone

Executive Impersonation (sender)

Call to action; Gift Card

Executive Impersonation (signature)

Impersonation of President and CEO of a certain College. The peculiar thing here is this BEC email was sent as a campaign to many employees in the organization. This is an unusual trend.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

BEC: Initial Lure

Establish a conversation





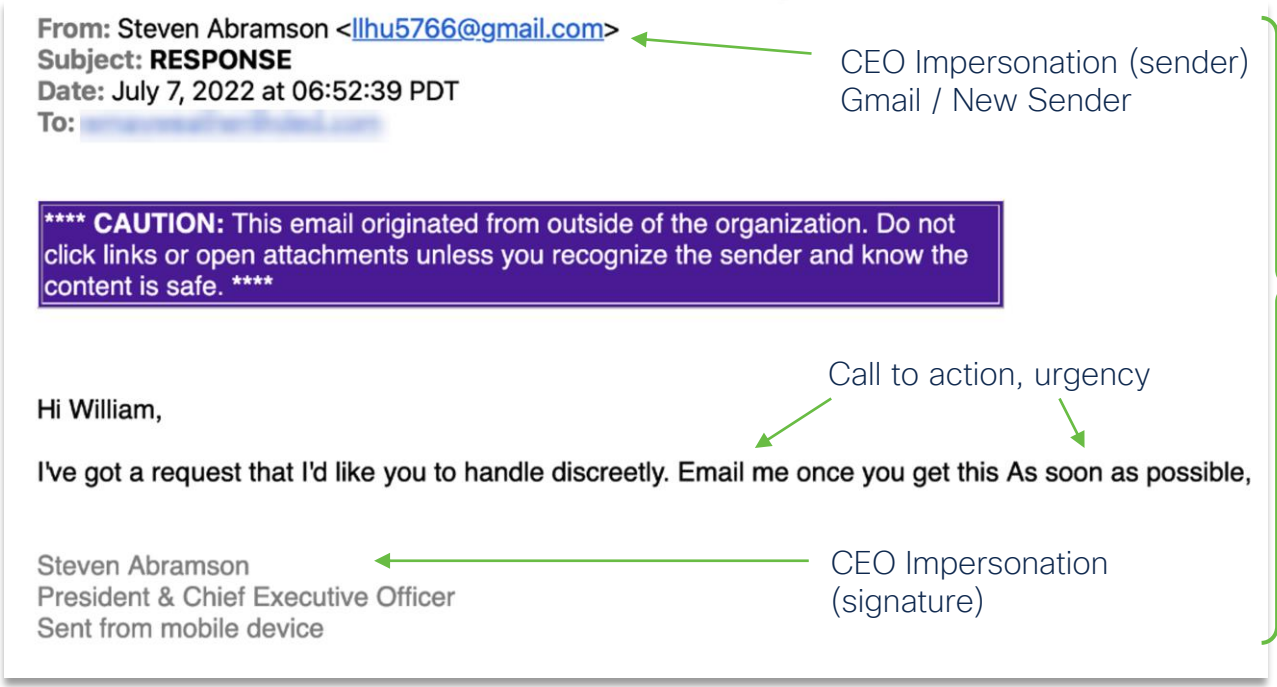
Hey man, can you send me your WhatsApp number? I need to send you something...



Absolutely! Here you go +358 2245...

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

BEC – Initial Lure



The threat Actor is impersonating Steven Abramson, President and CEO of Universal Display. Email was sent to many employees including Senior Director, Scientists of the company. No customer input needed to detect the VIP spoof.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

BEC: Payroll Scam

Deception of being employed in the company





I've got a new bank account; I want to update my payroll details.



Absolutely! Please send your new account info...

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Payroll Scam

From: Brad Green <ooficeonee@gmail.com>
Subject: **[EXTERNAL] - PAYROLL ACCOUNT UPDATE**
Date: July 11, 2022 at 07:25:36 PDT
To: [redacted]

Impersonation (sender)
Gmail / New Sender

Good Day,

I have a new account details which I would like to be my new payroll direct deposit information for all future payments. Can I please get a direct deposit form to fill out or do I just email you the details?
Kindly Advice.

Payroll Request coming from external

Thank you for your assistance
Regards,

Brad Green
Professor of Theological Studies

Impersonation (signature)

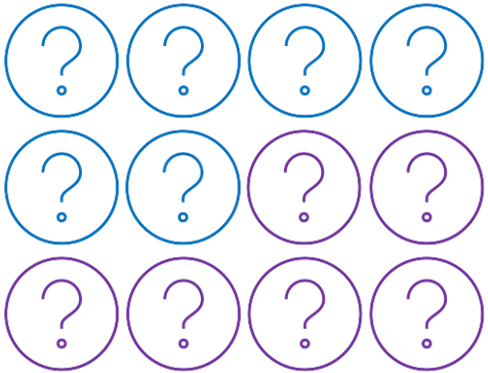
This is another interesting behavior in BEC Payroll Scam which we detected. The same sender is changing its display name and sending Payroll Scam emails to people in the same org with different signatures but the same message.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Some of the logic behind the scenes

