Cisco Secure Email Threat Defense

Elektroniskā pasta komunikācijas kanāla aizsardzība

Mārtiņš Zeipe

E-pasts joprojām ir galvenais #1 uzbrukumu vektors

AI - mākslīgā intelekta vadīti uzbrukumi, kas apiet tradicionālās aizsardzības.

Tieši tāpēc nepieciešama AI analīze, kas saprot e-pasta kontekstu, nevis tikai pārbauda pielikumu vai URL.

E-pasta draudu attīstība

Evolūcija

Liela apjoma uzbrukumi

Spam

Vīrusi

Inficētas tīmekļa vietnes

IP reputācija

Antivīruss

SPF / DKIM / DMARC

Heiristiskā (Heuristic) analīze

Mākslīgais intelekts un izvairīšanās

MI ģenerēti e-pasti

QR kodu uzbrukumi

HTML Smuggling

Lietotāju identitātes viltošana

Business Email Compromise

Komunikācijas attiecību modelēšana

OCR

Lielie valodu modeļi (LLM)

Agrīnie 2000. gadi | 2010-2020 | Mūsdienās

Maldināšanas tehnikas un izspiedējvīrusi

Pikšķerēšana

Lietotāju identitātes viltošana

Business Email Compromise

URL analīze

Dinamiskā failu analīze

Dabīgās valodas apstrāde (NLP)

Signālu korelācija

Cisco Secure Email Threat Defense

Vienota mākoņplatforma e-pasta drošībai

Mākslīgā intelekta atbalstīta draudu izvērtēšana

Automātiska un kontekstu balstīta e-pastu analīze, izmantojot mākslīgo intelektu.

Pilnīga pārskatāmība

Visu ienākošo un izejošo e-pasta plūsmu uzraudzība vienā konsolē.

Vietējās integrācijas

Integrācija ar Cisco XDR, Secure Access, Microsoft, Splunk un citām drošības platformām.

Elastīga ieviešana

Iespēja izvēlēties organizācijai piemērotāko ieviešanas modeli.

Vienkāršota

MI nodrošināta uzlabota draudu aizsardzība

Proaktīva apdraudējumu meklēšana

MI, mašīnmācīšanās un dabīgās valodas apstrāde palīdz identificēt sarežģītus uzbrukumus.

Automatizācija

Integrācija XDR procesos paātrina reakciju uz incidentiem.

Plaša pārskatāmība

Cisco Talos draudu izlūkošana nodrošina globālu redzamību.

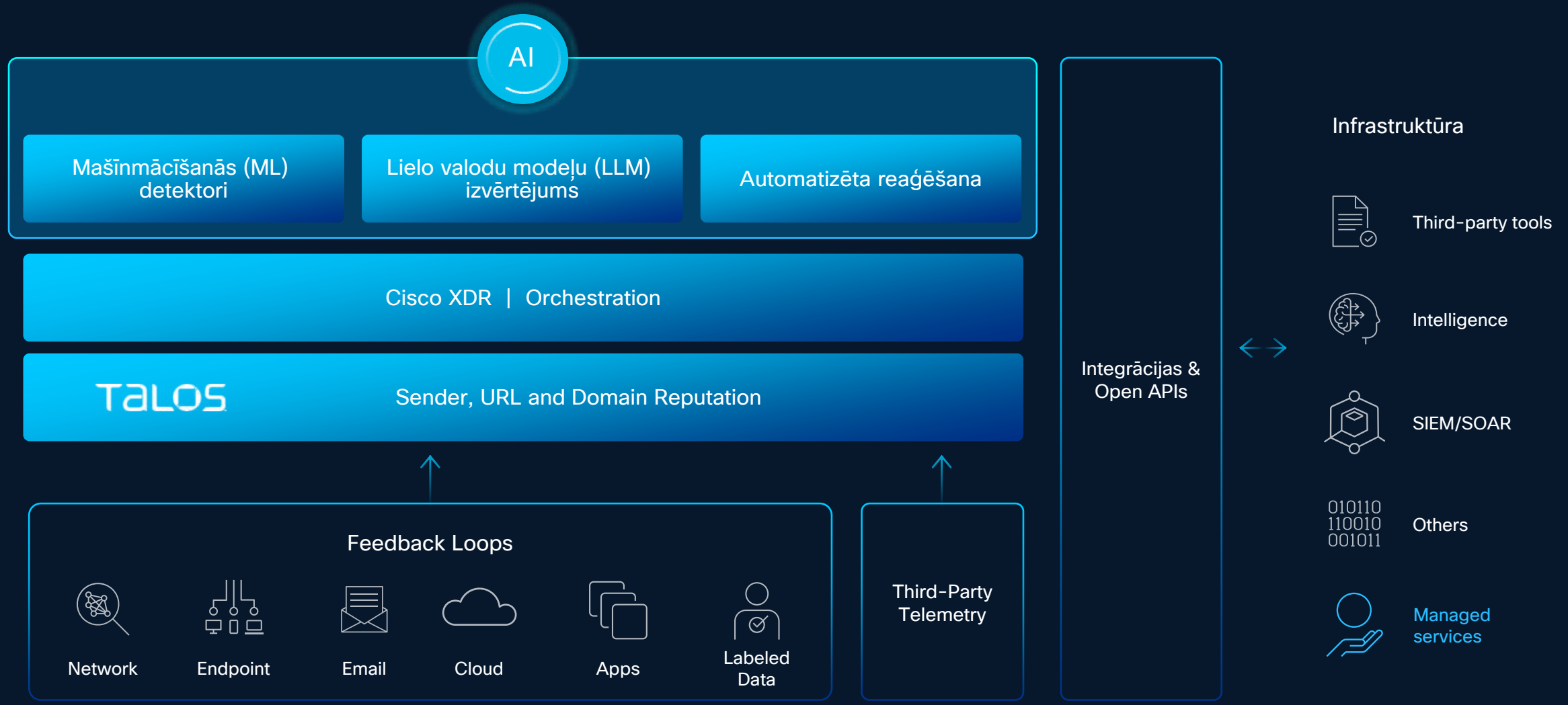
Esošo drošības risinājumu papildināšana

Papildina Microsoft 365, Google Workspace un tradicionālos e-pasta drošības risinājumus.

Konteksts un efektivitāte, kas dod jūsu uzņēmumam pārliecību rīkoties ātri.

AI viens pats par sevi nav risinājums – Svarīga ir MI, telemetrijas, reputācijas datu un cilvēku analīzes kombinācija.

Visaptveroša draudu noteikšanas arhitektūra



Visaptveroša e-pasta aizsardzība

Cisco Secure Email Threat Defense nodrošina daudzslāņu aizsardzību pret mūsdienu e-pasta draudiem.

Cisco Email Threat Defense

Secure Email Gateway

+

Cloud Integrated Email Security

Vienota administrēšanas vide

MI balstīta aizsardzība

Vienkārša pārvaldība

Cisco Secure Email Threat Defense apvieno tradicionālās e-pasta drošības funkcijas un modernas mākoņtehnoloģijas vienotā platformā.

