CISCO
SECURE

CISCO The bridge to possible

Inteligência Artificial na Cibersegurança

Abinee

Giuseppe Marrara
Diretor Senior Politicas Publicas
América Latina

What is AI?

What it means?

Is it NEW?

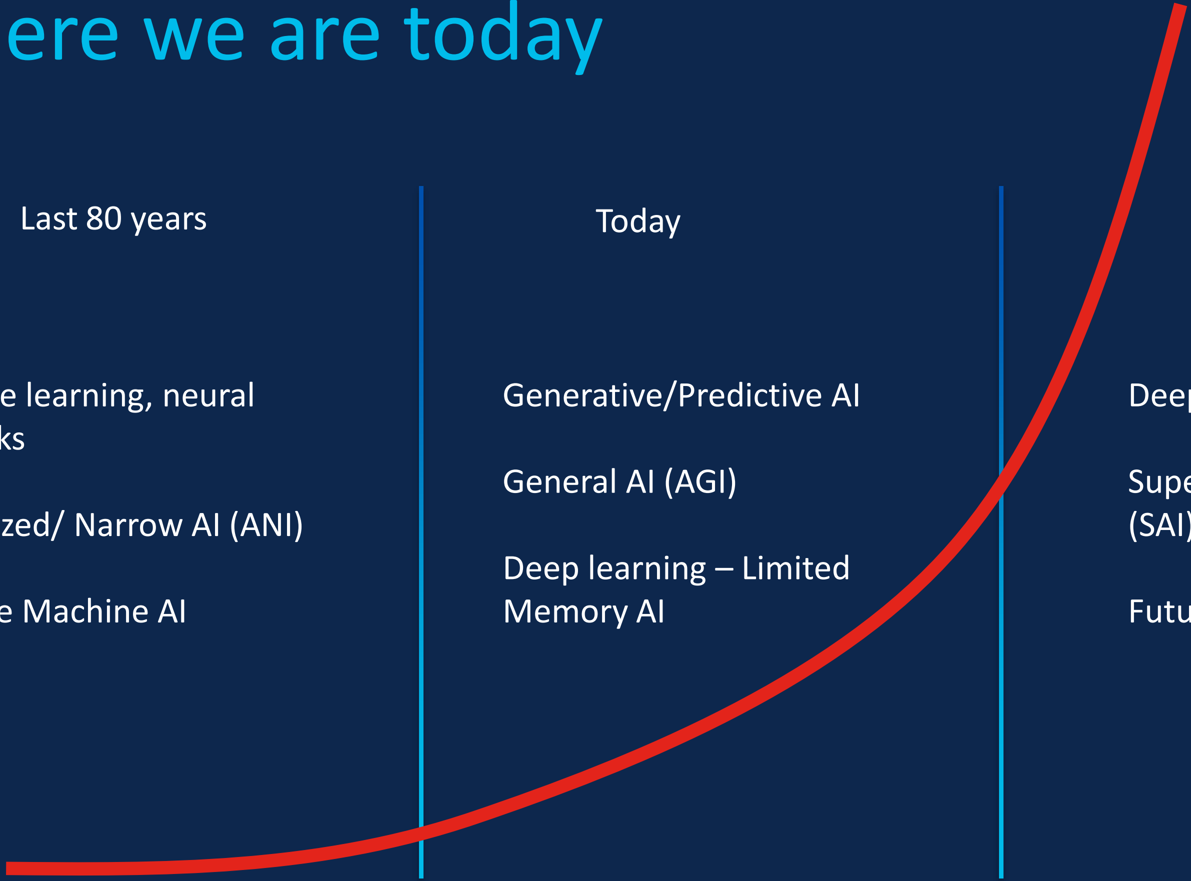
Types of AI

Machine Learning

Generative/Predictive

Deep Learning

Where we are today



Last 80 years

Machine learning, neural networks

Specialized/ Narrow AI (ANI)

Reactive Machine AI

Today

Generative/Predictive AI

General AI (AGI)

Deep learning – Limited Memory AI

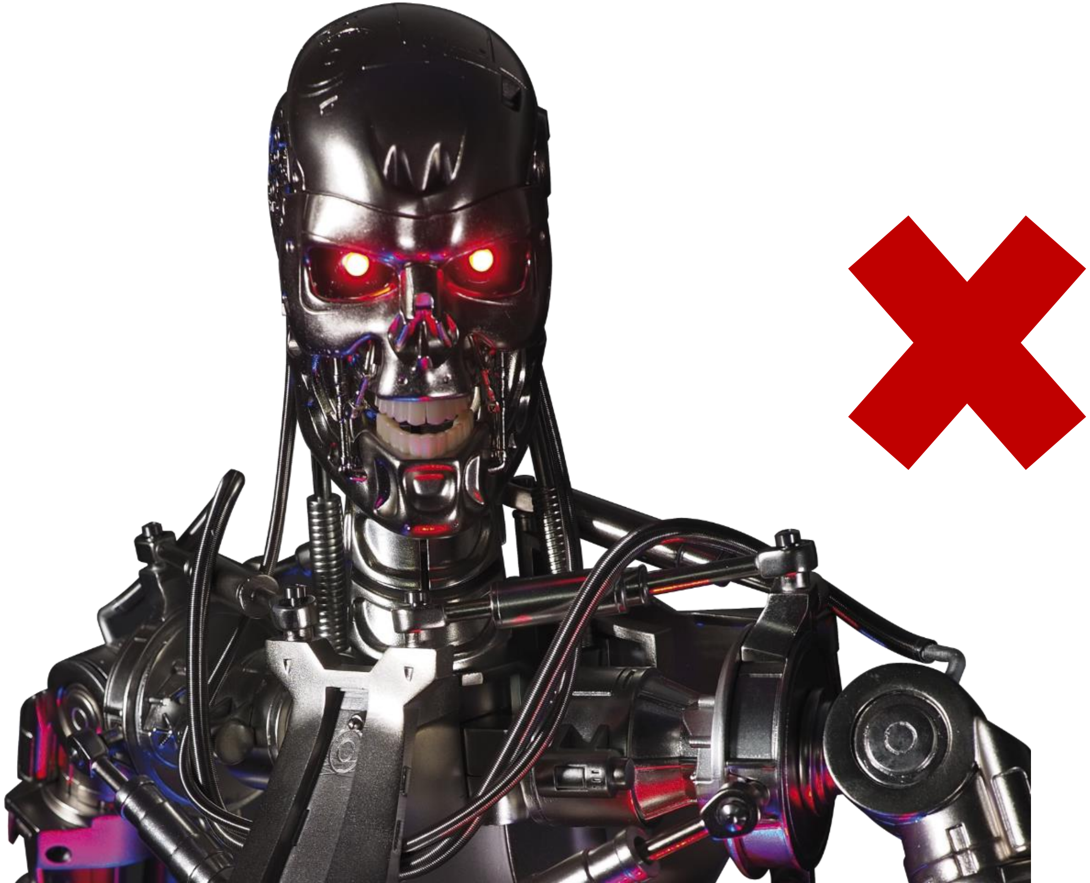
Future (or never?)

Deep learning

Superior/Superintelligent (SAI)

Future or Science fiction?

- Theory of Mind AI
- Self-aware AI?



✕

PHISHING

AI is shaping the future

15.7T AI is expected to contribute to the global economy by 2030

75% of enterprise-generated data will be created and processed at the edge by 2025

90% of enterprise AI workloads will run on Ethernet by 2025

300B Global spending on AI by 2026

97% of business owners believe that Generative AI will benefit their businesses

40% Increase in productivity from utilizing AI by 2035

AI Transformation Benefits

Increased Efficiency & Automation

Intelligent capabilities

- Automated workflows drive efficiencies between business and IT
- Extensible solution adds new capabilities to single pane of glass
- Real-time actionable metrics maximize value regarding spend decisions

Enhanced Security Decision-Making

Security and Observability

- Capture, analyze and reduce spend for cloud & on-prem resources
- Greater visibility and understanding of the environment and data.
- Improve chargeback across the cloud and on-prem by geo and LOB

Work Force Enhancement

Work Force Efficiency

- End-to-end automation of common tasks
- Shift from common tasks to business priorities
- Focus on upskilling workforce
- Secure Hybrid work
- Talent attraction and Retention