Context vs Content





Context-based signals consider the **relationship** between entities

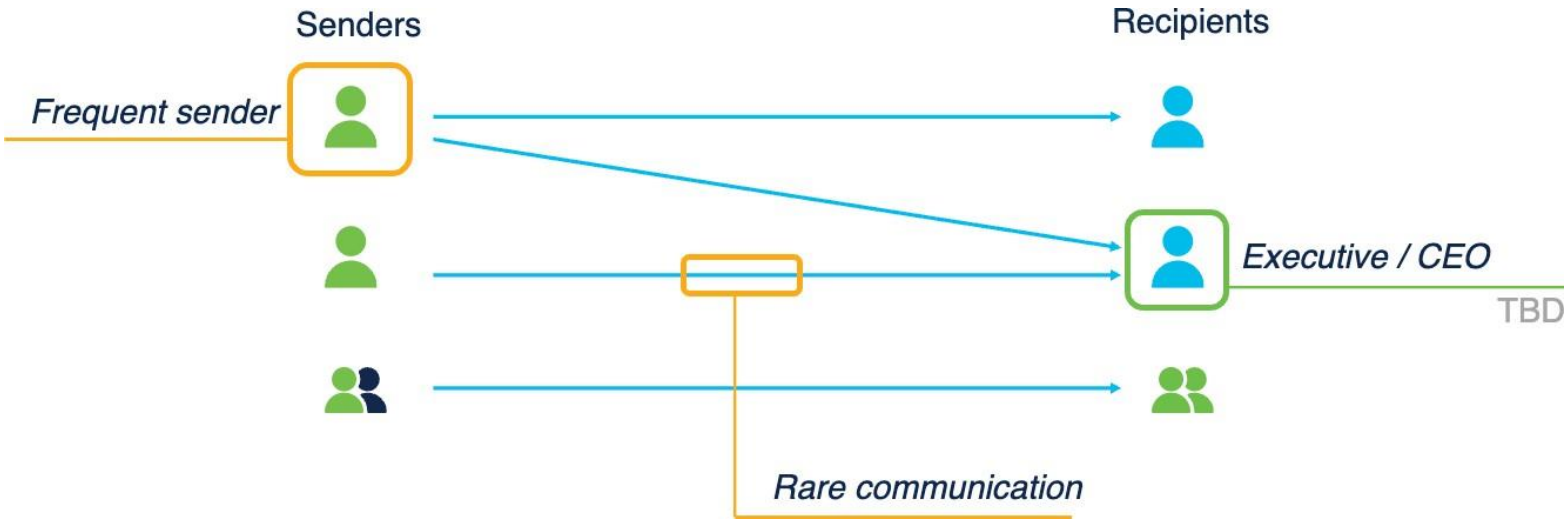


Content-based signals analyze the **individual** email



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Communication Modelling



8%
Of all emails are from ‘rare’ senders

90%
Of phishing are from ‘rare’ senders

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example Content Signals

Brand Impersonation

Hidden Text

Call To Action

Unicode Masquerade

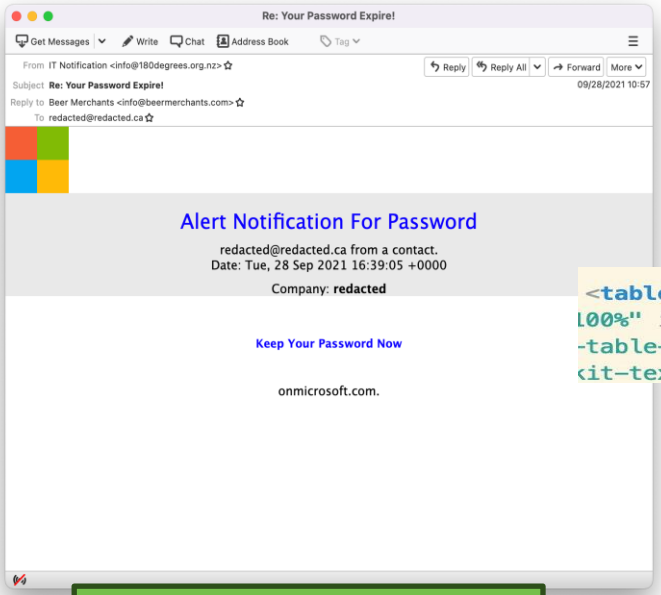
Subject Topic Understanding

Sender Text Mismatch

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

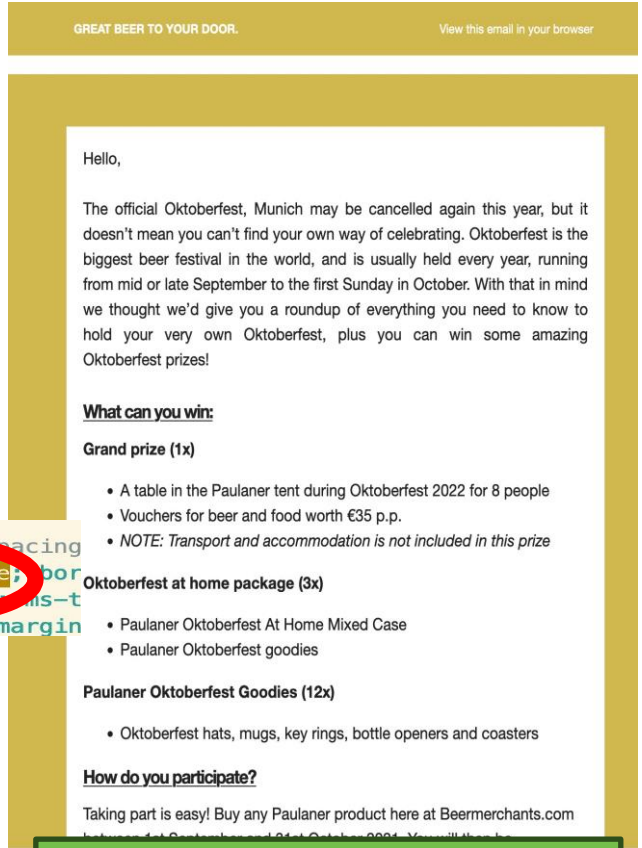
Hidden Text example

Hide text to confuse classic filter techniques



What the user sees

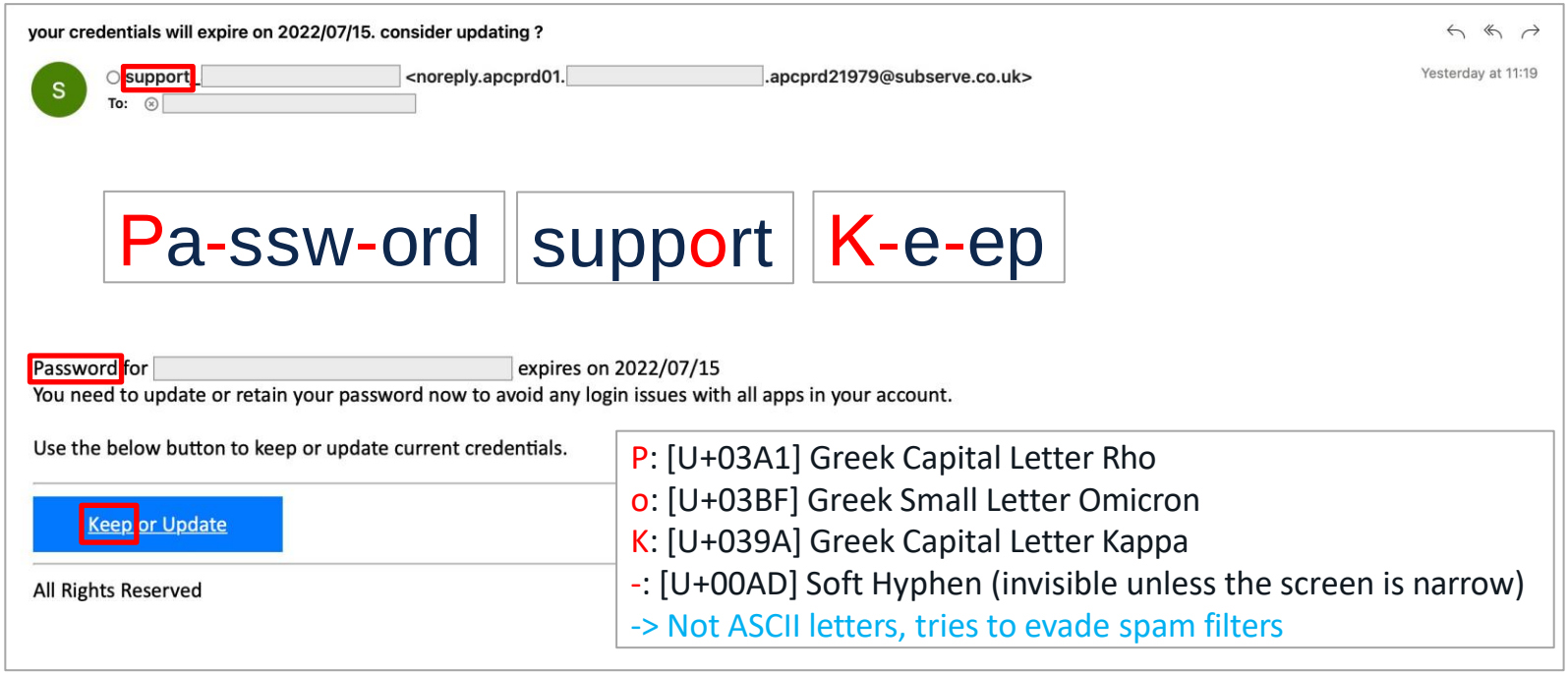
```
<table border="0" cellpaddi                    acing
100%" id="bodyTable" style                DiSplAy:nONe; bor
-table-lspace: 0pt;mso-tab                rspace: 0pt                ms-t
xit-text-size-adjust: 100%;height: 100%;margin
```



What the computer sees

