

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Cisco Secure Email Threat Defense Workshop

Subtitle goes here

Bradley Anstis, Security Services Creation Specialist
Sergio Pinto, TME Secure Email BU
[LTRSEC-2169](#)

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

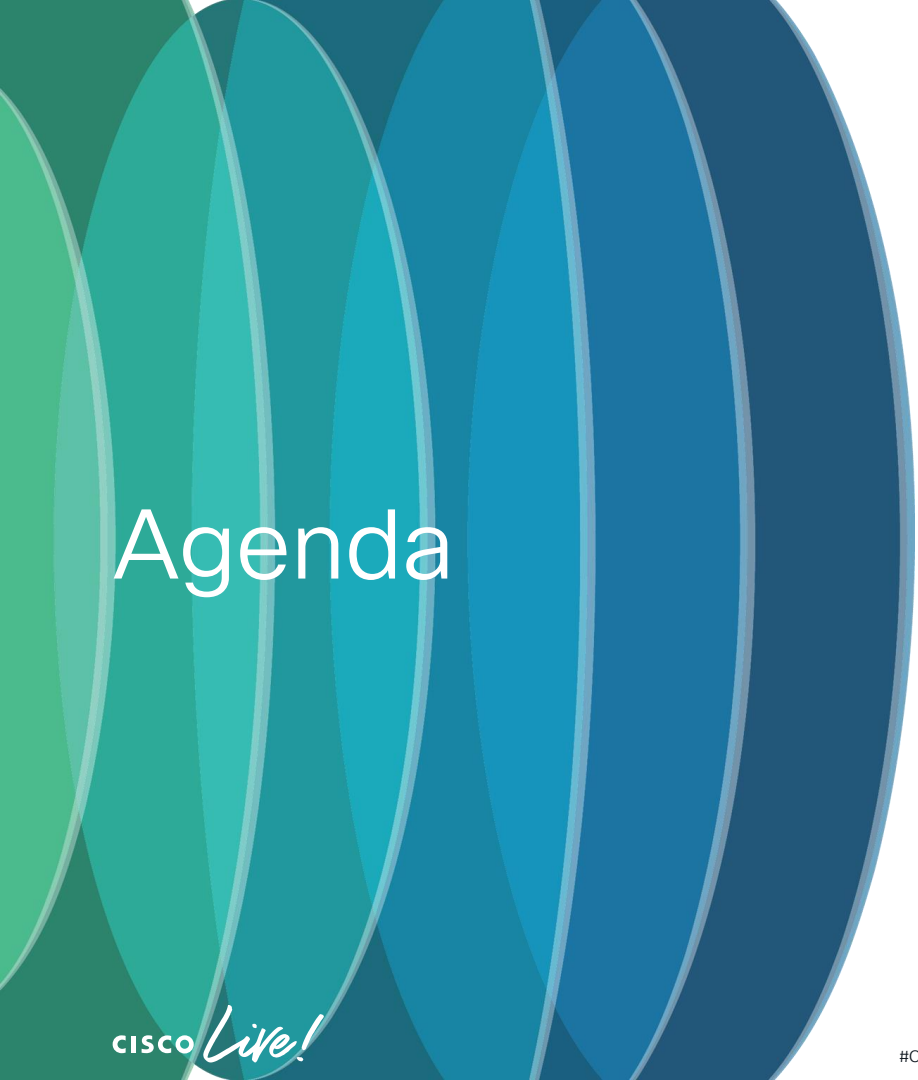
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#LTRSEC-2169>