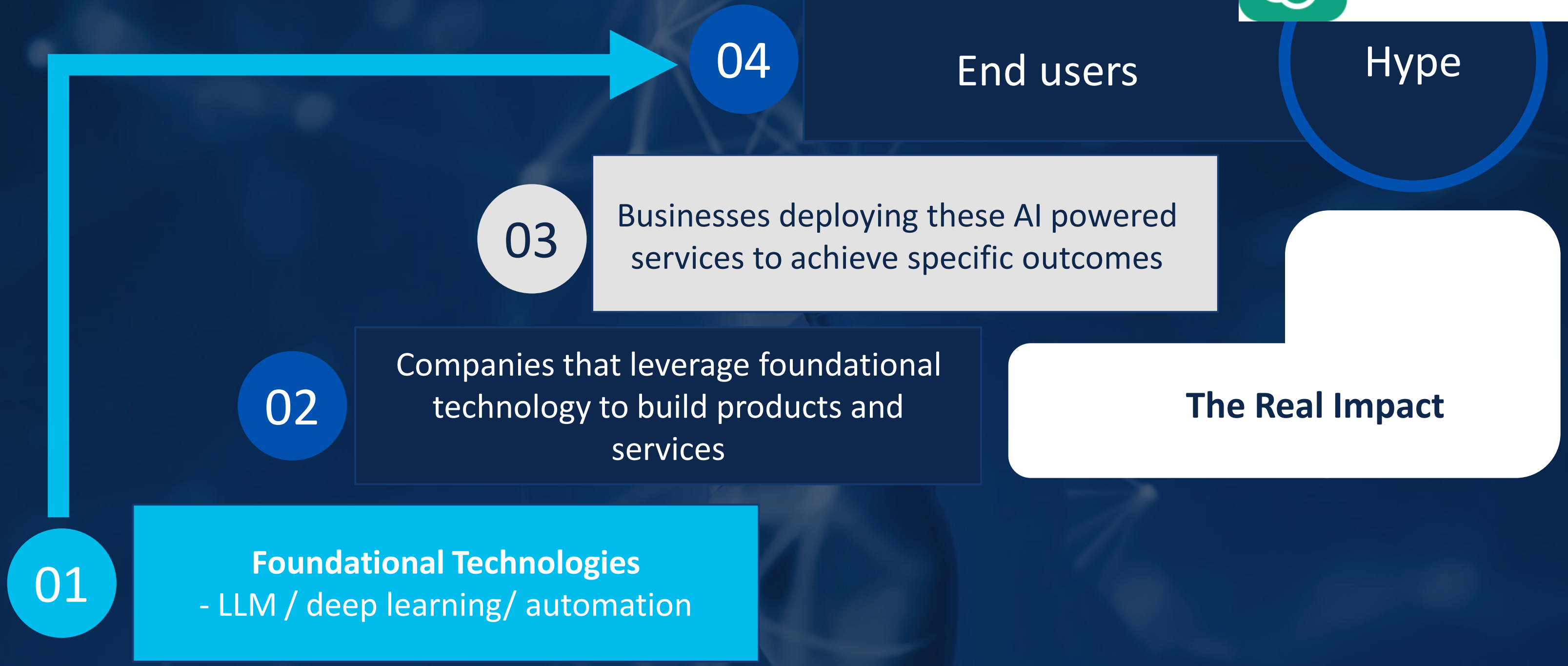
Service Improvements & Cost Savings

Modernization savings

- Streamlining research and development processes
- predicting market trends, and simulating outcomes.
- Creation of new products and services
- Meet evolving customer needs more effectively.

Artificial Intelligence: The Hype versus reality

ChatGPT



04 End users

Hype

03 Businesses deploying these AI powered services to achieve specific outcomes

02 Companies that leverage foundational technology to build products and services

The Real Impact

01 **Foundational Technologies**
- LLM / deep learning/ automation

AI Readiness Index

AI Readiness: The foundational building blocks

Strategy

Do they **have it** and how well-defined it is?

Is there **a clear owner** of strategy?

Do they have **measurement metrics** and how well defined they are?

Do they have a **financial strategy** to sustainably fund AI deployments in the long term?

How is funding for AI **prioritized**?

Infrastructure

Compute
- GPU Resources
- Scalability
- Allocation

Network
- Scalability
- Latency and Throughput
- AI Integration (data flow)

Cybersecurity
- Awareness of threats
- Ability to detect and prevent tampering
- Protection of data used in AI models (encryption)
- Managing access control

Sustainable Infra
- Ready from power consumption perspective

Data

Quality of in-house data
- How centralized it is
- Cleaned & pre-processed
- Process for data access

Analytics Tool
- Sophistication
- Scalability
- Integration

Staff proficiency
- To leverage AI Data sets and Analytics tools

Quality of external data
- Processes to check quality and reliability
- Effectiveness to track origin and lineage
- Effectiveness to check accuracy of data

Governance

Bias and fairness in data
- Awareness
- Ability to detect
- Process to remediate

Algorithms
- Transparency of workings of algorithms deployed
- Ability to detect bias or lack of fairness

Data Privacy
- Understanding of global standard
- Data anonymization
- Preparedness to address and rectify data breaches

Data Sovereignty
- Understanding of global standards
- Data storage in compliance
- Data transfer in compliance

Comprehensives of AI policies and protocols

Talent

How well / under resourced their in-house talent is pool is for AI?

What is the **overall proficiency level** of the in-house talent from an AI perspective?

Are **they investing in training programs** to ensure talent stay up to date with requisite skills, if yes, what is the scale of investments?

Do they **have policies to ensure accessibility** of AI technologies for differently abled employees?

Culture

Level of **urgency to deploy AI / AI-powered technologies**

Level of **receptiveness to changes** triggered by AI
- **Board**
- **Executive leadership**
- **Middle Management**
- **Employees**

Do they have a **change management plan** in place to tackle with the changes?

Quality and depth of the **change management plan**

AI Readiness: The foundational building blocks

Strategy

15%

Do they have it and how well defined it is?	20
Is there a **clear owner** of strategy?	20
Do they have **measurement metrics** & how well-defined they are?	20
Do they have **a financial strategy** to sustainably fund AI deployments in the long-term?	20
How is **funding for AI prioritized**?	20

Infrastructure

25%

Compute • GPU Resources Scalability • Allocation	30
Network • Scalability • Latency & Throughput • AI Integration (data flow)	30
Cybersecurity • Awareness of threats • Ability to detect & prevent tampering • Protection of data used in AI models (encryption) • Managing access control	30
Sustainable Infra • Ready from power consumption perspective	10

Data

20%

Quality of In-house Data • How centralized it is • Cleaned & pre-processed	30
Analytics Tool • Sophistication • Scalability • Integration	30
Staff Proficiency • To leverage AI Data sets and Analytics tools	10
Quality of External Data • Processes to check quality & reliability • Effectiveness to track origin & lineage • Effectiveness to check accuracy of data	30

Governance

15%

Bias & Fairness in Data • Awareness • Ability to detect • Process to remediate	25
Algorithms • Transparency of workings of algorithms deployed • Ability to detect bias or lack of fairness	15
Data Privacy • Understanding of global standard • Data anonymization • Preparedness to address & rectify data breaches	25
Data Sovereignty • Understanding of global standards • Data storage in compliance • Data transfer in compliance	20
Comprehensives of AI policies and protocols	15

Talent

15%

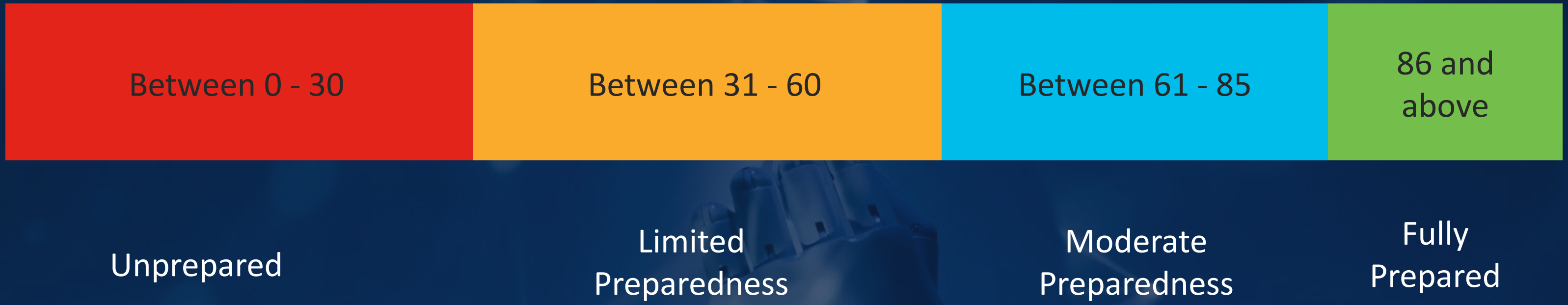
How **well / under resourced** their in-house talent is pool is for AI?	30
What is the **overall proficiency level** of the in-house talent from an AI perspective?	25
Are they **investing in training programs** to ensure talent stay up to date with requisite skills, if yes, what is the scale of investments?	25
Do they have **policies to ensure accessibility** of AI technologies for differently abled employees?	20

Culture

10%

Level of **urgency to deploy AI / AI-powered technologies**	15
Level of receptiveness to changes triggered by AI • Board • Executive leadership • Middle Management • Employees	60
Do they have a **change management plan** in place to tackle with the changes?	10
Quality & depth of the change management plan	15