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unicode Masquerade

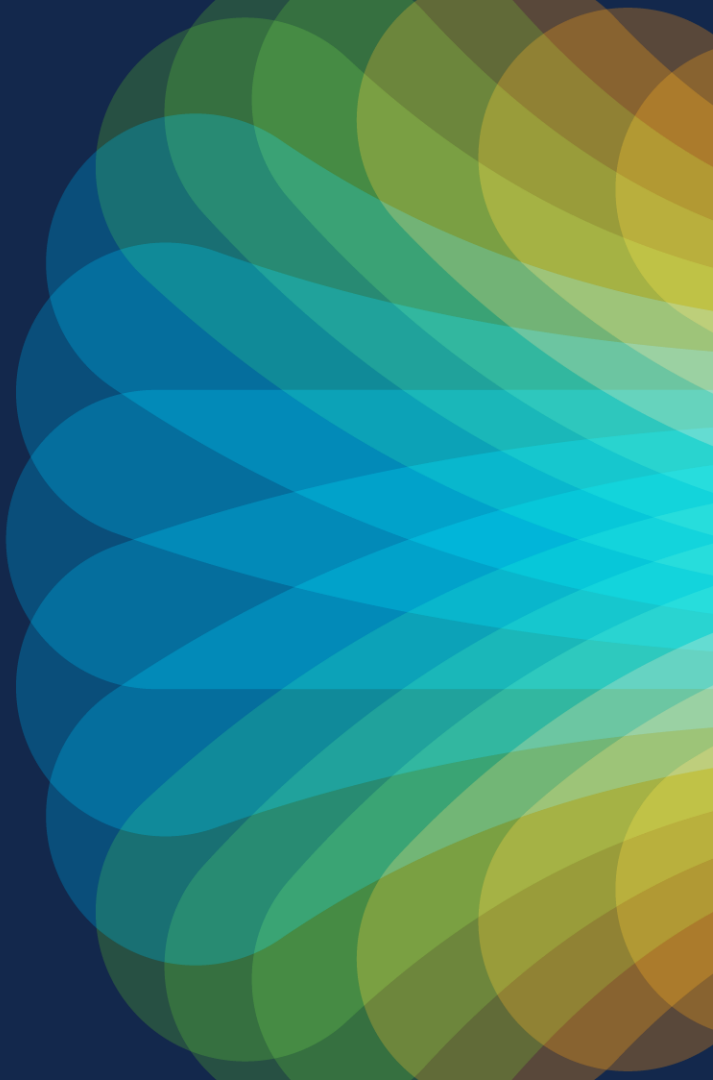


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Email Threat Defense Demo

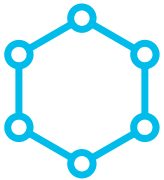
cisco Live!

Extended Detection and Response with Cisco XDR



cisco Live!

What is Extended Detection and Response?



Collection of telemetry from multiple security tools



Application of analytics to the collected and homogenized data to arrive at a detection of maliciousness



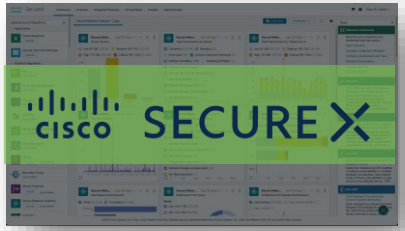
Response and remediation of that maliciousness

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco XDR: A new product offer

Data collection
Analytics
Detection

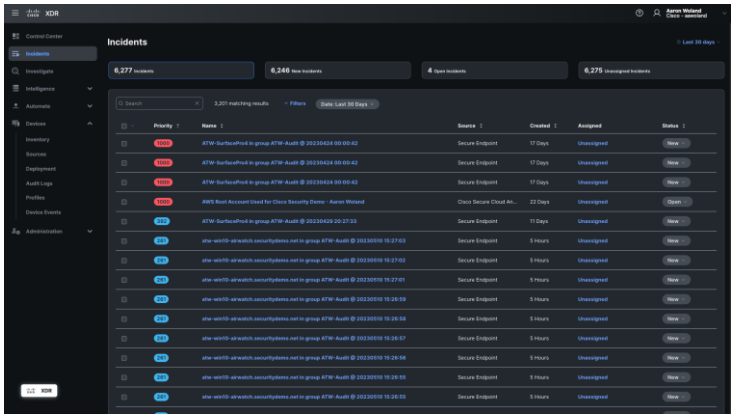




Incident framework
Enrichment
Response

Evolved Into

Cisco XDR



Along with
Significant
Enhancements

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

BRKSEC-2113 – Cisco SecureX XDR: Making sense of the solution and how it's a Security Productivity Tool – Aaron Woland, Friday Dec 8 @ 1:30 pm