Email Threat Defense

E-pasta drošības modernizācija vienuviet

Architecture

Arhitektūra

Enrichment

Draudu bagātināšana

Enablement

Drošības iespēju paplašināšana

Scalable Cloud Infrasturcture:

Mākonī balstīta SaaS platforma
Privātuma un datu aizsardzības princips (Privacy First)
Datu rezidences prasību atbalsts
Vienkārša ieviešana un pārvaldība

Detecting Digital Footprints of Attacks:

Dabīgās valodas apstrāde (NLP)Cisco Talos draudu izlūkošanaLietotāju komunikācijas analīze (User Graph)URL un ļaunprogrammatūras analīze

Searchable Intelligence:

Reāllaika indeksēšanaPolitiku piemērošanaAPI piekļuve un forensiskā analīzeIntegrācija ar XDR un citām drošības platformām

Vienkārša un elastīga ieviešana

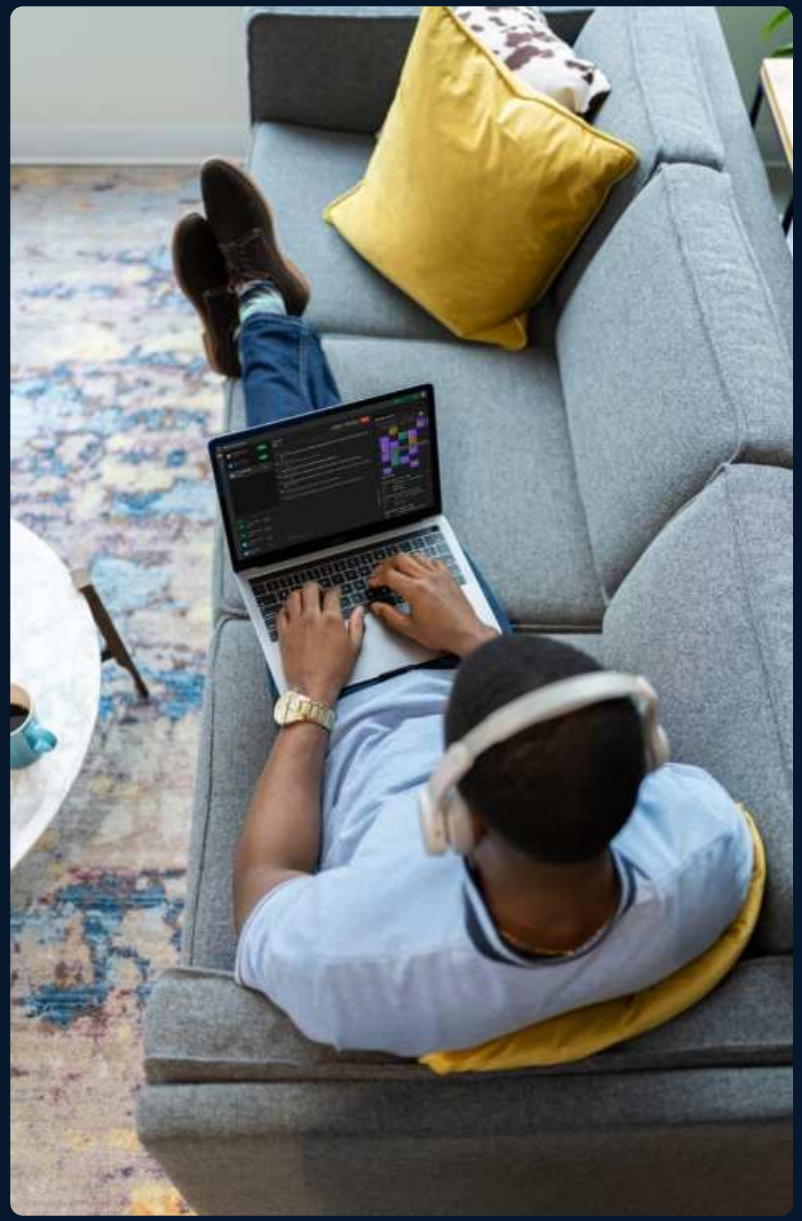
Journal or Connector

- Ātra ieviešana
- Nav jāmaina e-pasta plūsma
- Darbojas ar Microsoft 365 un Cisco Email Security Appliance
- Darbības tiek veiktas caur API
- Vienkārša sākotnējā konfigurācija

Inline

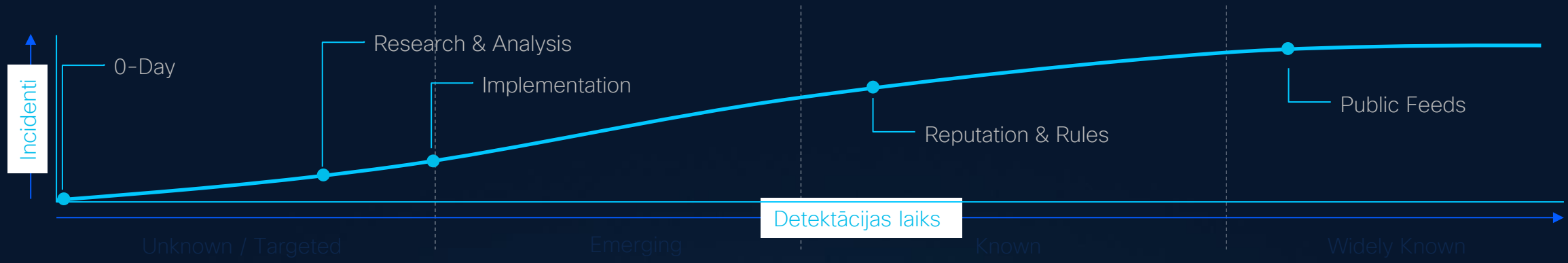
- Pilnīga ienākošā un izejošā e-pasta kontrole
- Draudu bloķēšana pirms e-pasta piegādes lietotājam
- Savienojumu līmeņa kontrole
- Elastīga maršrutēšana pēc domēniem
- Savietojams ar jebkuru SMTP pakalpojumu

Prasība: nepieciešama e-pasta maršrutēšanas izmaiņa.



Aizsardzība pret visu moderno e-pasta draudu spektru

Cisco Secure Email Threat Defense izmanto daudzslāņu analīzi, lai atklātu gan zināmus, gan iepriekš neredzētus e-pasta draudus.