AI Readiness: Measuring overall preparedness of companies



Between 0 - 30

Unprepared

Between 31 - 60

Limited Preparedness

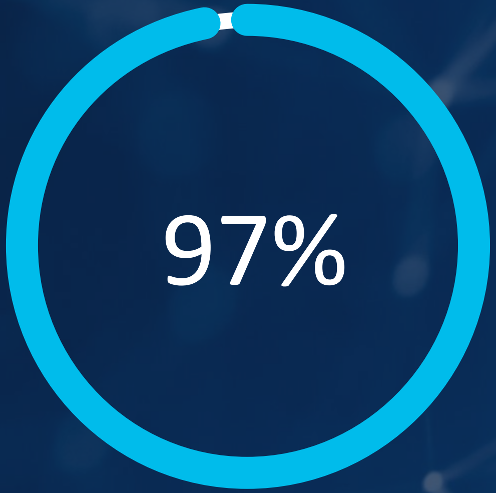
Between 61 - 85

Moderate Preparedness

86 and above

Fully Prepared

Artificial Intelligence: Hype is driving urgency



Urgency to deploy AI / AI-powered technologies has increased in the past six months

*61% say it has increased *SIGINIFICANTLY*

The pressure is coming from everyone

Board of Directors

Client-facing Team Members

Investors & Shareholders

Corp. Function Leaders & Team Members

CEO & Leadership Team

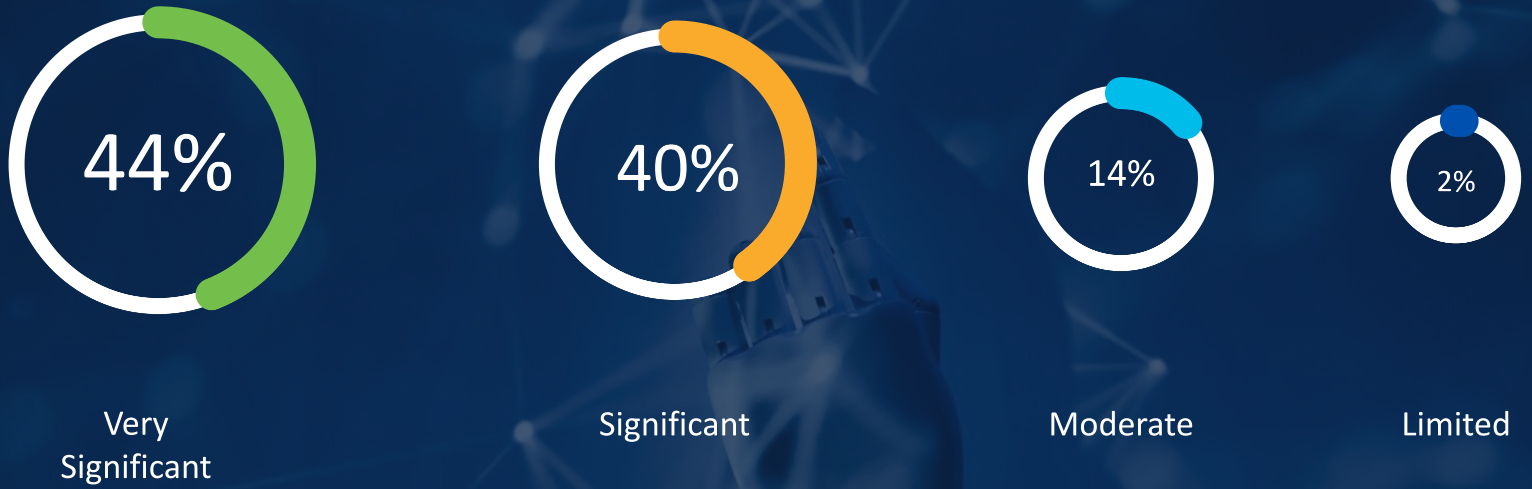
Increased Hype Around AI

Fear of Being Left Behind

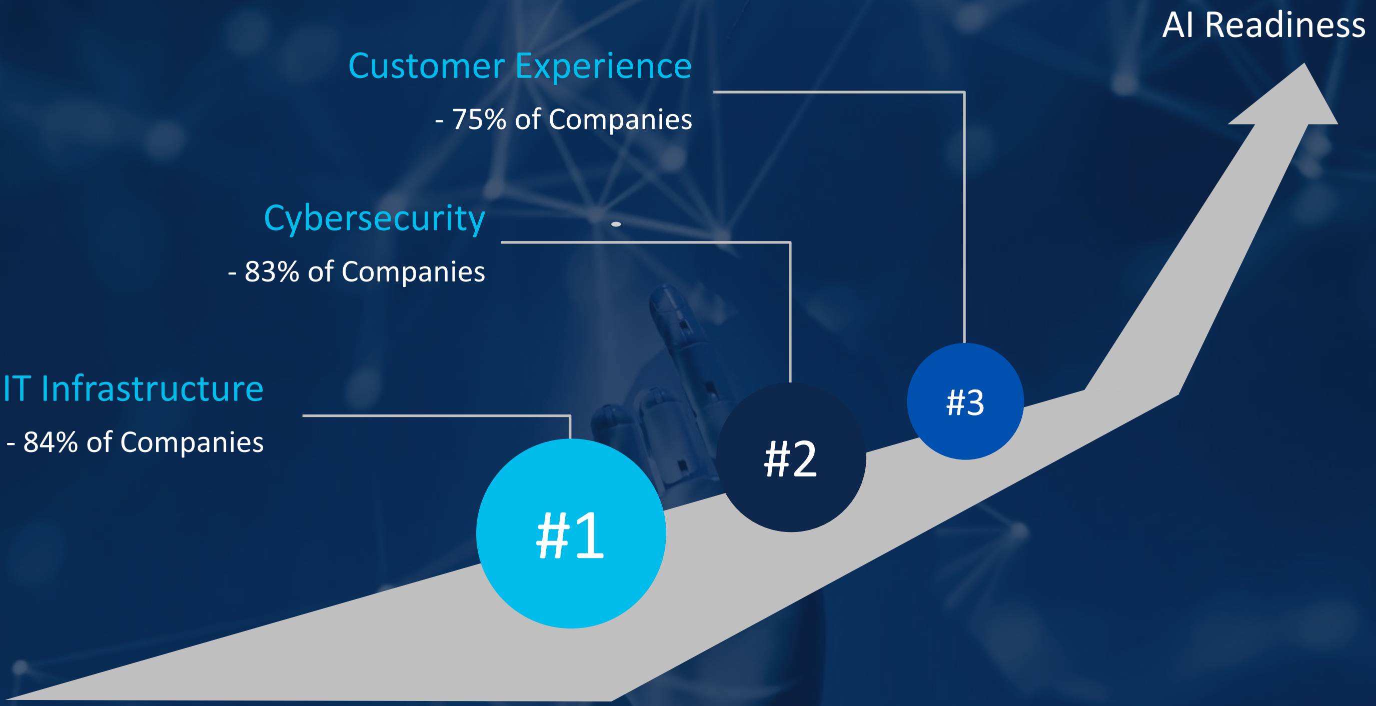
Middle Management & Business Unit Leaders

Revenue Opportunities

Companies realise the importance of AI for their business



Top Areas Where Businesses Are Deploying AI



AI Readiness

Customer Experience

- 75% of Companies

Cybersecurity

- 83% of Companies

IT Infrastructure

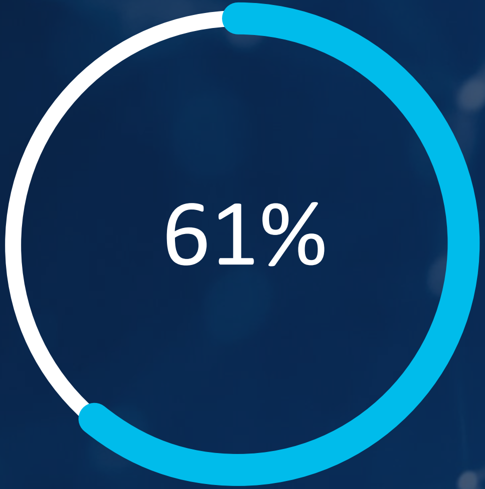
- 84% of Companies

#1

#2

#3

Global AI Readiness: Losing competitive advantage



Feel they have a maximum of one year to implement their AI strategy before significant negative business impacts

What can organizations do to boost AI Readiness?