Integrations Make XDR Possible

Data Analytics and Correlation

Logs and security events are ingested into the data warehouse and are correlated and analyzed using AI and ML to create actionable *XDR incidents*

Threat Hunting and Investigation

Security information is collected from multiple sources in real time and available for investigation, threat hunting, and enrichment of security incidents

Asset Insights and Context

Consolidated inventory of devices and users across an organization. Understanding the asset value contributes to the prioritization and context available for security incidents

Automation and Response

Provides automated, guided and/or manual actions using a customer's security control points to more rapidly contain and eradicate a security incident.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ETD and XDR Integrations

Data Analytics and Correlation

Logs and security events are ingested into the data warehouse and are correlated and analyzed using AI and ML to create actionable *XDR incidents*



Email Threat Defense

Automation and Response

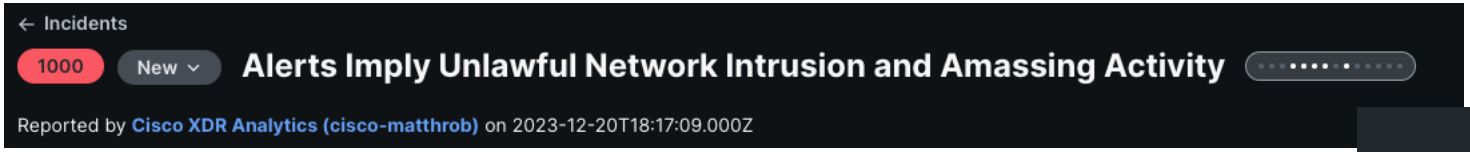
Provides automated, guided and/or manual actions using a customer's security control points to more rapidly contain and eradicate a security incident.

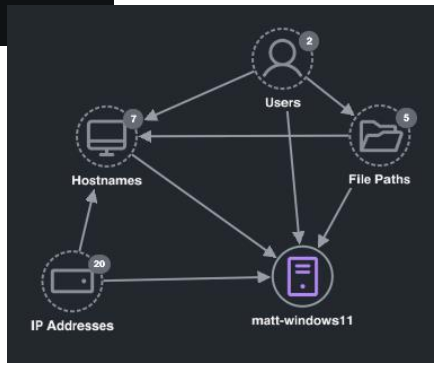
Threat Hunting and Investigation

Security information is collected from multiple sources in real time and available for investigation, threat hunting, and enrichment of security incidents