Unknown / Targeted	Emerging	Known	Widely Known
Relationship Models	Malware Analytics	Sender IP Reputation	Public Threat Feeds / VirusTotal
Natural Language Understanding	Cloud URL Analysis	Domain Reputation	STIX/TAXII Subscriptions
Phishing Models	Algorithm Matching	Web Reputation, Category	
BEC Models		File Reputation	
		Sender Authentication (DMARC, SPF)	
		Anti-Spam & Graymail	
		Anti-Virus	

Dabiskā izpratne un mašīnmācīšanās

Cisco sūtītāja reputācija, URL reputācija
Cisco surogātpasta novēršana, Talos vienotais spriedumu pakalpojums (TUVS)

skatāmies uz 2026. gada tendencēm, svarīgākie ir:

- 🤖 AI ģenerēts phishing
- 🎭 AI balss (vishing) kopā ar e-pastu
- 💰 Business Email Compromise (BEC)
- 📱 QR phishing (Quishing)
- 🔗 OAuth Consent phishing (viltotas Microsoft/Google aplikāciju piekļuves)
- ☁️ Cloud phishing (Microsoft 365, Google Workspace)
- 🧵 Thread hijacking
- 📄 SVG un HTML pielikumi
- 📦 Password-protected ZIP/RAR/7z pielikumi
- 📱 MFA fatigue un MFA bypass uzbrukumi
- 🔑 Session cookie theft (Adversary-in-the-Middle)
- 🎯 Deepfake vadītāju uzbrukumi (CEO Fraud 2.0)

Tavai kiberdrošības prezentācijai es ieteiktu ne tikai uzskaitīt draudus, bet sagrupēt tos **4 lielās kategorijās** kas auditorijai ir vieglāk uztveramas:

1. **Sociālā inženierija**
    1. Phishing
    2. Spear Phishing
    3. Whaling
    4. BEC
    5. AI phishing
2. **Identitātes viltošana**
    1. Spoofing
    2. Display Name Spoofing
    3. Thread Hijacking
3. **Tehniskie uzbrukumi**
    1. Malware pielikumi
    2. Kaitīgas saites
    3. QR phishing
    4. OAuth phishing
4. **Konta pārņemšana**
    1. Account Takeover
    2. Session hijacking
    3. MFA bypass

Daudzslāņu draudu noteikšana, izmantojot mašīnmācīšanos

Dziļa satura un konteksta analīze, izmantojot ML un NLP

Komunikācijas un attiecību uzvedības izpēte

Atklāj gan zināmus, gan iepriekš neredzētus draudus

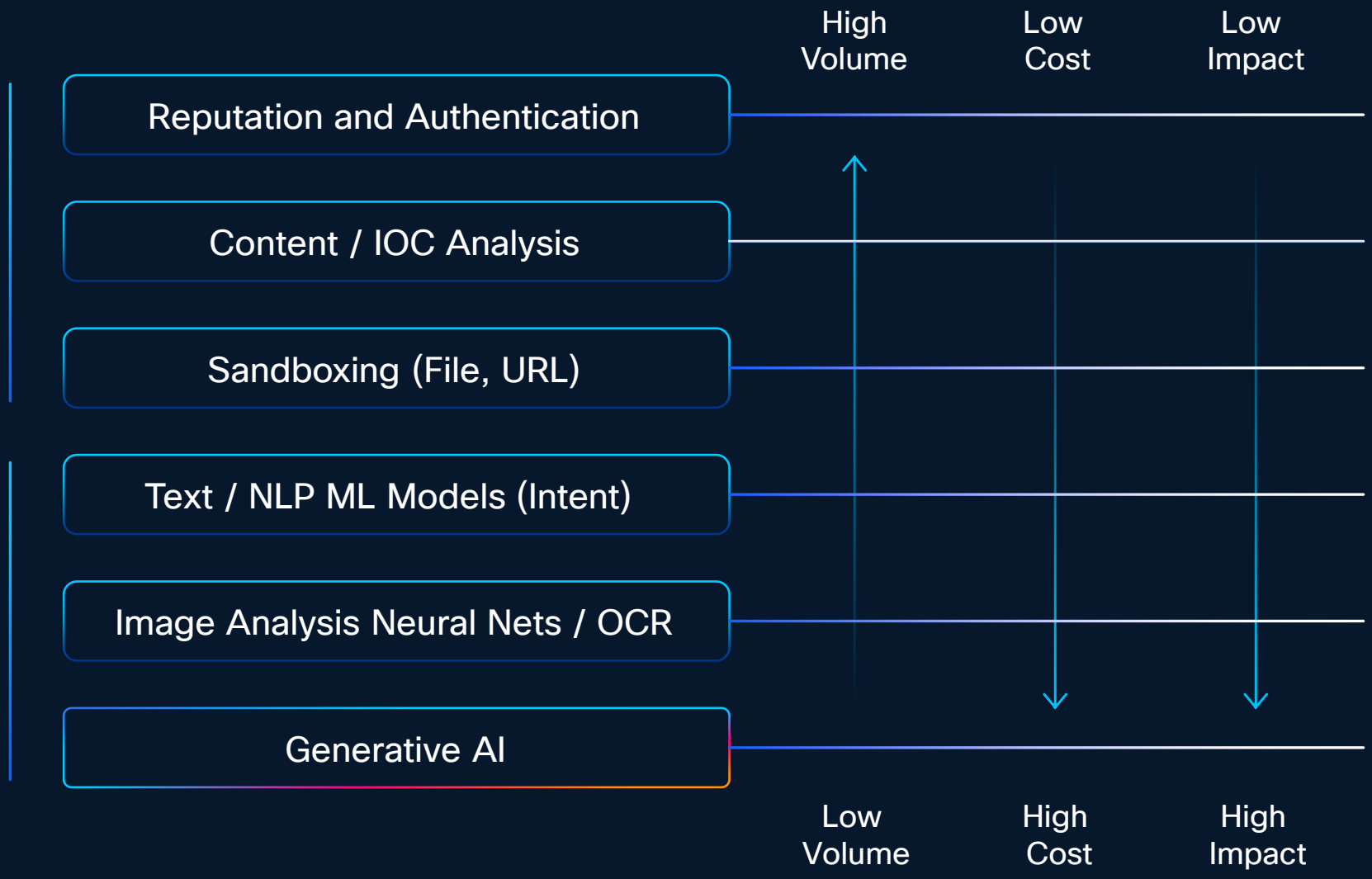
Augsta precizitāte pret BEC, phishing un citām uzbrukumu tehnikām

Modern Threats

AI atbalstīta e-pasta draudu noteikšana

Tradicionālās e-pasta drošības metodes

AI vadīta draudu noteikšana



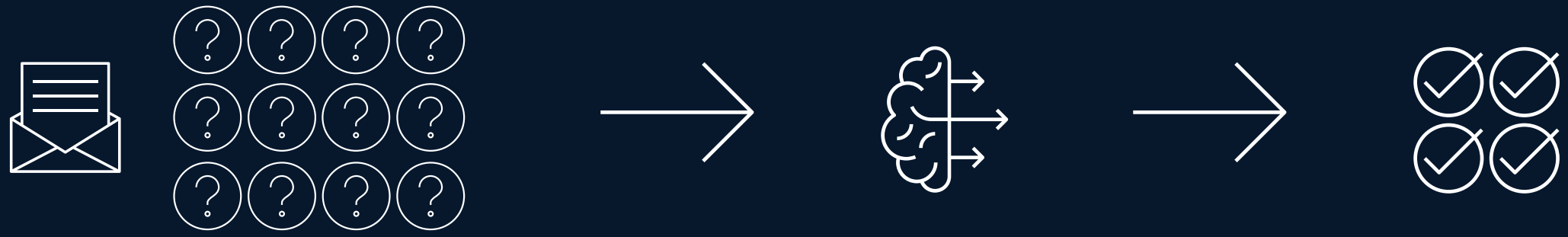
Moderni draudi

Datu analītika un signālu analīze

Katrs e-pasts tiek analizēts, izmantojot daudzus neatkarīgus signālus

Moderni draudi

Datu analītika un signālu analīze



Galīgais drošības spriedums tiek pieņemts, apvienojot visu neatkarīgo signālu rezultātus.