Look long-term and think big

Build infrastructure for the future

Breakdown data silos

Keep people at the core

Deploy timely internal policies and protocols to keep pace with the industry

CISCO Evolving AI-driven portfolio: today

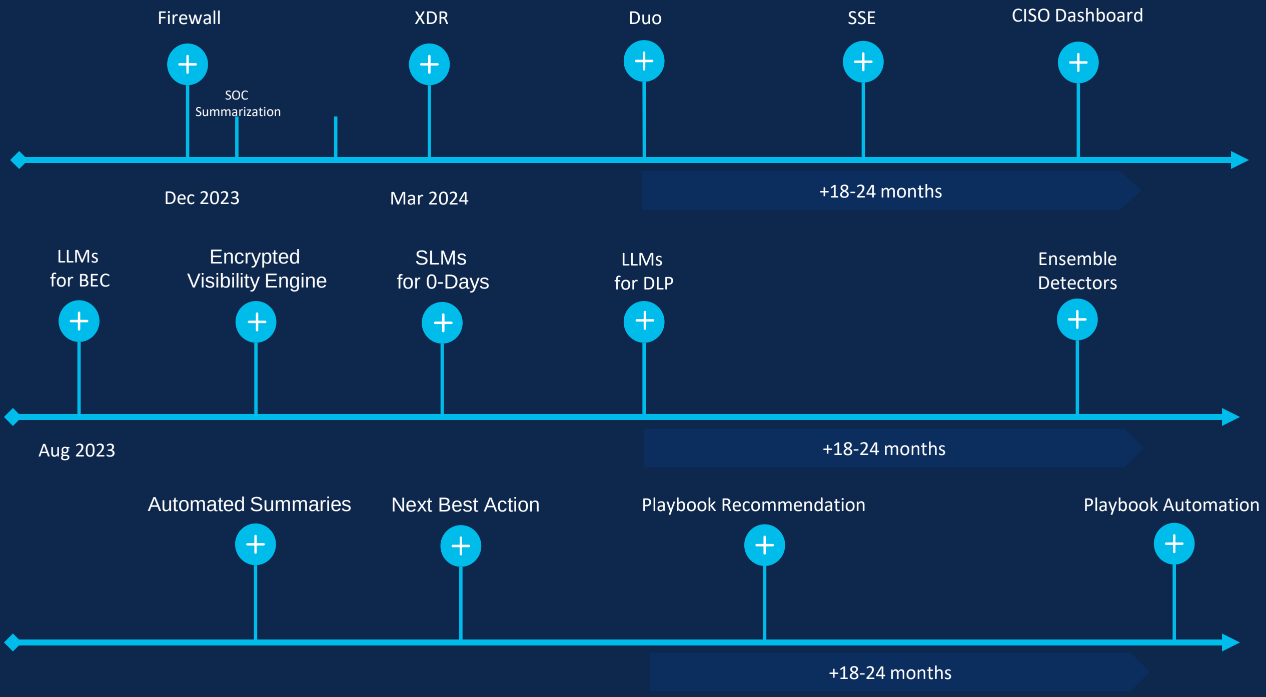
	Security	Networking	Collaboration	Observability	CX/Sales
Generative AI	• Email text threat analysis **In development:** • Simplifying Security (e.g., Policy Assistant for Firewall) • Sophisticated attack prevention (e.g., SOC assistant) • Secure use of LLMs (e.g., DLP)	• Enabled by Silicon One Scheduled Fabric Ethernet Solution **In development:** • AIOps • Assurance **Long-term:** • Virtual Network Assistant (incl network config. generator)	**In development:** • Webex GPT • Webex Assistant **Long-term:** • Intelligent Contact Center	**In development:** • Model observability • Prompt interface • AI assistant for summarization	**In development:** • AI framework and generated test cases • AI assisted automation **Long-term:** • Proactive protection of devices and services • Proactive sustainability
Predictive AI	• Statistical modeling • Threat Analysis • Endpoint, Policy, and Trust Analysis • Advanced Endpoint Malware Protection/ Prediction • Cloud-based infra, application, and data protection	• Network Management • Network Assurance • Network Deployment • Anomaly Detection • Change Automation • Predictive QoS impact • Root Cause Analysis • AIOps automation • EVE / AI assistants	• Noise Removal • People Focus (video) • Personal/team Insights • Inclusive Meetings (transcription, live translation) • Real-time speech enhancements	• Statistical Modeling • Baselining • Anomaly Detection • Intelligent Automation	• TAC Support Assistant • Sentiment Prediction • SW Anomaly Detection • HW Failure Prediction • Text Scraping • Statistical Modeling • Change Automation • Problem Diagnosis

CISCO AI

Networking	Security	Collaboration	Observability	Cloud
Catalyst Center AIOps	AI Assistant for Security	Webex AI Assistant	Anomaly Detection	Workload Infrastructure
AI Assistant for Networking	Identity Intelligence	Nvidia Powered Devices	Dynamic Baseline	Nvidia Partnership
Silicon One	Endpoint Analytics	Real Time Media Model	Business Risk Score	SaaS delivered AI

AI Powered Cross Architecture Portfolio

AI é fundamental em toda a cadeia de telecomunicações



Assistente Experiencia

Firewall

SOC Summarization

XDR

Duo

SSE

CISO Dashboard

Dec 2023

Mar 2024

+18-24 months

Potencialização Detecção

LLMs for BEC

Encrypted Visibility Engine

SLMs for 0-Days

LLMs for DLP

Ensemble Detectors

Aug 2023

+18-24 months

Automação Ações

Automated Summaries

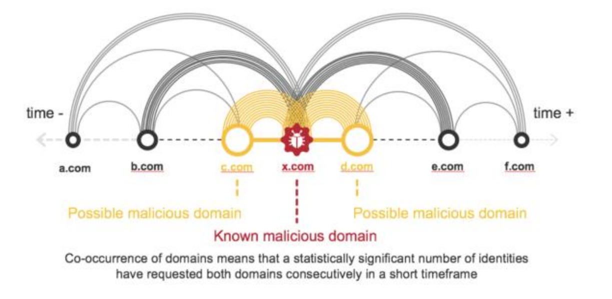
Next Best Action

Playbook Recommendation

Playbook Automation

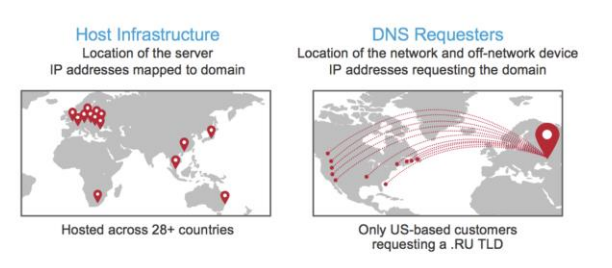
+18-24 months

We Make Sense of Data



Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

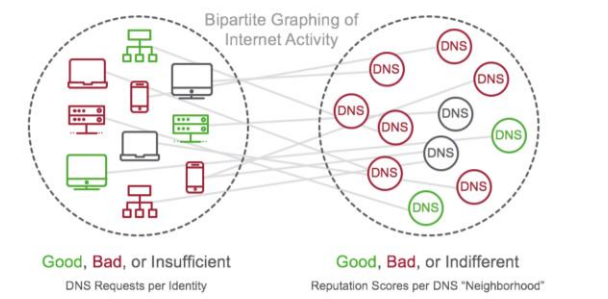
Guilt by inference


Host Infrastructure
Location of the server
IP addresses mapped to domain

Hosted across 28+ countries

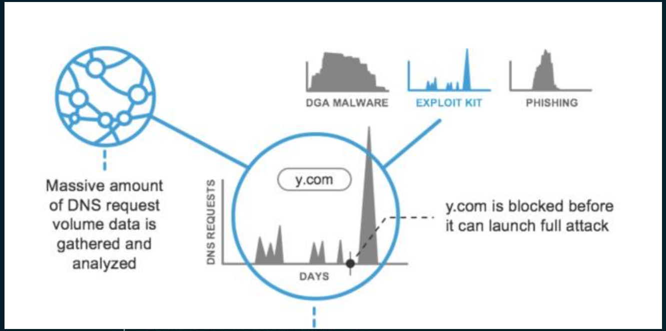
DNS Requesters
Location of the network and off-network device
IP addresses requesting the domain

Only US-based customers requesting a .RU TLD


Bipartite Graphing of Internet Activity

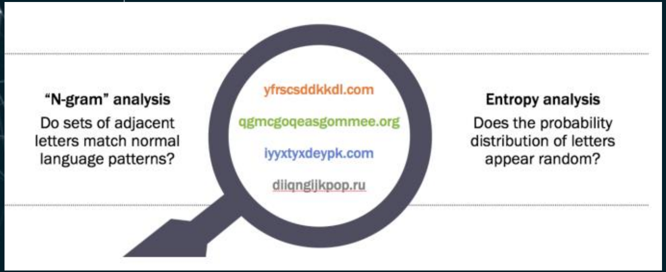
Good, Bad, or Insufficient
DNS Requests per Identity

Good, Bad, or Indifferent
Reputation Scores per DNS "Neighborhood"