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extended Detection with XDR





XDR Incident

Correlate data sources together and reconstruct the attack timeline

Email

Network

Endpoint

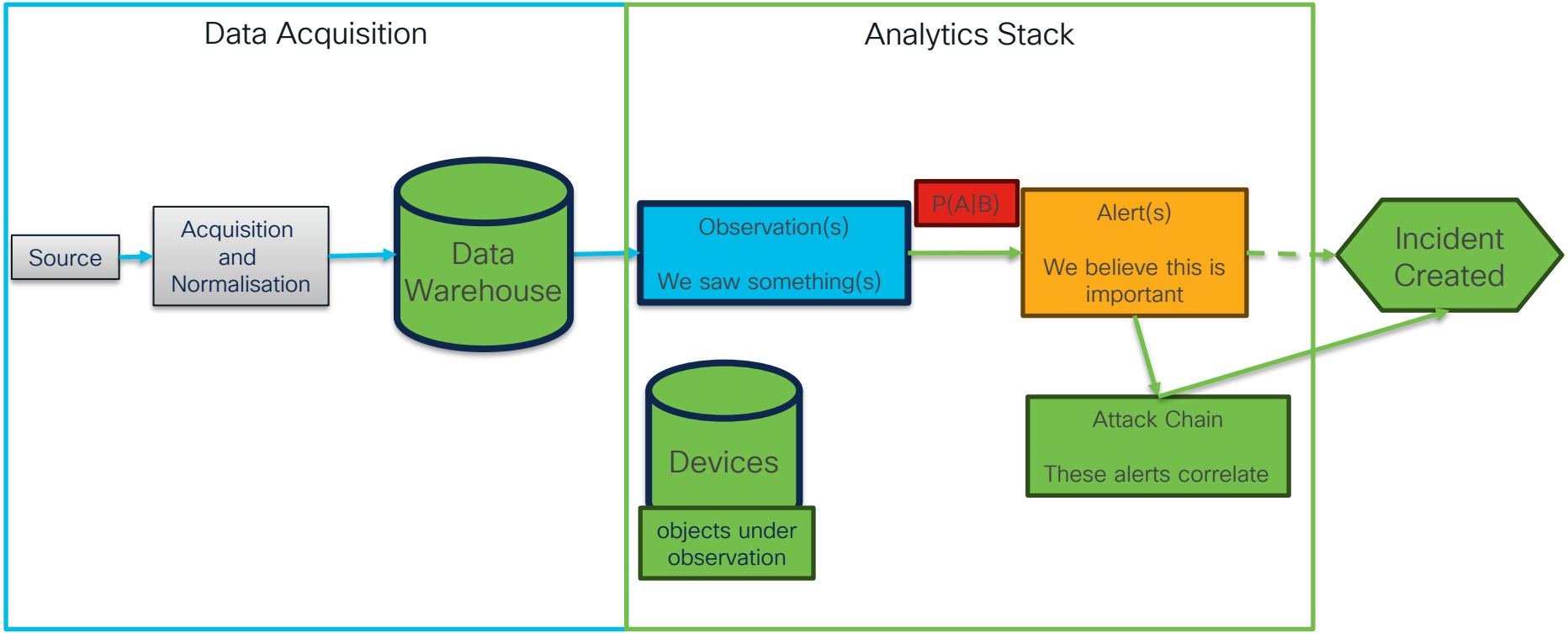
Identity

IaaS

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

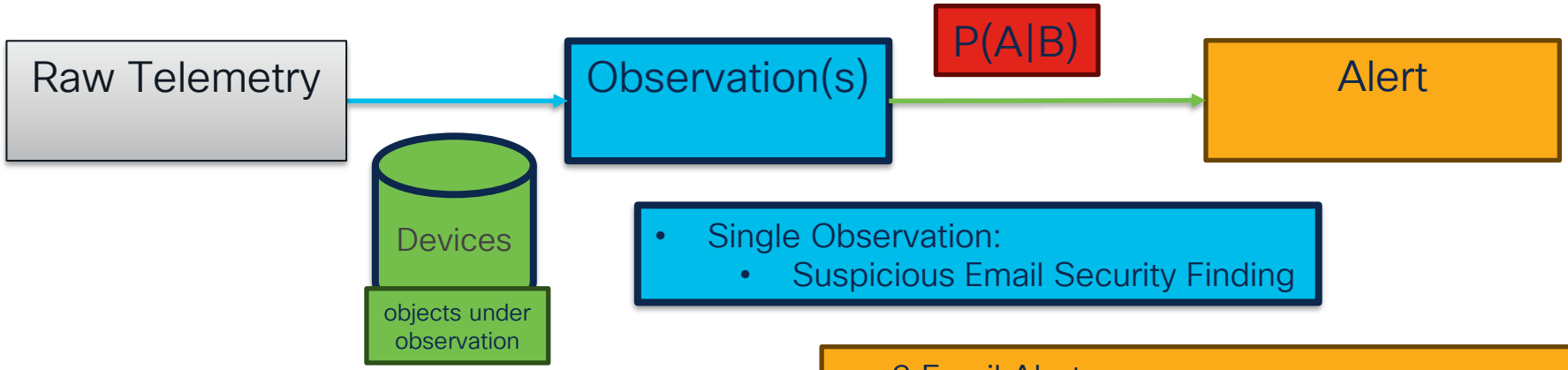
BRKSEC-2178 – Extended Detection with Cisco XDR – Matt Robertson, Thursday Feb 8 @ 4:45 pm

XDR Analytics Pipeline



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ETD Data Analytics Pipeline



- Call API every 30 minutes
- Ingest Emails with = verdict
- Normalize and store data
- Associate to user/device (where possible)

- 2 Email Alerts
  - Suspicious Email findings by Initial Access
  - Suspicious Email Findings by Resource Development
- Contain source observations
- Assigned to user/device
- Correlated into Attack Chains