Agenda

- Introduction
- An Introduction to Email Threat Defense
- Hands on Lab

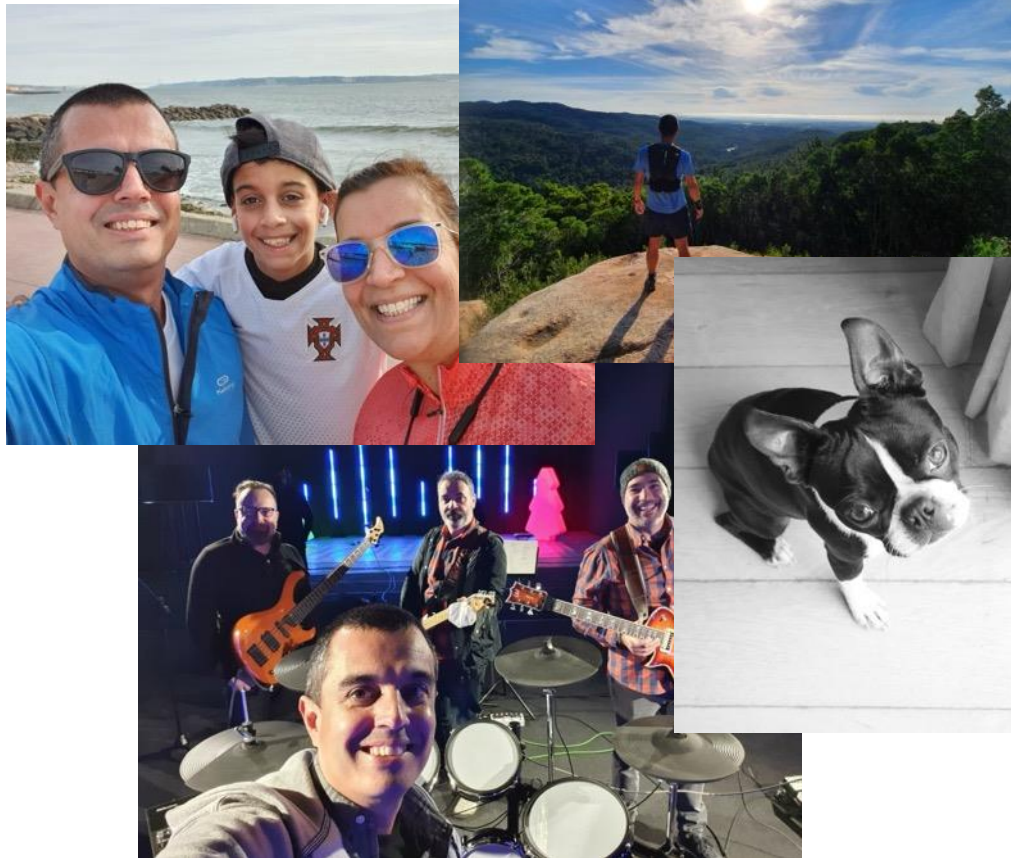
Who am I?

Sergio Pinto

TME @ Secure Email BU,
Cisco



Who am I



Secure Email Technical Marketing Engineer

Married, Father, and dog lover(recently)

17 years in Cisco across Sales and Eng

Cisco Live and External Events speaker

Sports enthusiast (Krav Maga, Running,
Padel)

Music lover (I play Guitar, Drums, and Piano)

Based out of Lisbon, Portugal

Who am I?

Bradley Anstis

Security Service Creation APJC @ GPRS,
Cisco

(Previously Email Security Specialist,
APJC @ GSSO)



Who am I



Security Service Creation Lead, APJC

Married, Father, and another dog lover...