Moderni draudi

Datu analītika un signālu analīze

Saturs & Konteksts

Content-based analizē **konkrēto** e-pasta ziņojumu

Context-based analizē attiecības starp iesaistītajām pusēm

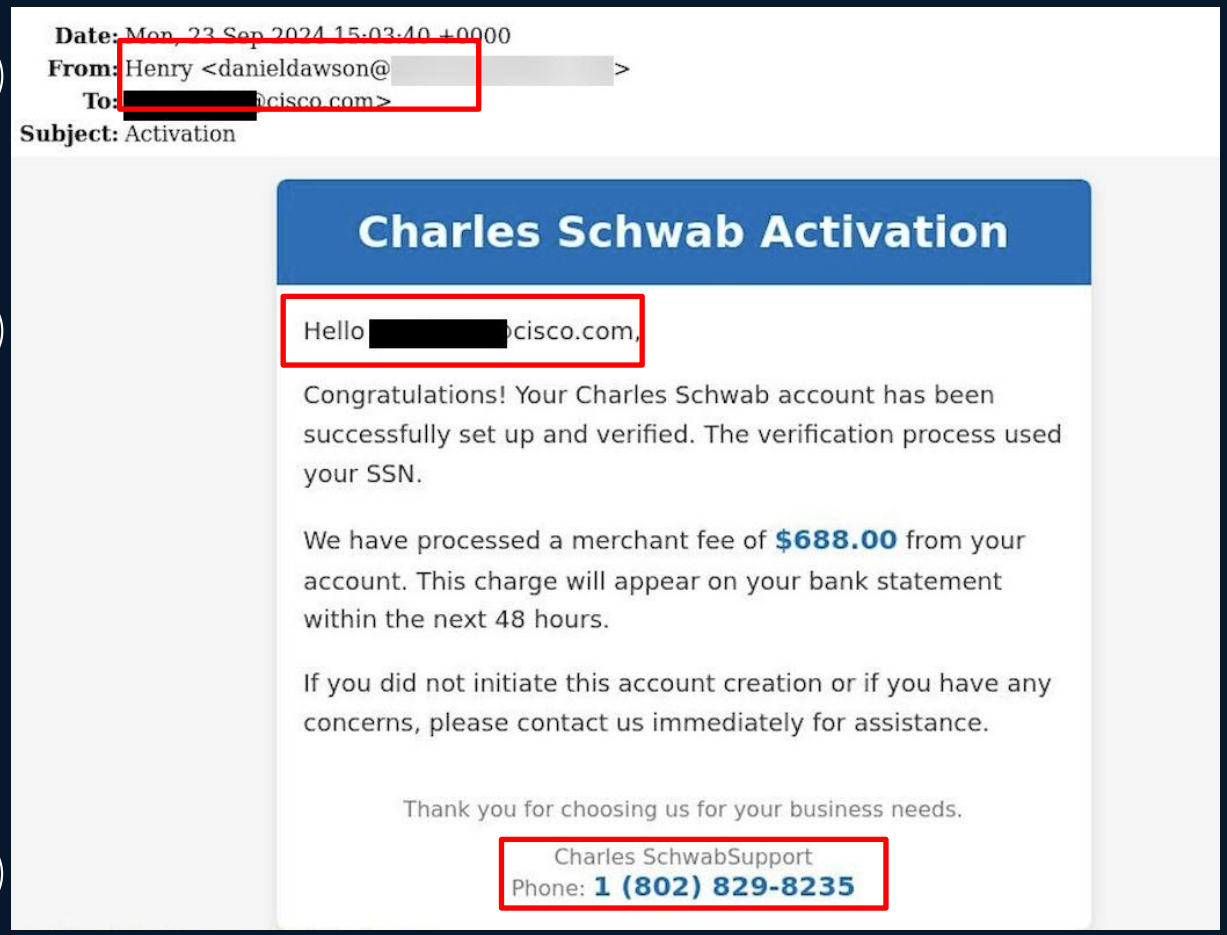
Moderni draudi

Zīmola imitācija (Brand Impersonation)

Sūtītāja vārda neatbilstība

Sveiciens, izmantojot tikai lietotājvārdu

Kontakta pieprasījums



Saņēmējam neraksturīgs sūtītāja domēns

Tiek imitēts Charles Schwab zīmols

Temats saistīts ar finanšu jautājumiem

Ja šajā e-pastā nebūtu neviena ļaunprātīga pielikuma un nevienas kaitīgas saites, vai tradicionāls e-pasta filtrs to noteikti bloķētu?