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

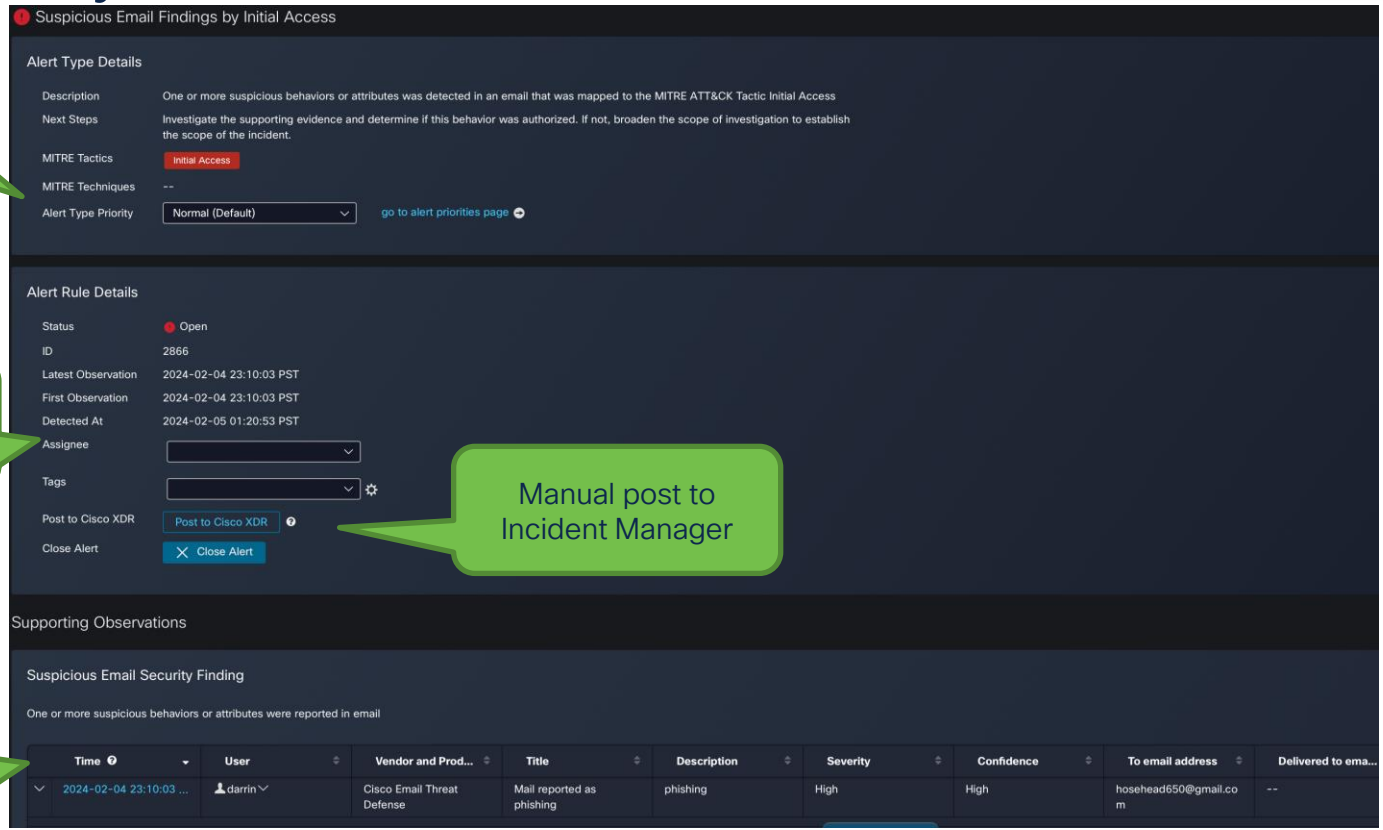
XDR Analytics Alert

New alerts are frequently published into production

Alert Type Details

Alert Occurrence Details

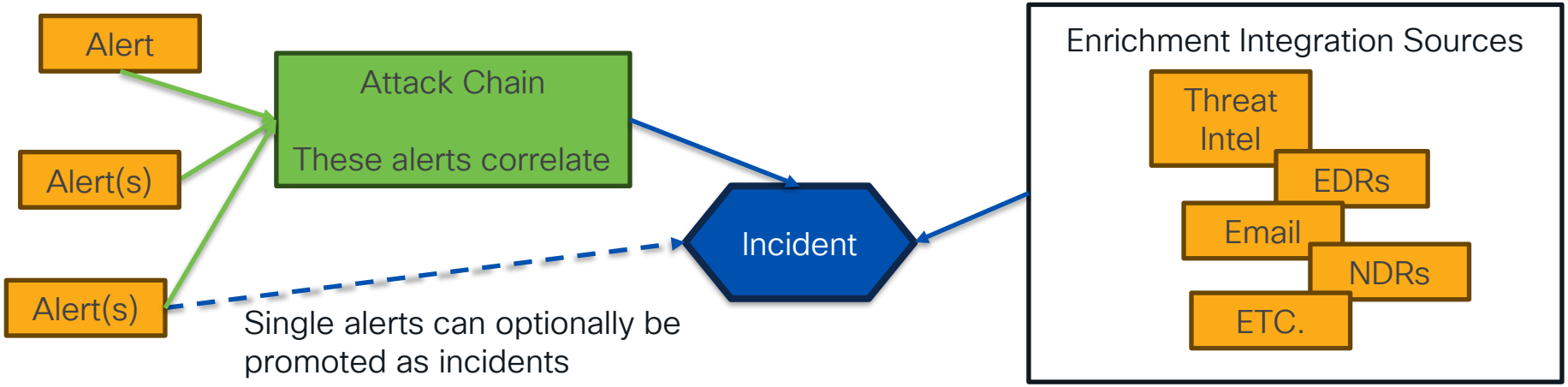
Supporting Observations



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Important note:
Some XDR Analytics alerts contain data from multiple tools!

Extending a Detection



Correlation (pre-incident creation):

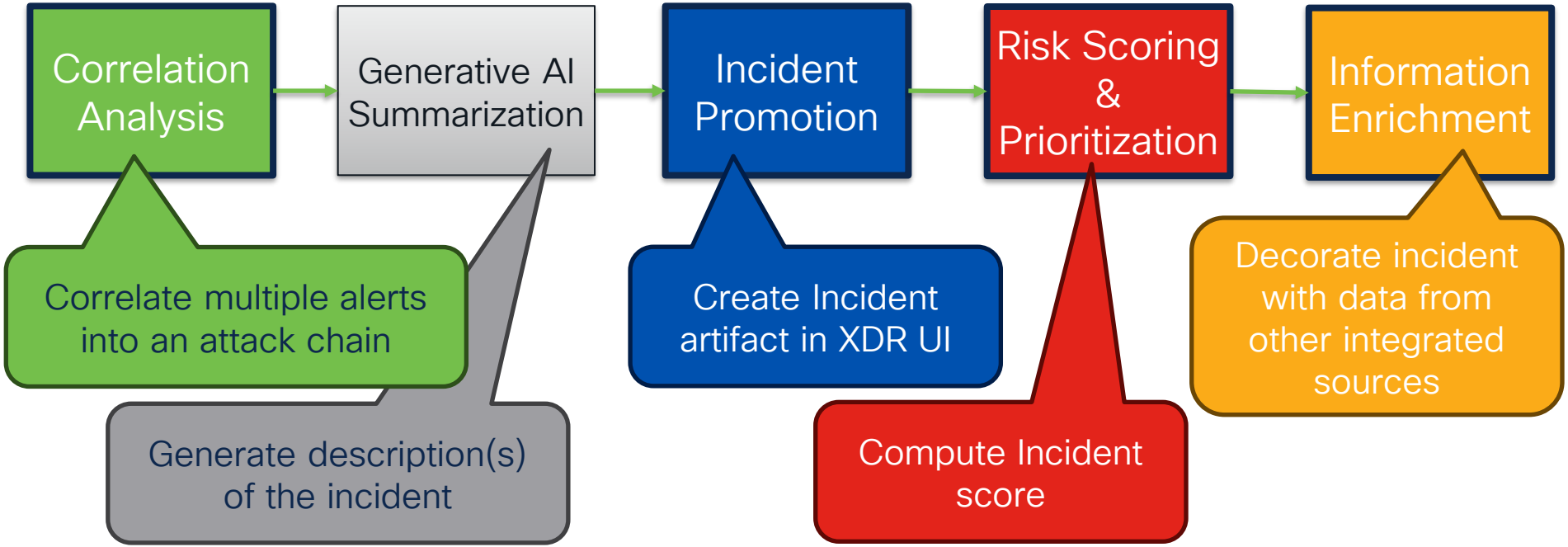
Data from multiple security tools is analysed to arrive at a detection of maliciousness

Enrichment (post-incident creation):

A detection of maliciousness is decorated with data from integrated security tools.