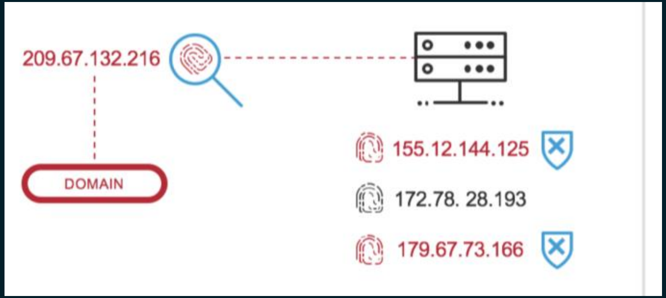


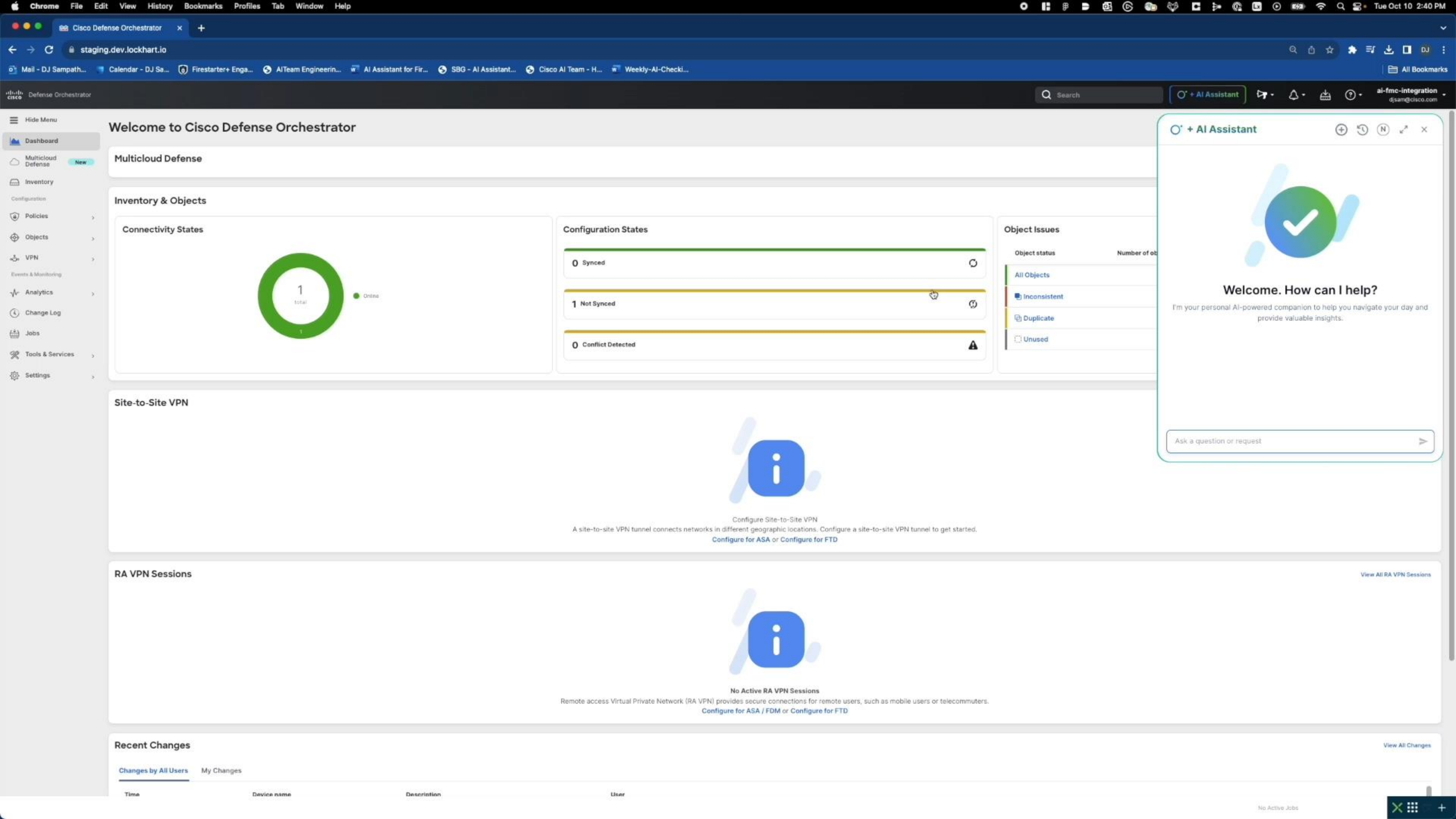
Massive amount of DNS request volume data is gathered and analyzed

y.com is blocked before it can launch full attack


"N-gram" analysis
Do sets of adjacent letters match normal language patterns?

Entropy analysis
Does the probability distribution of letters appear random?





Welcome to Cisco Defense Orchestrator

Multicloud Defense

Inventory & Objects

Connectivity States

Configuration States

0 Synced

1 Not Synced

0 Conflict Detected

Object Issues

Object status	Number of ob
All Objects	
Inconsistent	
Duplicate	
Unused	

Site-to-Site VPN

Configure Site-to-Site VPN

A site-to-site VPN tunnel connects networks in different geographic locations. Configure a site-to-site VPN tunnel to get started.

Configure for ASA or Configure for FTD

RA VPN Sessions

View All RA VPN Sessions

No Active RA VPN Sessions

Remote access Virtual Private Network (RA VPN) provides secure connections for remote users, such as mobile users or telecommuters.

Configure for ASA / FDM or Configure for FTD

Recent Changes

View All Changes

Changes by All Users | My Changes

Time	Device name	Description	User

No Active Jobs

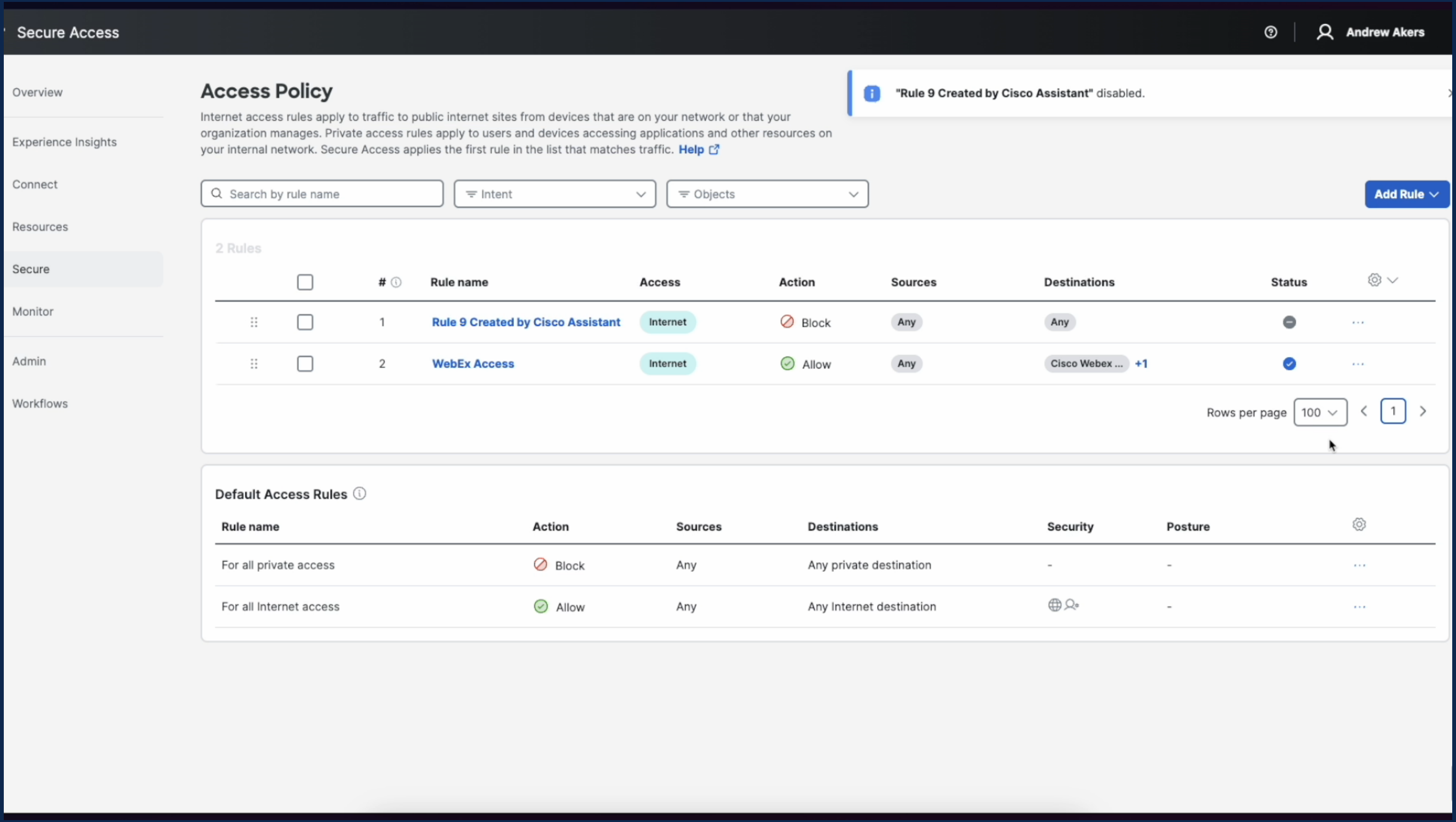
+ AI Assistant

Welcome. How can I help?

I'm your personal AI-powered companion to help you navigate your day and provide valuable insights.

Ask a question or request

Peça a IA para criar uma regra que bloqueia o acesso de um usuário ao Jira



"Rule 9 Created by Cisco Assistant" disabled.

Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. Help

2 Rules

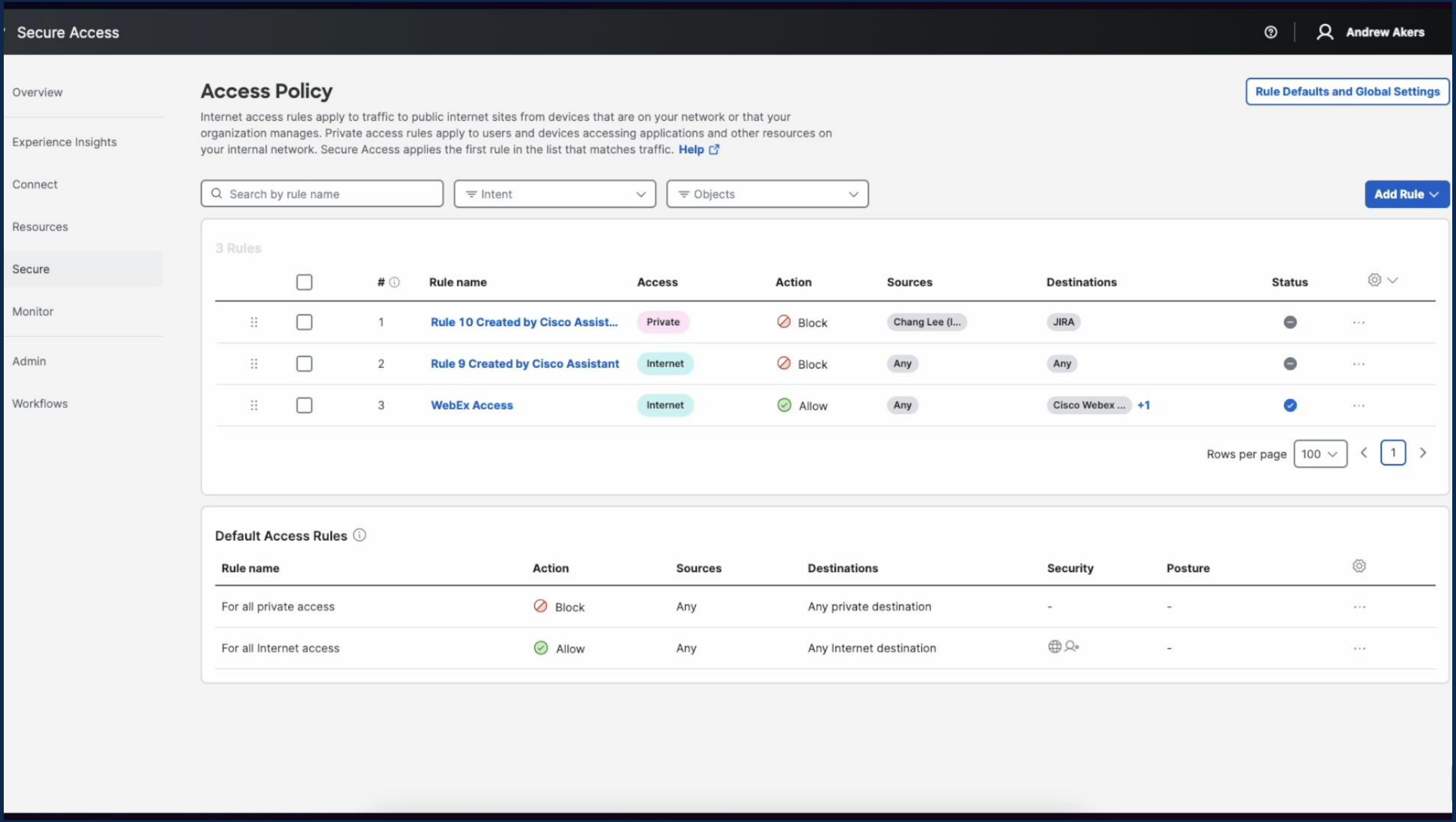
□	#	Rule name	Access	Action	Sources	Destinations	Status
□	1	Rule 9 Created by Cisco Assistant	Internet	Block	Any	Any	⊖
□	2	WebEx Access	Internet	Allow	Any	Cisco Webex ... +1	✓

Rows per page 100 ‹ 1 ›

Default Access Rules

Rule name	Action	Sources	Destinations	Security	Posture
For all private access	Block	Any	Any private destination	-	-
For all Internet access	Allow	Any	Any Internet destination		-

Peça a IA para criar um acesso a internet e a intranet



Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. Help

3 Rules

□	#	Rule name	Access	Action	Sources	Destinations	Status
□	1	Rule 10 Created by Cisco Assist...	Private	Block	Chang Lee (I...	JIRA	⊖
□	2	Rule 9 Created by Cisco Assistant	Internet	Block	Any	Any	⊖
□	3	WebEx Access	Internet	Allow	Any	Cisco Webex ... +1	✓

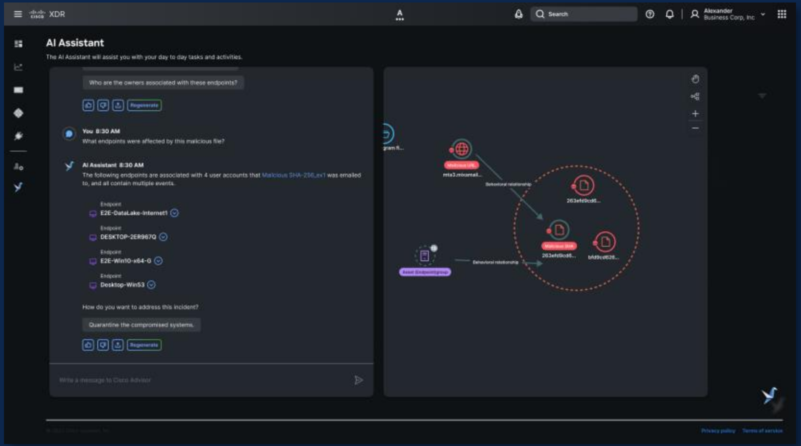
Rows per page 100 ‹ 1 ›

Default Access Rules

Rule name	Action	Sources	Destinations	Security	Posture
For all private access	Block	Any	Any private destination	-	-
For all Internet access	Allow	Any	Any Internet destination		-

Assistentes de IA para Cyber

Integração e Plataforma



AI Assistant

The AI Assistant will assist you with your day to day tasks and activities.

Who are the owners associated with these endpoints?

Regenerate

You 8:30 AM
What endpoints were affected by this malicious file?

AI Assistant 8:30 AM
The following endpoints are associated with 4 user accounts that Malicious SHA-256_ex1 was emailed to, and all contain multiple events.

Endpoint
E2E-DataLake-Internet1

Endpoint
DESKTOP-2ER967Q

Endpoint
E2E-Win10-x64-G

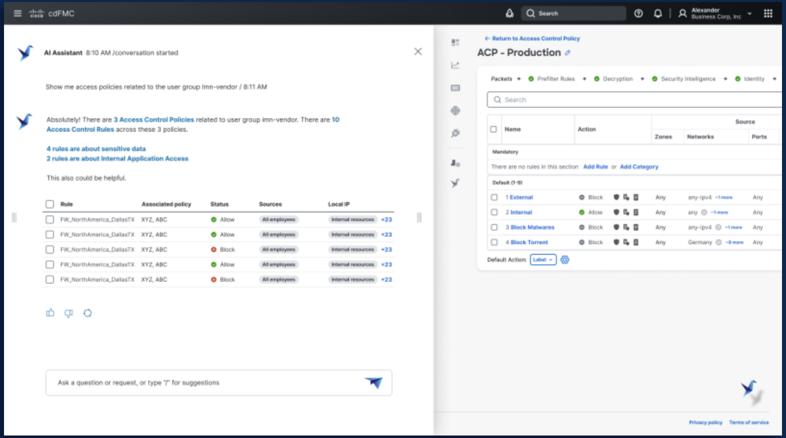
Endpoint
Desktop-Win53

How do you want to address this incident?

Quarantine the compromised systems.

Regenerate

Write a message to Cisco Advisor



AI Assistant 8:10 AM /conversation started

Show me access policies related to the user group imn-vendor / 8:11 AM

Absolutely! There are 3 Access Control Policies related to user group imn-vendor. There are 10 Access Control Rules across these 3 policies.

4 rules are about sensitive data
2 rules are about Internal Application Access

This also could be helpful.