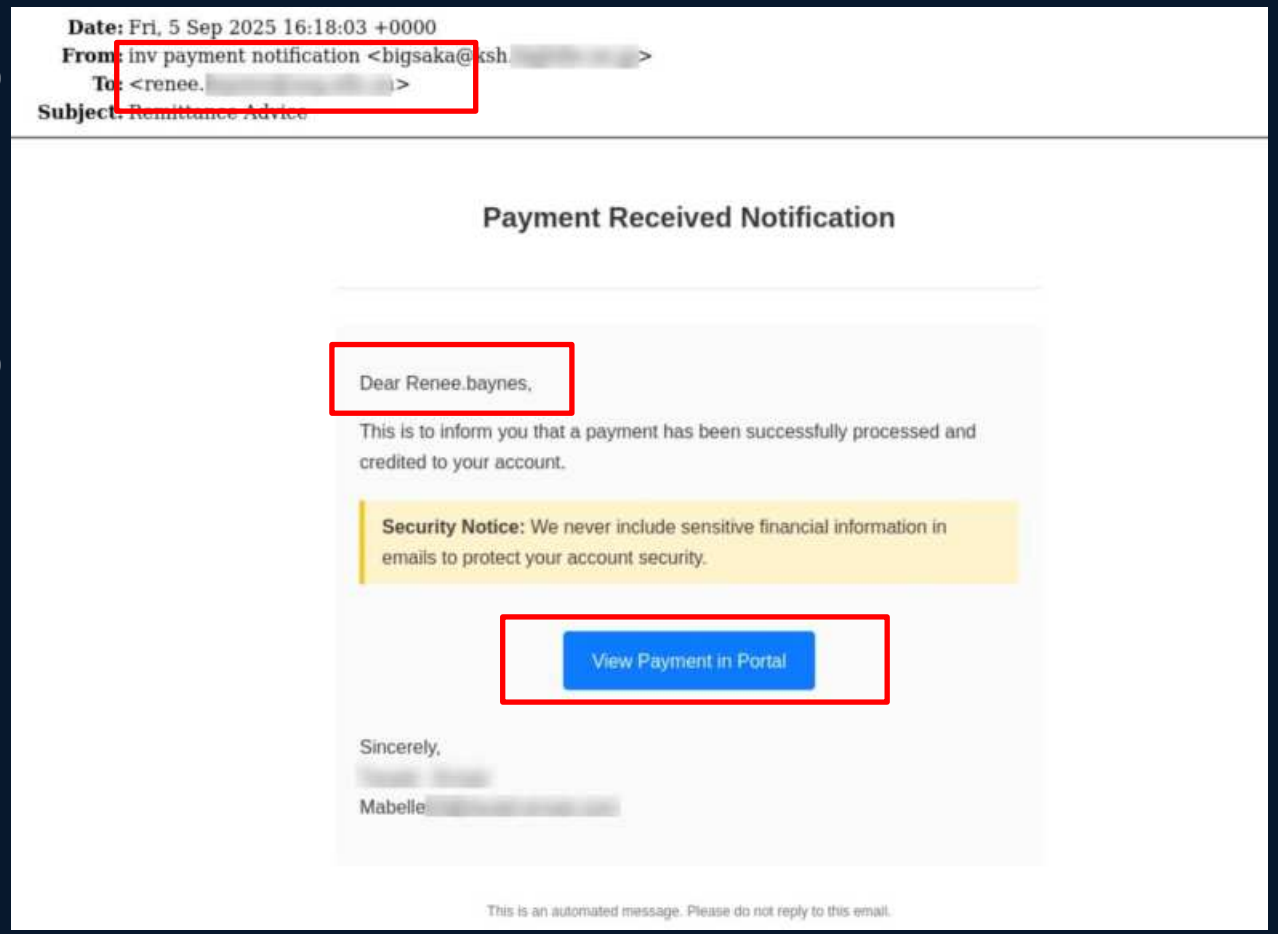
Moderni draudi

Zīmola imitācija (Brand Impersonation)

Sūtītāja vārda neatbilstība

Sveiciens, izmantojot tikai lietotājvārdu

Saņēmējam unikāla (personalizēta) saite



Saņēmējam neraksturīga sūtītāja adrese

Aicinājums veikt darbību

Temats saistīts ar finanšu jautājumiem

Moderni draudi

levilināšanas / pievilināšanas tehnika

Aicinājums rīkoties | Vienreizlietojama e-pasta adrese | Lietotāja identitātes imitācija | Rets sūtītājs konkrētajam saņēmējam

Datums: Pirmd., 19. maijs 2026 14:32:47 +0300

No: Jānis Kalniņš <janis.kalnins01@latbiznespartneri.lv>

Kam: ealvarez1@uznemums.lv

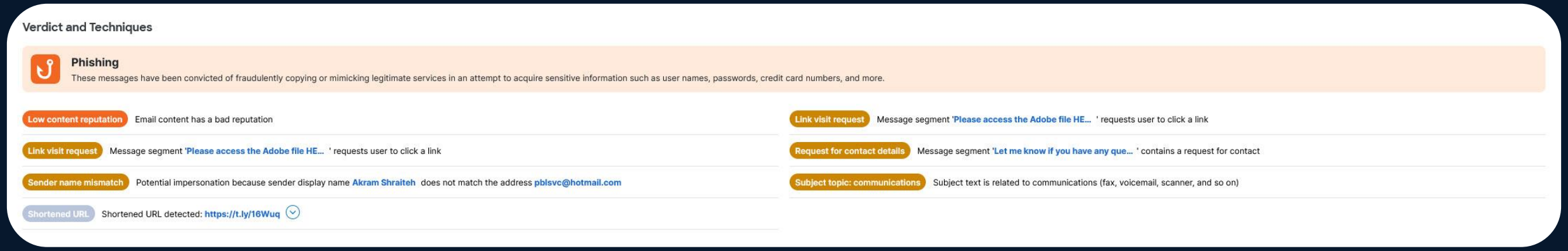
Temats: [ĀRĒJS]

Iedod man mobilo tālruņa numuru, uz kuru varu ar tevi sazināties, rakstot SMS. Kāds ir tavs tālruņa numurs.

Draudu tehnikas

Uzvedības analīze

Kā uzvedības analīze uzlabo detekcijas efektivitāti



Adaptīvs

Atpazīst nepārtraukti mainīgās uzbrukumu tehnikas.

Izskaidrojams

Parāda, kādi indikatori izraisīja drauda noteikšanu.

Rīcībspējīgs

Sniedz konkrētus riska iemeslus, lai drošības komanda varētu ātri pieņemt lēmumu.