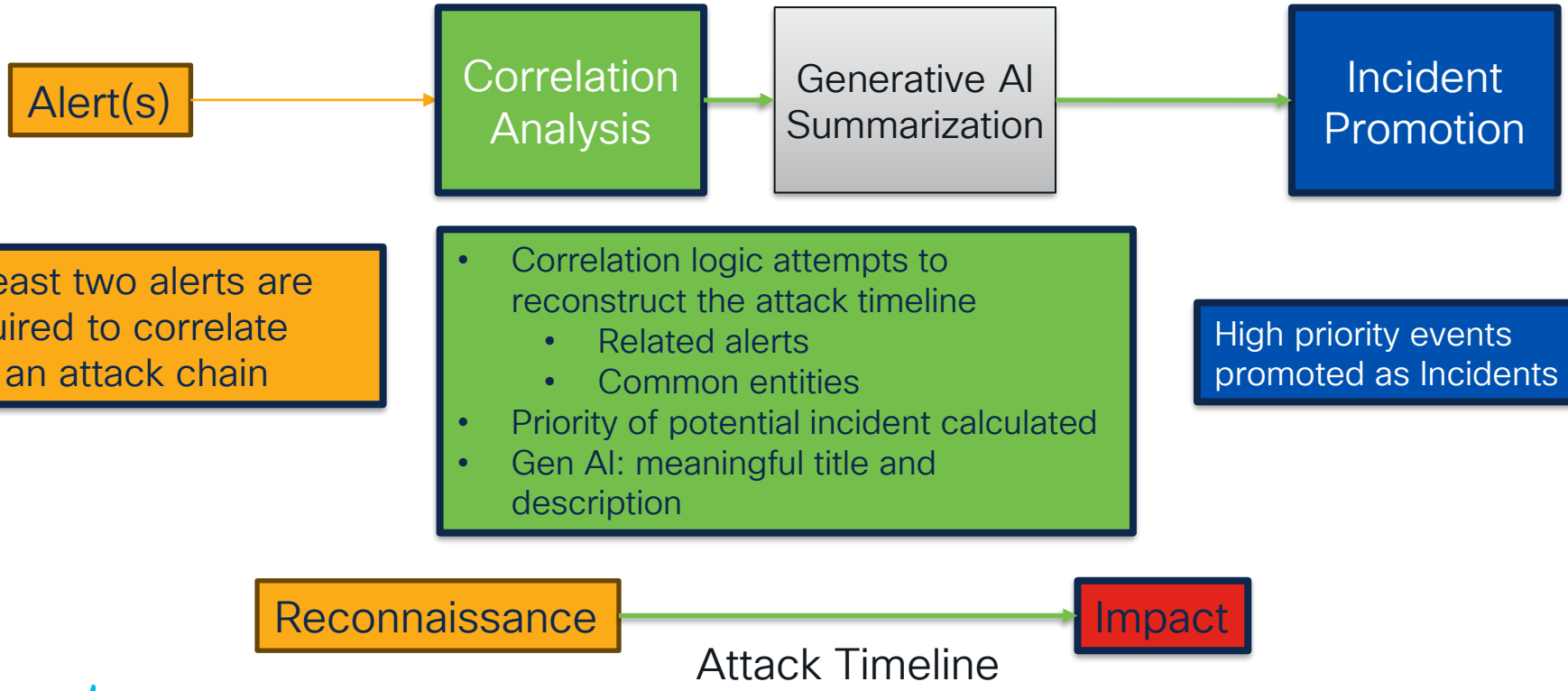
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Correlated Incident Generation