☐	Rule	Associated policy	Status	Sources	Local IP
☐	FW_NorthAmerica_DallasTX	XYZ, ABC	● Allow	All employees	Internal resources +23
☐	FW_NorthAmerica_DallasTX	XYZ, ABC	● Allow	All employees	Internal resources +23
☐	FW_NorthAmerica_DallasTX	XYZ, ABC	● Block	All employees	Internal resources +23
☐	FW_NorthAmerica_DallasTX	XYZ, ABC	● Allow	All employees	Internal resources +23
☐	FW_NorthAmerica_DallasTX	XYZ, ABC	● Block	All employees	Internal resources +23

Ask a question or request, or type "/" for suggestions

← Return to Access Control Policy

ACP - Production

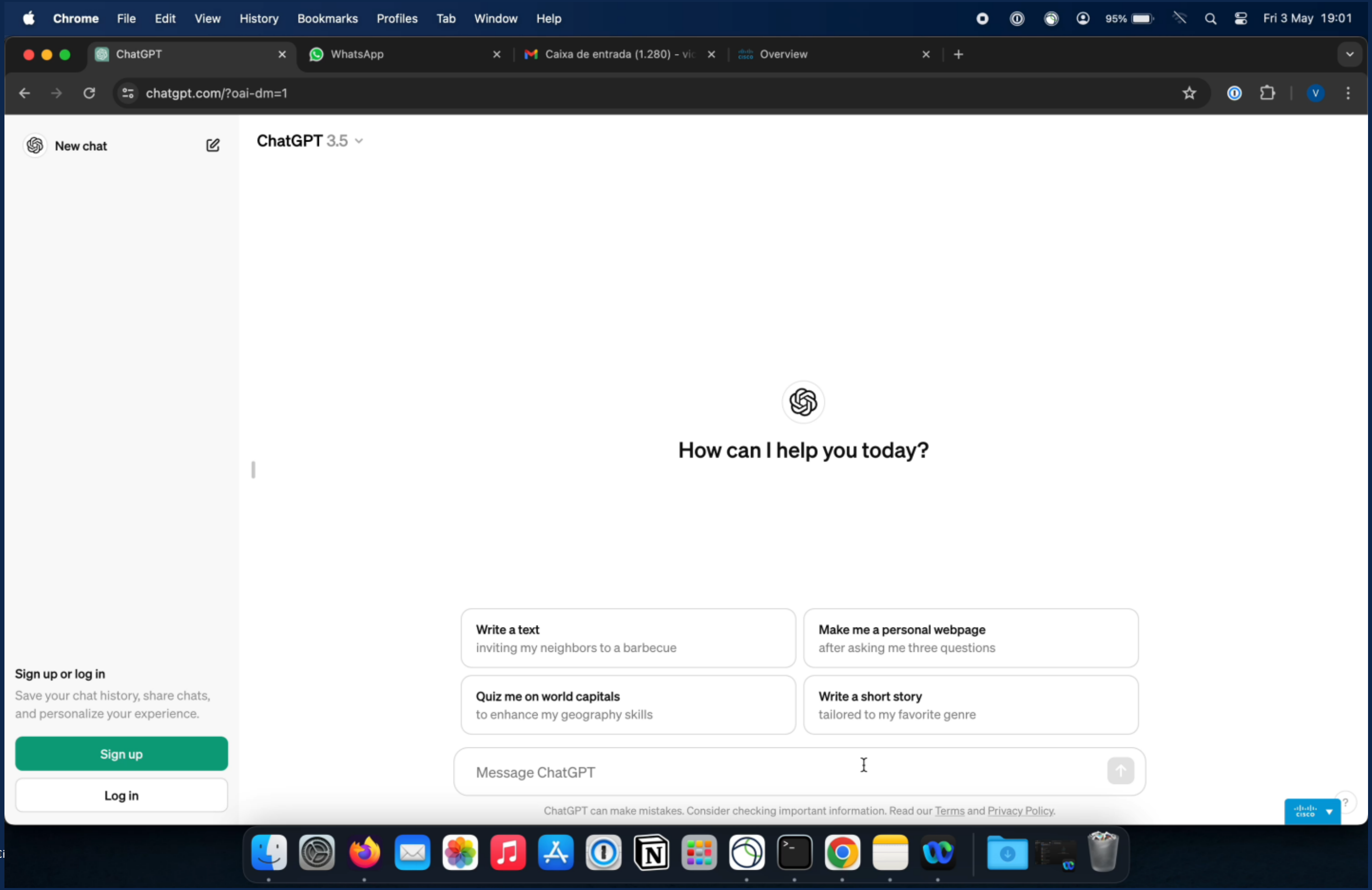
Packets → Prefilter Rules → Decryption → Security Intelligence → Identity →

Search

☐	Name	Action	Source		
			Zones	Networks	Ports
	Mandatory				
	There are no rules in this section Add Rule or Add Category				
	Default (1-9)				
☐	1 External	Block	Any	any-ipv4 +1 more	Any
☐	2 Internal	Allow	Any	any +1 more	Any
☐	3 Block Malwares	Block	Any	any-ipv4 +1 more	Any
☐	4 Block Torrent	Block	Any	Germany +8 more	Any

Default Action: Label

Controle de IA - Demo



How can I help you today?

Write a text
inviting my neighbors to a barbecue

Make me a personal webpage
after asking me three questions

Quiz me on world capitals
to enhance my geography skills

Write a short story
tailored to my favorite genre

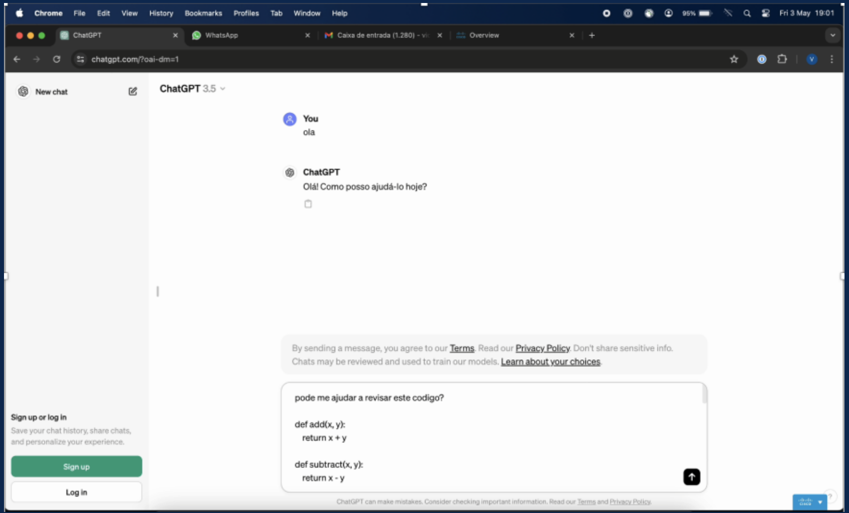
Message ChatGPT

ChatGPT can make mistakes. Consider checking important information. Read our Terms and Privacy Policy.

Sign up or log in

Save your chat history, share chats, and personalize your experience.

Controle de IA – ChatGPT – Análise de Código



You
ola

ChatGPT
Olá! Como posso ajudá-lo hoje?

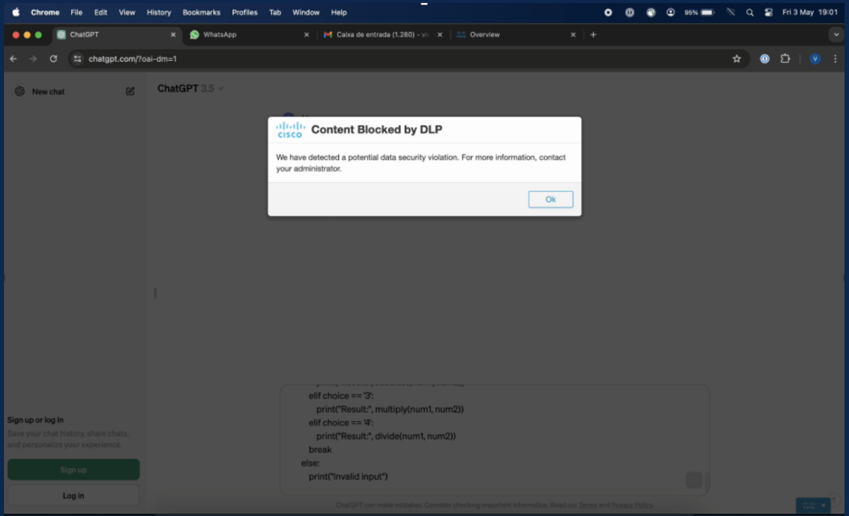
By sending a message, you agree to our Terms. Read our Privacy Policy. Don't share sensitive info. Chats may be reviewed and used to train our models. Learn about your choices.

```
pode me ajudar a revisar este codigo?

def add(x, y):
  return x + y

def subtract(x, y):
  return x - y
```

Sign up or log in

Save your chat history, share chats, and personalize your experience.

ChatGPT can make mistakes. Consider checking important information. Read our Terms and Privacy Policy.



Content Blocked by DLP

We have detected a potential data security violation. For more information, contact your administrator.