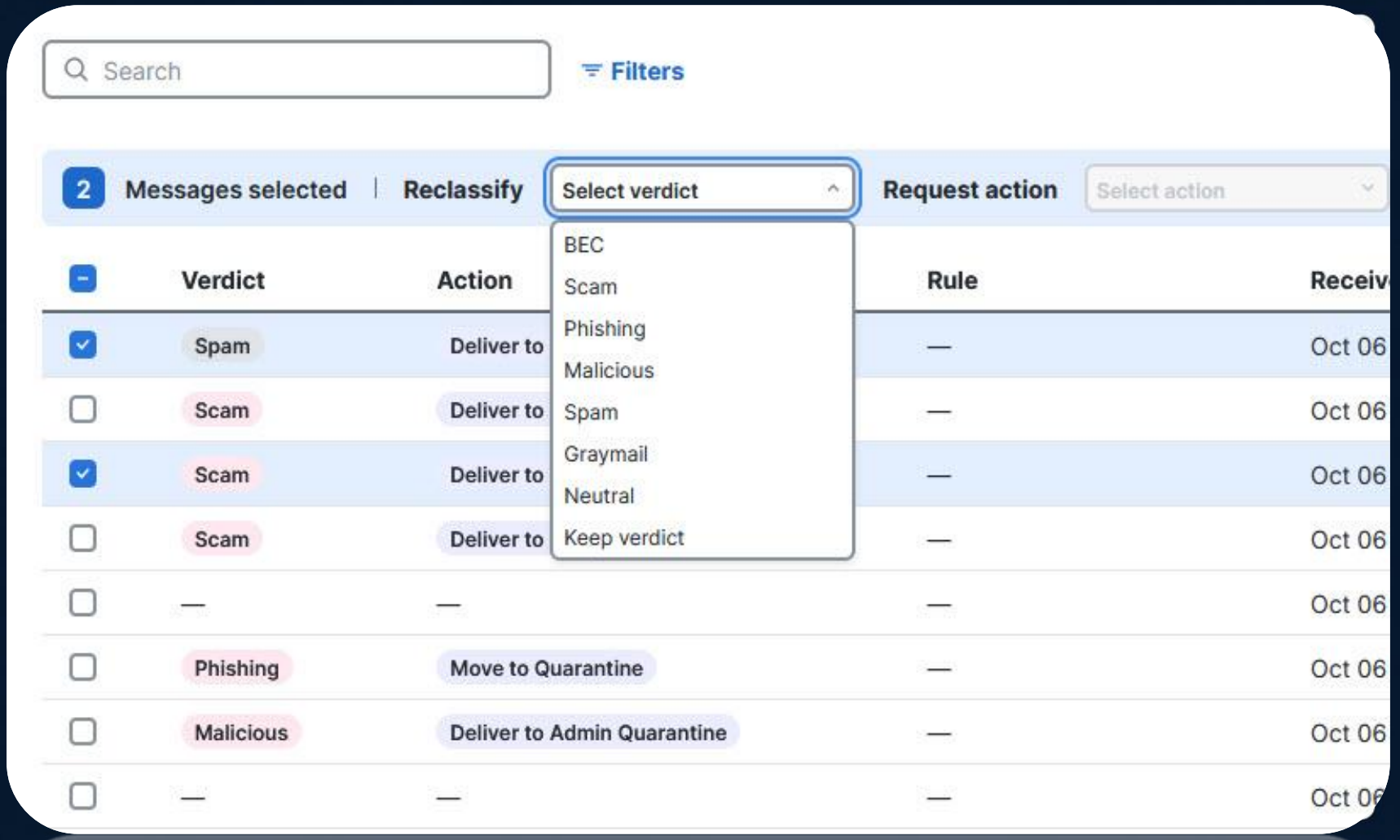
Modernie draudi

Datu marķēšana un pielāgošanās videi

Datu pārkategorizēšana sniedz **reālus darba vides datus**, kas atspoguļo katra klienta unikālo darbības un draudu kontekstu

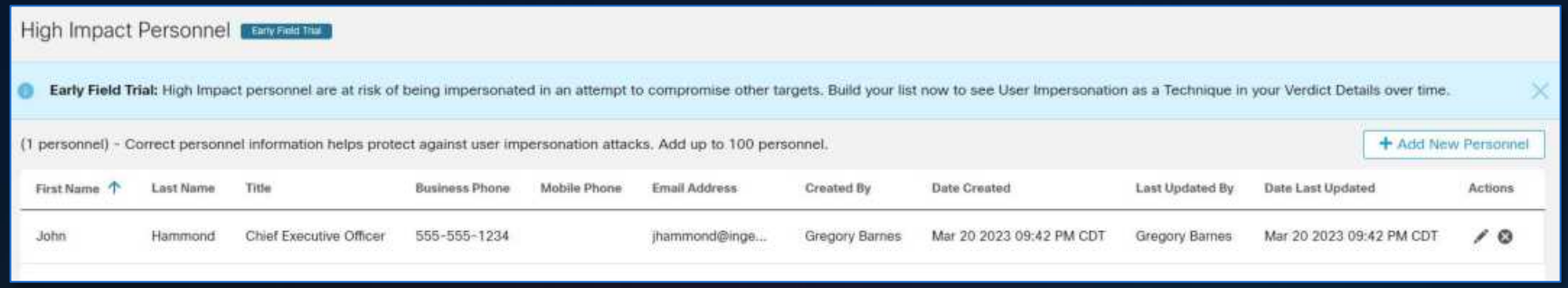
---

Datu zinātne identificē līdzīgus ziņojumus, lai nodrošinātu ātru reakciju uz **jauniem draudiem** un **mainīgām uzbrukumu** tehnikām

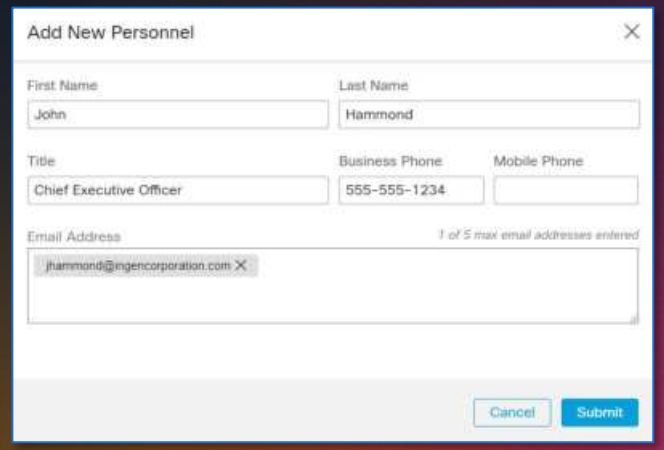


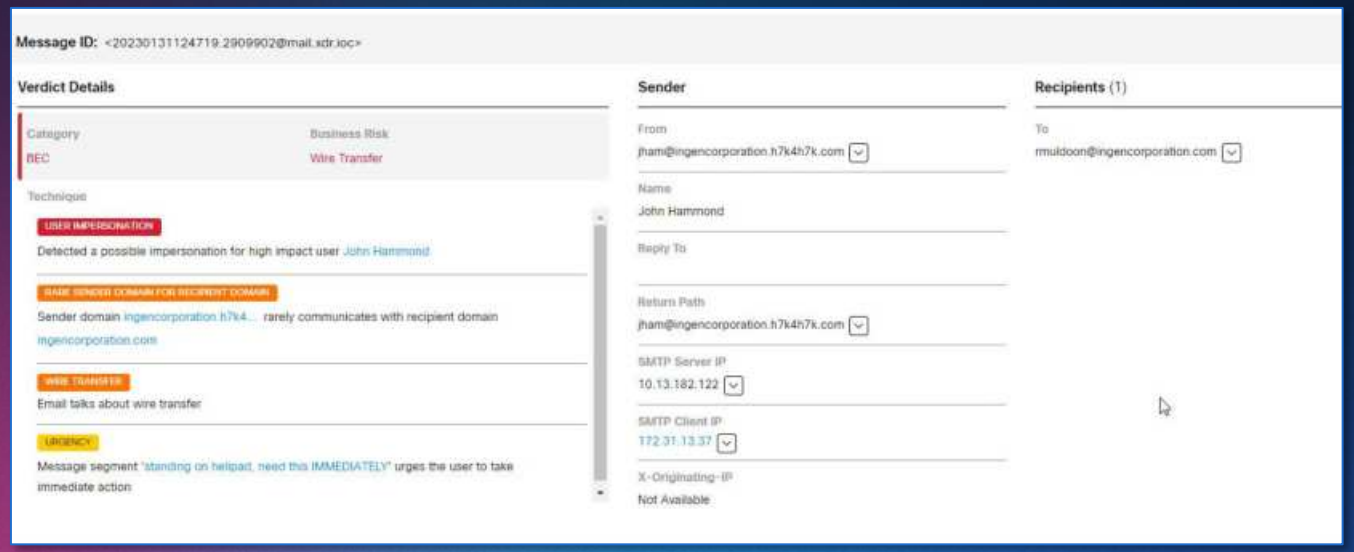
Augsta riska personu saraksts

Svarīgākie organizācijas darbinieki, piemēram, valdes locekļi un vadības komandas pārstāvji, bieži kļūst par identitātes viltošanas mērķiem, lai apdraudētu citus organizācijas darbiniekus.