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

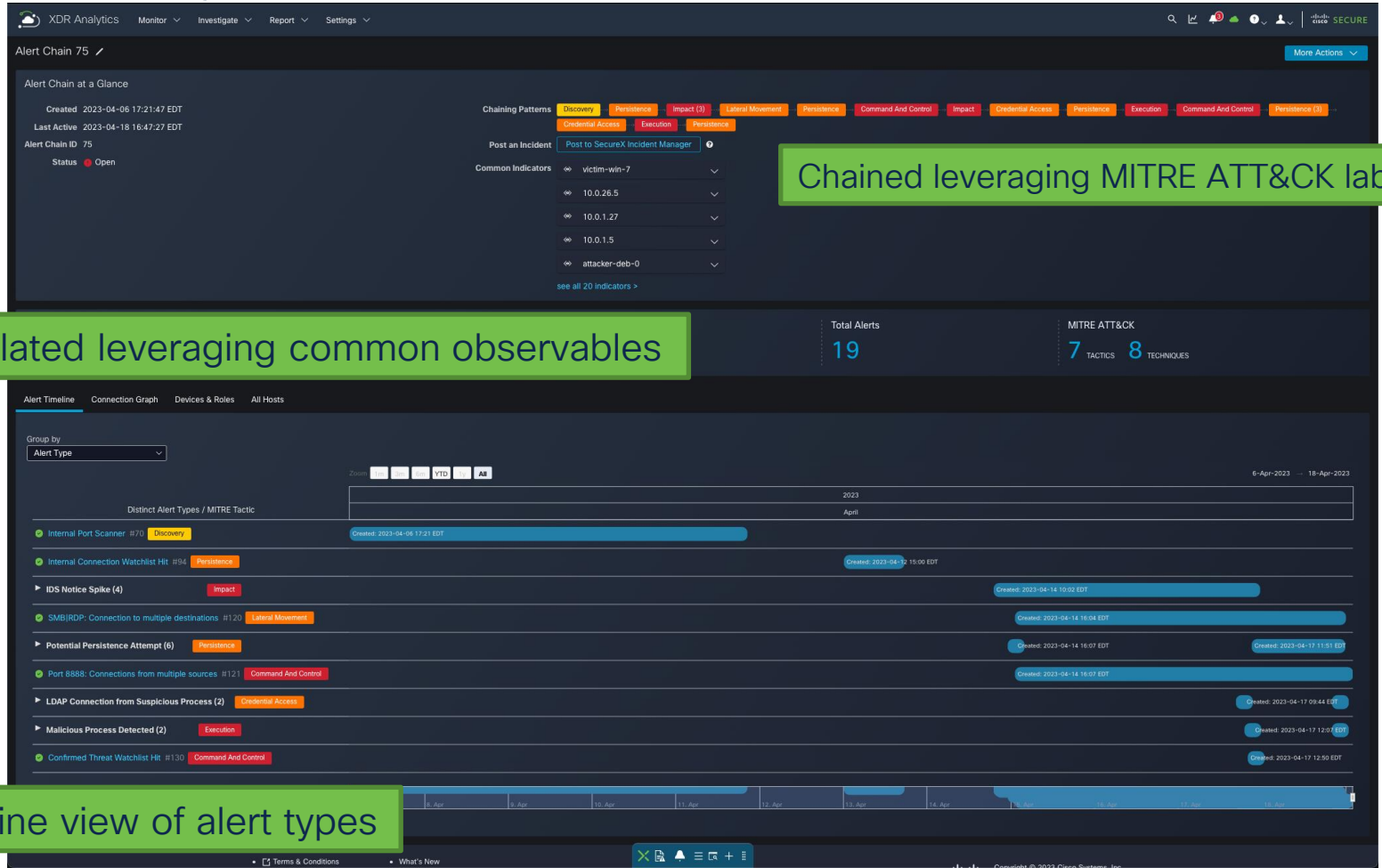
Correlation Analysis: Attack Chains



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

XDR Analytics: Attack Chain

Automatic correlation of related alerts

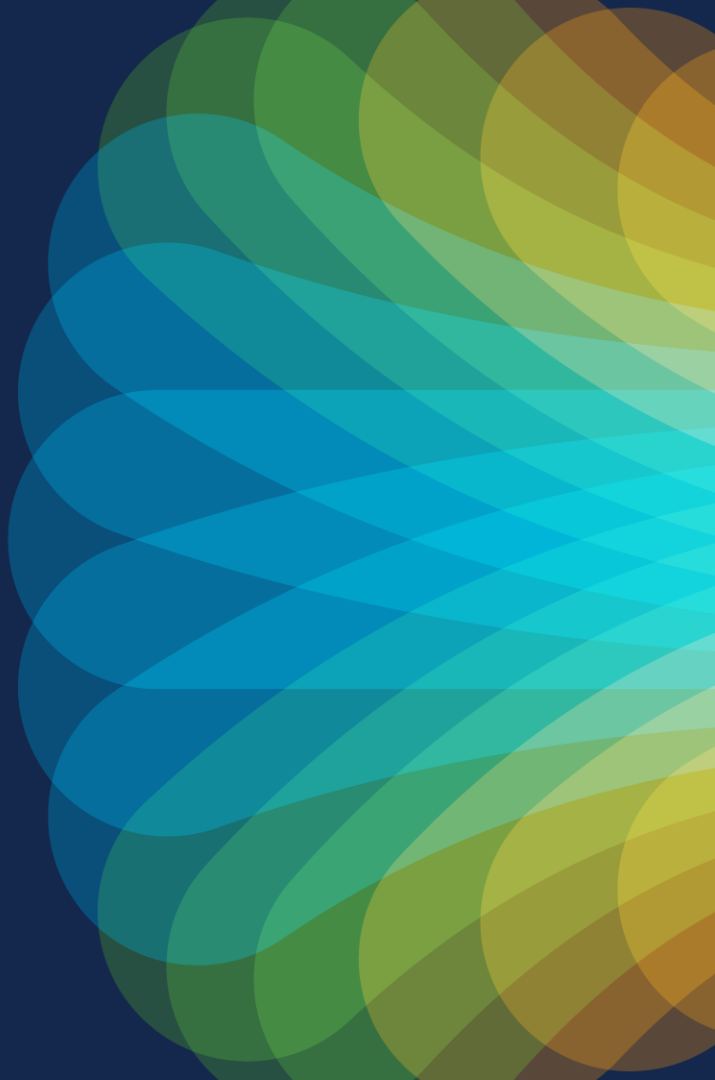


Chained leveraging MITRE ATT&CK labels

Correlated leveraging common observables

Timeline view of alert types

XDR Demo

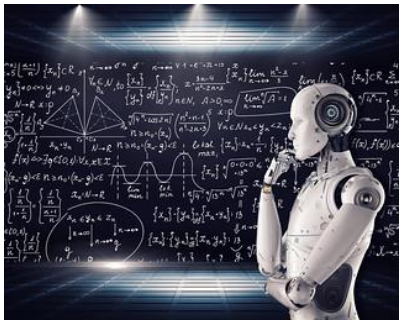


Summary

Do NOT take Email Security lightly

After all, it is #1 threat vector





As attackers are using more advanced techniques, anomalous behavior can be detected using AI/ML based engines.

Targeted attacks are harder to detect with systems that are solely based on global threat feed intelligence.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Email Threat Defense

Adding AI/ML-based detection to your email scanning





Using vast AI/ML based libraries and Cisco developed models, we can detect very advanced attacks. This way end users are not put to vulnerable spot and organization can stay safer.

Using Cisco XDR, automation and incident handling will be more effective and simplified.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

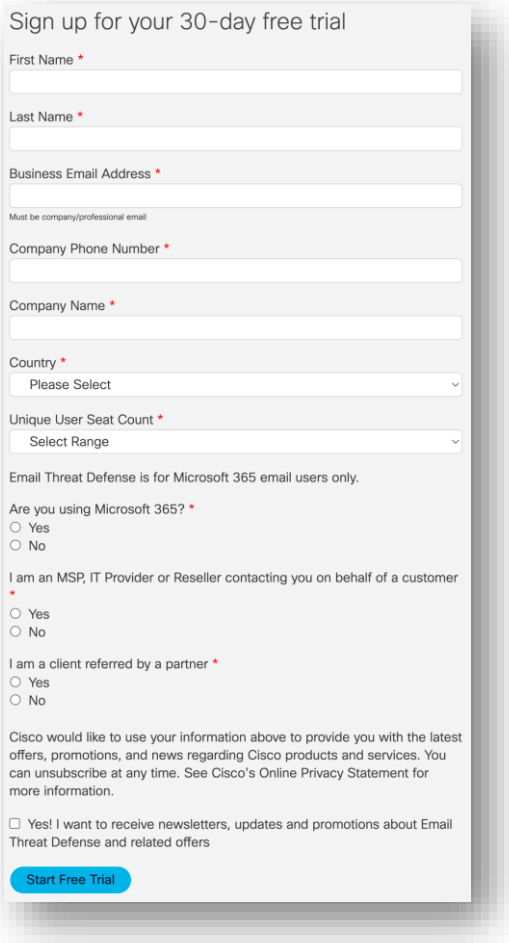
Get to know with ETD

Free Trial:

https://www.cisco.com/c/en/us/products/security/email-threat-defense-free-trial.html






Sign up for your 30-day free trial

First Name *

Last Name *

Business Email Address *

Must be company/professional email

Company Phone Number *

Company Name *

Country *

Please Select

Unique User Seat Count *

Select Range

Email Threat Defense is for Microsoft 365 email users only.

Are you using Microsoft 365? *

Yes

No

I am an MSP, IT Provider or Reseller contacting you on behalf of a customer *

Yes

No

I am a client referred by a partner *

Yes

No

Cisco would like to use your information above to provide you with the latest offers, promotions, and news regarding Cisco products and services. You can unsubscribe at any time. See Cisco's Online Privacy Statement for more information.

Yes! I want to receive newsletters, updates and promotions about Email Threat Defense and related offers

Start Free Trial

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Related Sessions

Session ID	Title	When
BRKSEC-2113	Cisco XDR – Making sense of the Solution and how it's a Security Productivity Tool	Wed 10:30 AM
BRKSEC-2178	Extended Detection with Cisco XDR: Security Analytics across the enterprise	Thursday 4:45 PM
BRKSEC-2227	Evaluating and Improving Defenses with MITRE ATT&CK	Thursday 4:30 PM
BRKSEC-2913	Why Cisco Secure Email if You Have Microsoft 365	Friday 9:00 AM

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Parting Thoughts

Email: The number one threat vector







Please rate my session!

Absolutely! It was Excellent!

Sophisticated threat actors can be detected!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go