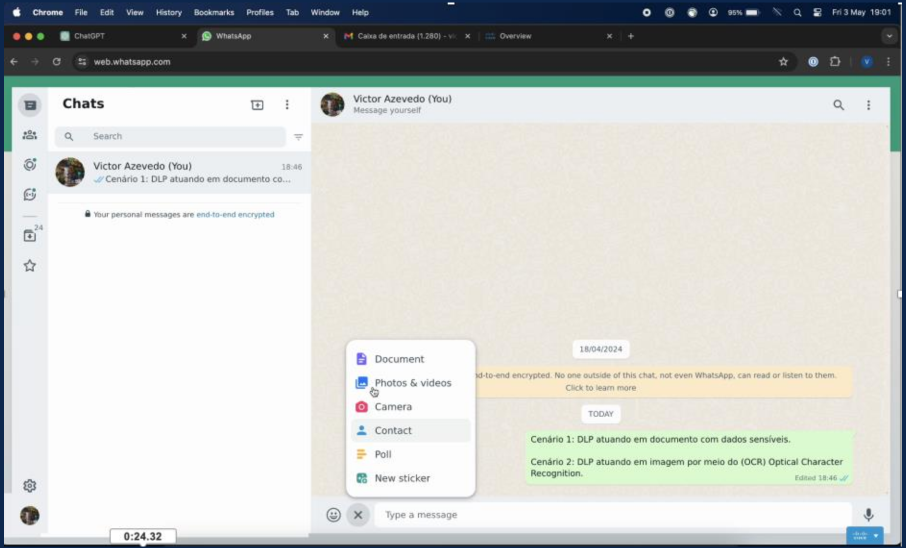
```
    elif choice == '3':
      print("Result:", multiply(num1, num2))
    elif choice == '4':
      print("Result:", divide(num1, num2))
    break
  else:
    print("Invalid input")
```

Sign up or log in

Save your chat history, share chats, and personalize your experience.

ChatGPT can make mistakes. Consider checking important information. Read our Terms and Privacy Policy.

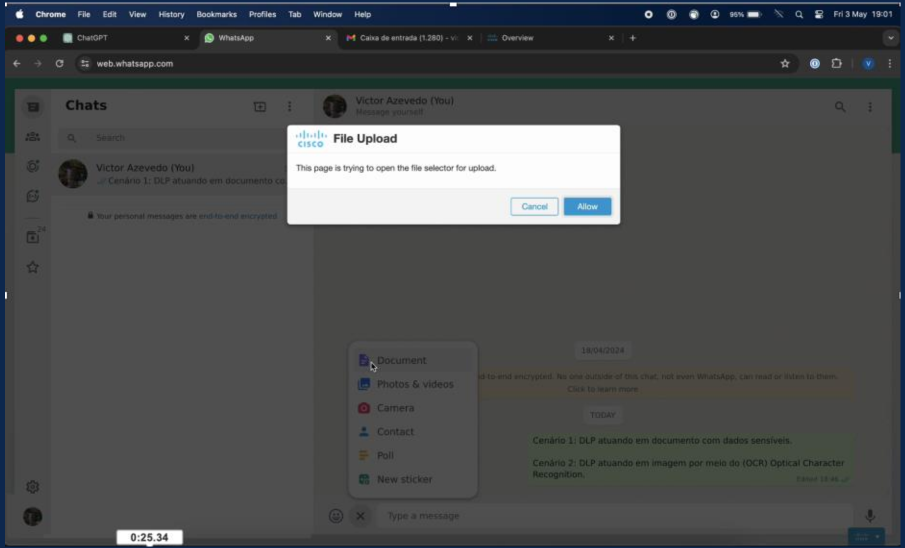
Controle de IA – Whatsapp Upload Arquivo



Cenário 1: DLP atuando em documento com dados sensíveis.

Cenário 2: DLP atuando em imagem por meio do (OCR) Optical Character Recognition.

Edited 18:46



File Upload

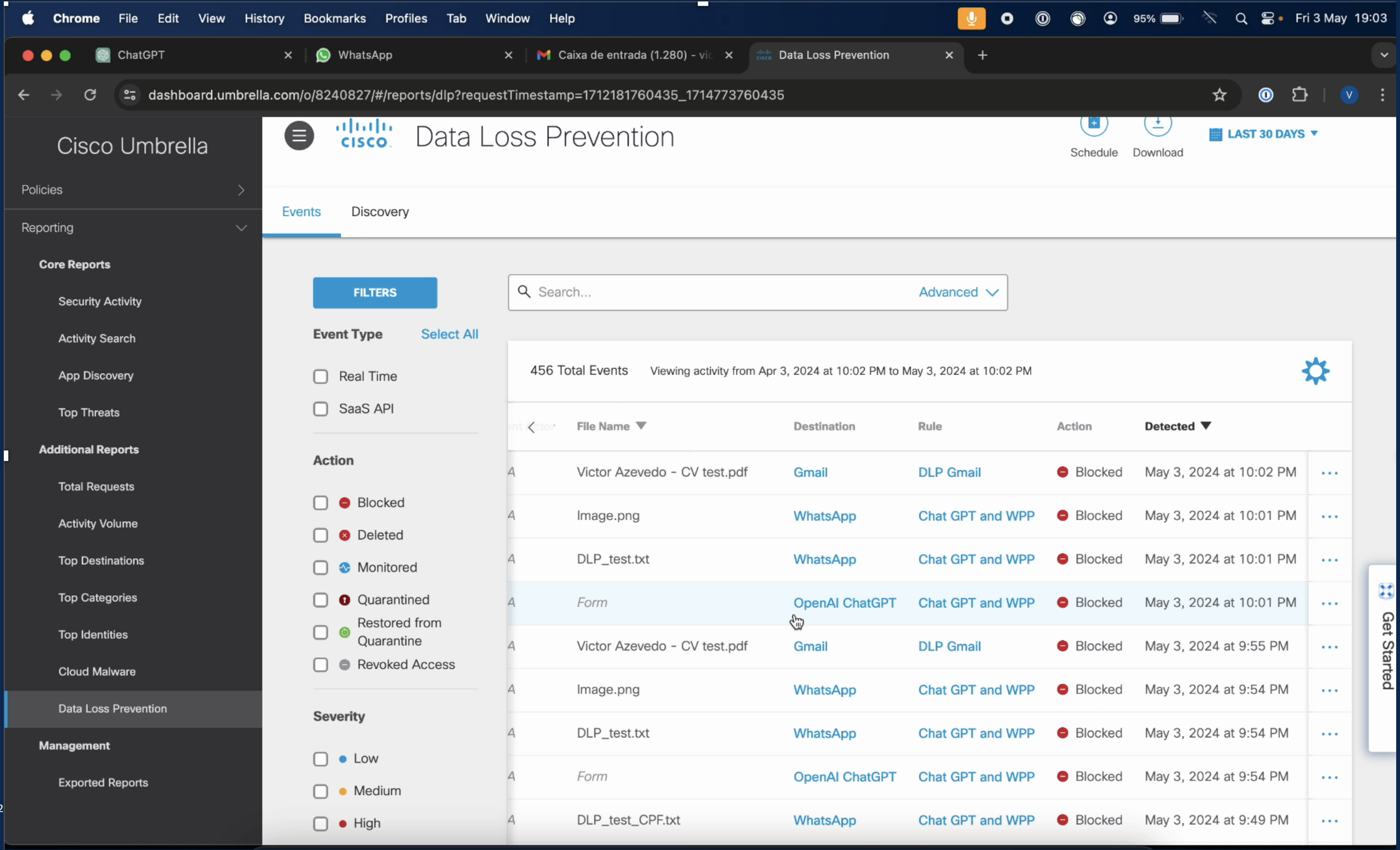
This page is trying to open the file selector for upload.

Cancel | Allow

Cenário 1: DLP atuando em documento com dados sensíveis.

Cenário 2: DLP atuando em imagem por meio do (OCR) Optical Character Recognition.

Controle de IA – Logging



Data Loss Prevention

Event Type Select All

- □ Real Time
- □ SaaS API

Action

- □ ● Blocked
- □ ☒ Deleted
- □ ● Monitored
- □ ● Quarantined
- □ ● Restored from Quarantine
- □ ● Revoked Access

Severity

- □ ● Low
- □ ● Medium
- □ ● High

456 Total Events Viewing activity from Apr 3, 2024 at 10:02 PM to May 3, 2024 at 10:02 PM

	File Name	Destination	Rule	Action	Detected
A	Victor Azevedo - CV test.pdf	Gmail	DLP Gmail	● Blocked	May 3, 2024 at 10:02 PM
A	Image.png	WhatsApp	Chat GPT and WPP	● Blocked	May 3, 2024 at 10:01 PM
A	DLP_test.txt	WhatsApp	Chat GPT and WPP	● Blocked	May 3, 2024 at 10:01 PM
A	*Form*	OpenAI ChatGPT	Chat GPT and WPP	● Blocked	May 3, 2024 at 10:01 PM
A	Victor Azevedo - CV test.pdf	Gmail	DLP Gmail	● Blocked	May 3, 2024 at 9:55 PM
A	Image.png	WhatsApp	Chat GPT and WPP	● Blocked	May 3, 2024 at 9:54 PM
A	DLP_test.txt	WhatsApp	Chat GPT and WPP	● Blocked	May 3, 2024 at 9:54 PM
A	*Form*	OpenAI ChatGPT	Chat GPT and WPP	● Blocked	May 3, 2024 at 9:54 PM
A	DLP_test_CPF.txt	WhatsApp	Chat GPT and WPP	● Blocked	May 3, 2024 at 9:49 PM

Making AI work for you.

cisco

cisco SECURE