Pievienojot papildu informāciju un atribūtus par šīm personām, analīzes dzinējs spēj precīzāk atpazīt identitātes viltošanas mēģinājumus.





Augstākie drošības standarti e-pasta aizsardzībā

Cisco Secure Email Threat Defense FedRAMP Moderate sertifikācija nodrošina

Drošības noturību (Security Resilience)
Nepārtraukta drošības uzraudzība un kontroles mehānismi nodrošina, ka risinājums spēj efektīvi aizsargāt pret pastāvīgi mainīgiem un arvien sarežģītākiem e-pasta draudiem.

Uzticamību un atbilstību (Trust & Adoption)
Valsts iestādes un regulētās nozares bieži pieprasa FedRAMP sertificētus risinājumus. Sertifikācija apliecina augstu drošības līmeni un atbilstību stingrām prasībām.

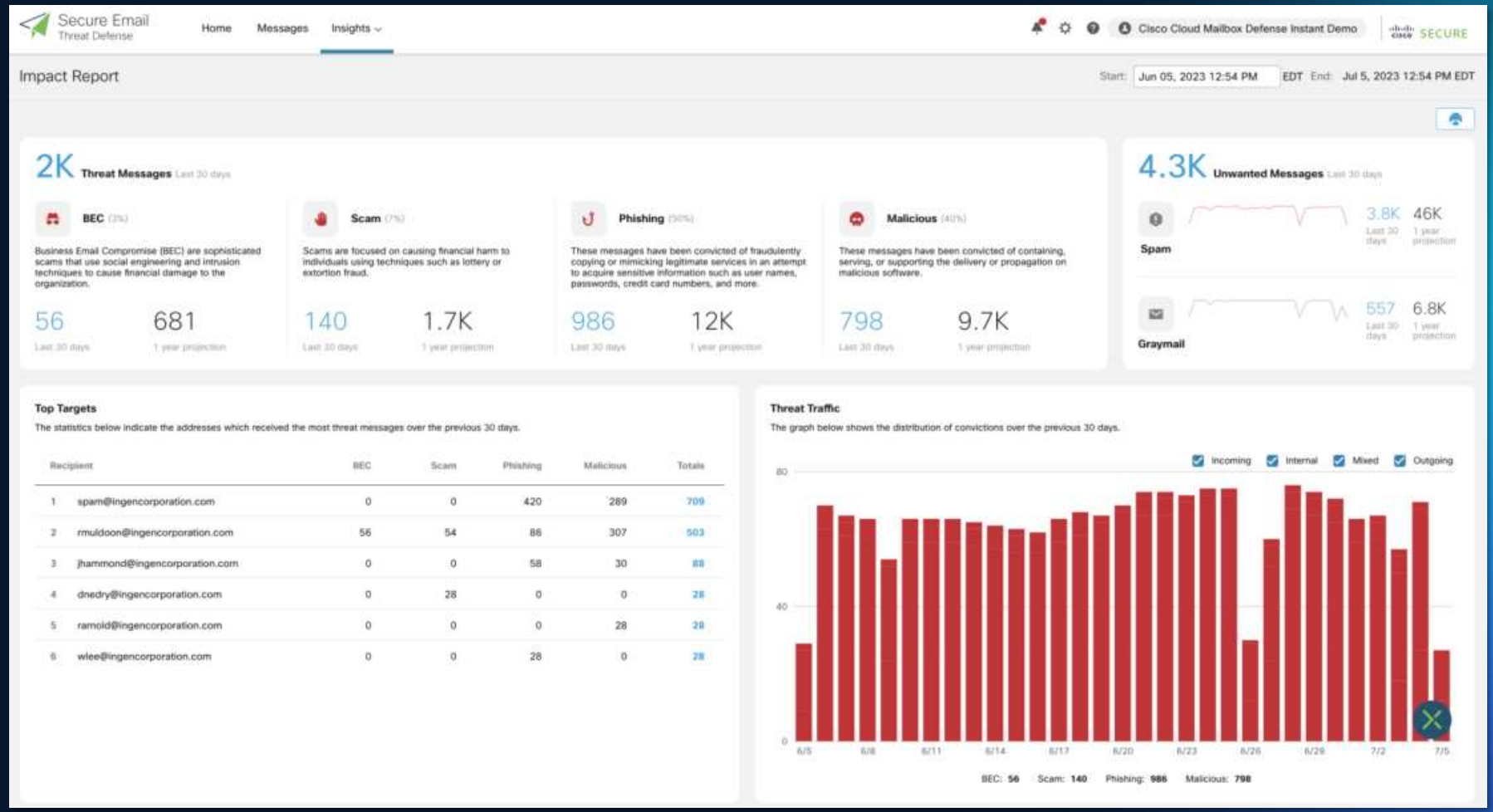
Risku pārvaldību un atbilstību normatīvajām prasībām (Risk Management & Compliance)
Automatizēta uzraudzība, regulāri drošības auditi un incidentu pārvaldība palīdz nodrošināt atbilstību un padara risinājumu par daļu no organizācijas drošības arhitektūras.

Ilgtermiņa drošības nodrošināšanu (Long-Term Assurance)
FedRAMP nav vienreizēja sertifikācija – tā paredz nepārtrauktu drošības kontroli un regulāras pārbaudes, kas nodrošina aizsardzību arī pret jaunākajiem apdraudējumiem.

FedRAMP™

Vienkārša un pārskatāma atskaišu veidošana

Galvenie drošības rādītāji ir viegli pieejami un sniedz skaidru pārskatu par e-pasta drošības efektivitāti. Tas ļauj vienkārši demonstrēt aizsardzības rezultātus vadībai, IT komandai un citām iesaistītajām pusēm.

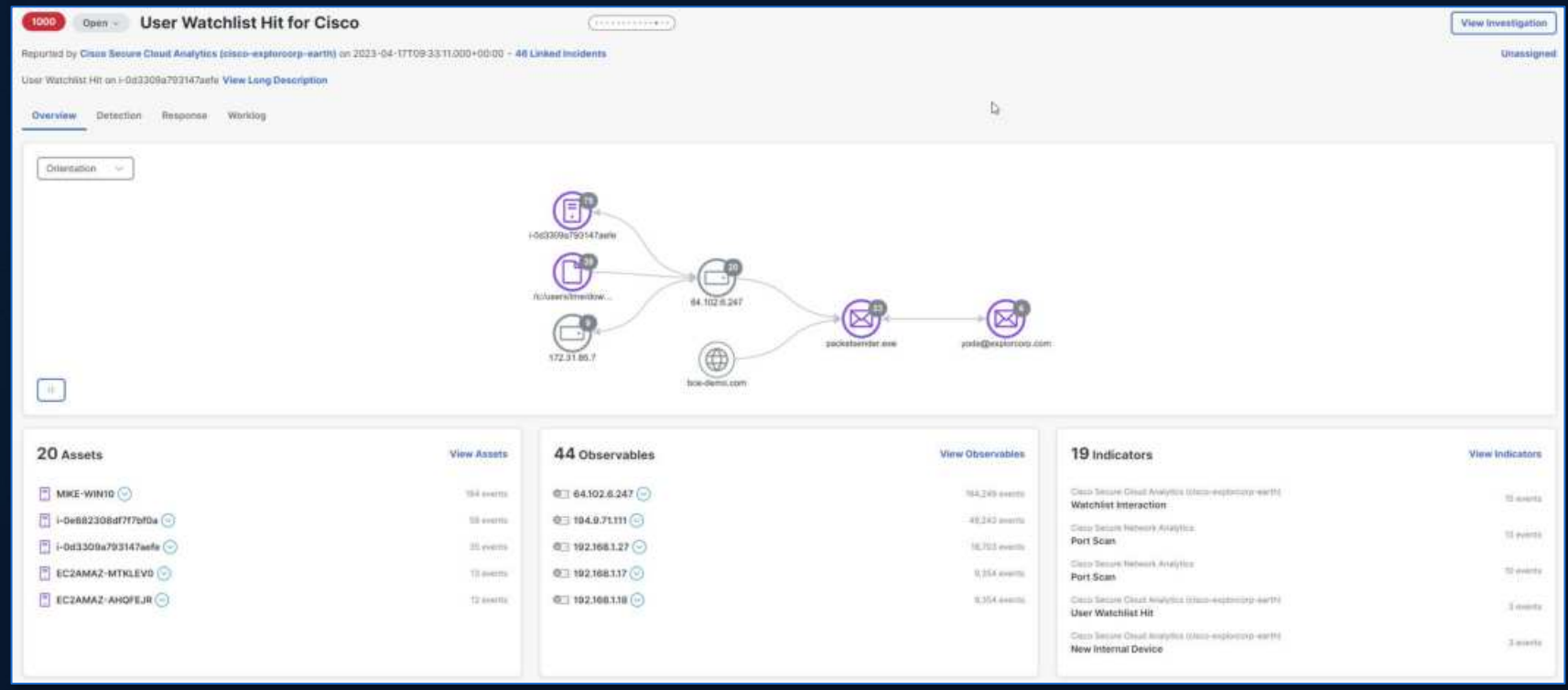


Padziļināta integrācija ar Cisco XDR

Cisco Secure Email Threat Defense ir cieši integrēts ar Cisco XDR platformu, ļaujot drošības analītiķiem ātri pāriet no e-pasta incidenta uz pilnu izmeklēšanu un nepieciešamības gadījumā nekavējoties veikt aizsardzības darbības.

No Cisco XDR iespējams analizēt un veikt darbības pēc šādiem indikatoriem

- Email Message ID
- Email Address
- Email Subject
- File Name
- Sender IP
- SHA 256
- URL



Simplify with Cisco XDR

Cisco

- Network
- Endpoint
- Email
- Cloud
- Applications
- Identity

Built on the Cisco security platform

Open and extensible

Clear prioritization

Automation and response guidance

Streamlined investigations

Your Infrastructure

- 3rd party tools
- Intelligence
- Others
- SIEM/SOAR

Your SOC

SecOps Analyst

CISO

Incident responder

The importance of a strong XDR strategy

Most attacks use a sequence like this...

You need a solution that sees deeply across the entire attack chain

Cisco XDR

Built on the Cisco Security Cloud platform

Kāpēc Cisco – ja runājam par e-pasta aizsardzību?

Cisco ilgtermiņa pieeja e-pasta drošībai

Daudzslāņu analīze un korelācija – jau sen pirms AI ēras

Cisco jau vairāk nekā ***20 gadus*** izmanto mašīnmācīšanos, uzvedības analīzi un daudzus neatkarīgus detektorus, lai korelētu dažādus signālus un atklātu e-pasta draudus.
LLM ir jaunākais papildinājums *šai jau esošajai detekcijas arhitektūrai.*

2000.–2007.
IronPort aizsardzības pamati

- Sūtītāja reputācija
- IP un domēnu reputācija
- URL reputācija
- Konteksta analīze (CASE)

2013.–2018.
Mašīnmācīšanās ēra

- ML algoritmi un anomāliju noteikšana
- Uzvedības modelēšana
- Telemetrijas korelācija starp dažādiem avotiem

2019.–2022.
Cisco Secure Email Threat Defense

- ~90 specializēti AI/ML detektori
- Uzvedības un attiecību analīze
- Daudzslāņu korelācija
- Integrācija ar Cisco XDR

2023+
LLM un nākamais evolūcijas solis

- LLM konteksta un nolūka izpratnei
- BEC un sarežģītu uzbrukumu uzlabošana
- Papildinājums – nevis aizstājējs

Kā tas darbojas šodien

Reputācijas dati (Cisco Talos) + Attiecību un uzvedības analīze + ML modeļi (~90 detektori) + LLM konteksta izpratne = Precīzs riska novērtējums

Galvenā ideja

Cisco nepāļaujas uz vienu indikatoru vai vienu AI modeli. Tā vietā mēs kombinējam ***desmitiem neatkarīgu signālu***, lai atklātu gan zināmus, gan iepriekš neredzētus uzbrukumus.

Mix & Match Tiers of User and Breach Protection Suites

User Protection Suite

Essentials

- Secure Access Essentials
  (Secure Internet + Secure Private Access)
- Duo Advantage
- Email Threat Defense

Advantage

Everything in Essentials **Plus**

- Secure Access Advantage
  (Secure Internet + Secure Private Access)
- ISE Premier
- Secure Endpoint Advantage

Breach Protection Suite

Essentials

- Cisco XDR Essentials
- Secure Endpoint Advantage
- Email Threat Defense

Advantage

Everything in Essentials **Plus**

- Cisco XDR Advantage
- Secure Endpoint Premier
- Secure Network Analytics
- Cisco Telemetry Broker

Premier

Everything in Advantage Plus

- Cisco XDR Premier (Managed XDR)
- Cisco Talos Incident Response
- Cisco Technical Security Assessments


CISCO