5 years in Cisco across GSSO & GPRS

Cisco Live and External Events speaker

Crazy car guy, active motorsport competitor

Trying to keep up with my son's and their sport

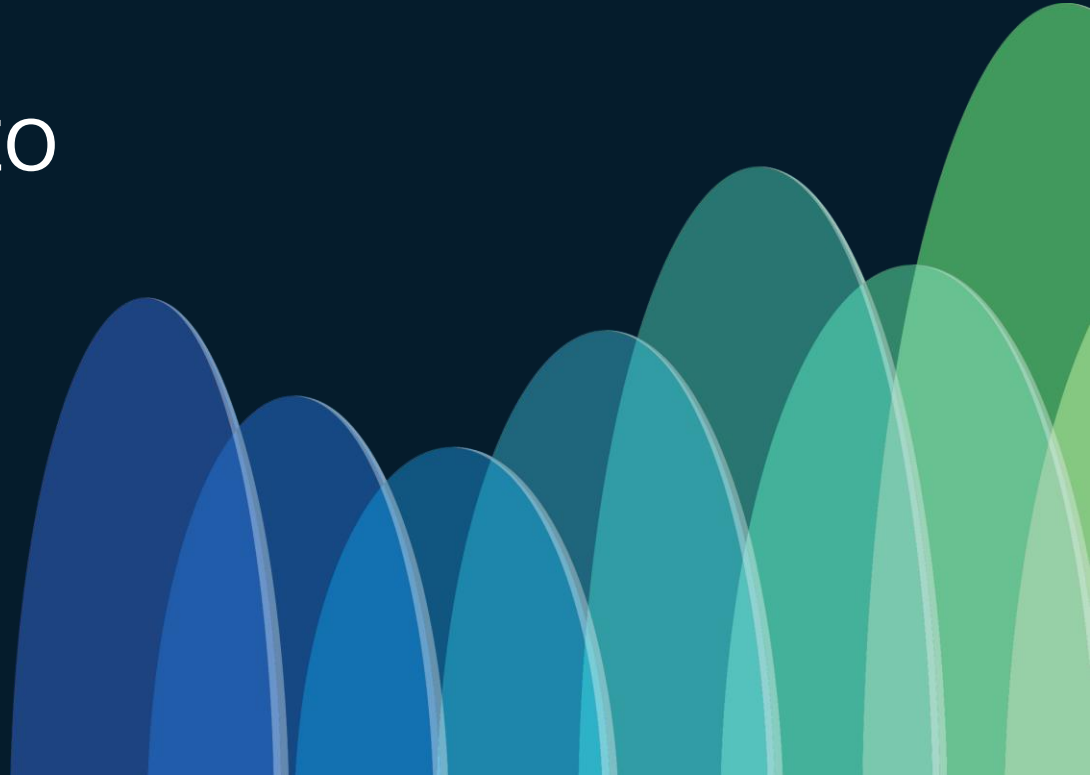
Based out of Sydney, Australia

Acknowledgments



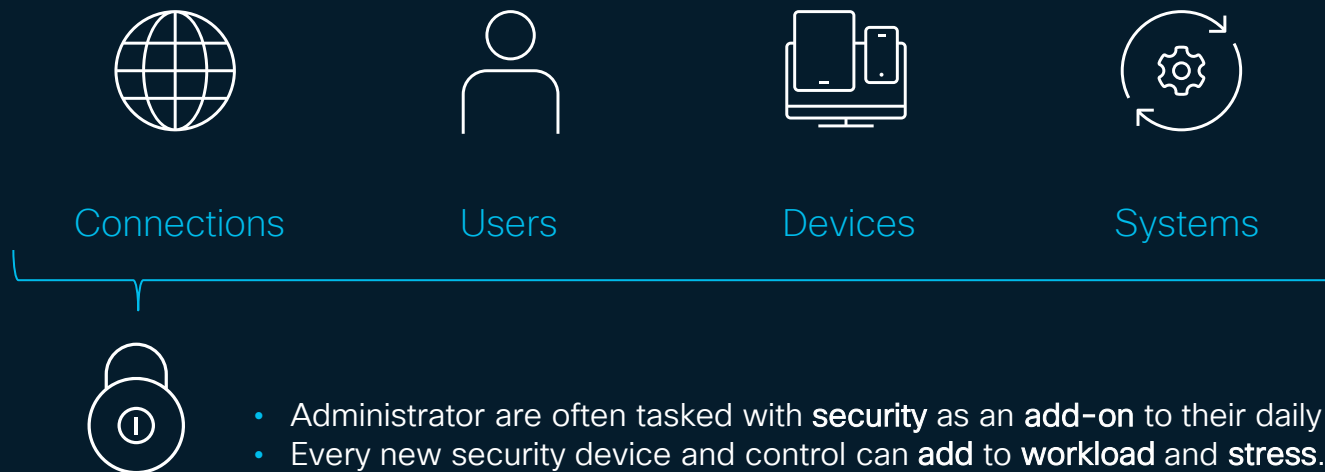
Tim Krzywonos

An Introduction to Email Threat Defense



Administrators are stretched thin

Small and mid-sized businesses are most affected



Time to Detection is key in any attack

Native MS tools are not sufficient for fast search and remediation



When a threat is reported, administrators need to quickly and easily:

- Search all messages including internal messages
- Access data from all messages with real-time reporting including lateral movement of an attack starting with patient ZERO
- Remove and isolate threats from inboxes without resorting to another tool or scripting

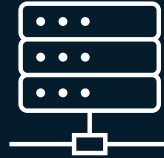
Product Overview

Cisco Secure Email Portfolio



Email Threat Defense

AI, Machine and Deep Learning
SaaS solution
Microsoft 365 and Hybrid Exchange
Incoming, outgoing, and internal
mailflow
Leverages Talos Intelligence
services



Email Gateway

Granular control
Recognized by the market
Integrates with Email Threat
Defense for additional ML/DL
scanning
Available on-prem (Virtual or
Private Cloud) or in a Cisco-
hosted instance



Secure Email Services

Cisco Security Awareness Training
Cisco Secure Email Encryption
Service
DMARC Protection and Monitoring
Red Sift (via Solutions+)
Email Archiving
Theta Lake (via Solutions+)

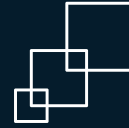
Email Threat Defense **unlocks value** for your organization



Simplicity



Visibility



Integration

Cloud-native email security platform powered by Cisco Talos

- Risk-Free Deployment
- Simple Configuration
- Point and Click Remediation
- All Messages
- Search/Triage
- Search Threat Indicators
- Talos Intelligence
- Native + MS APIs
- XDR

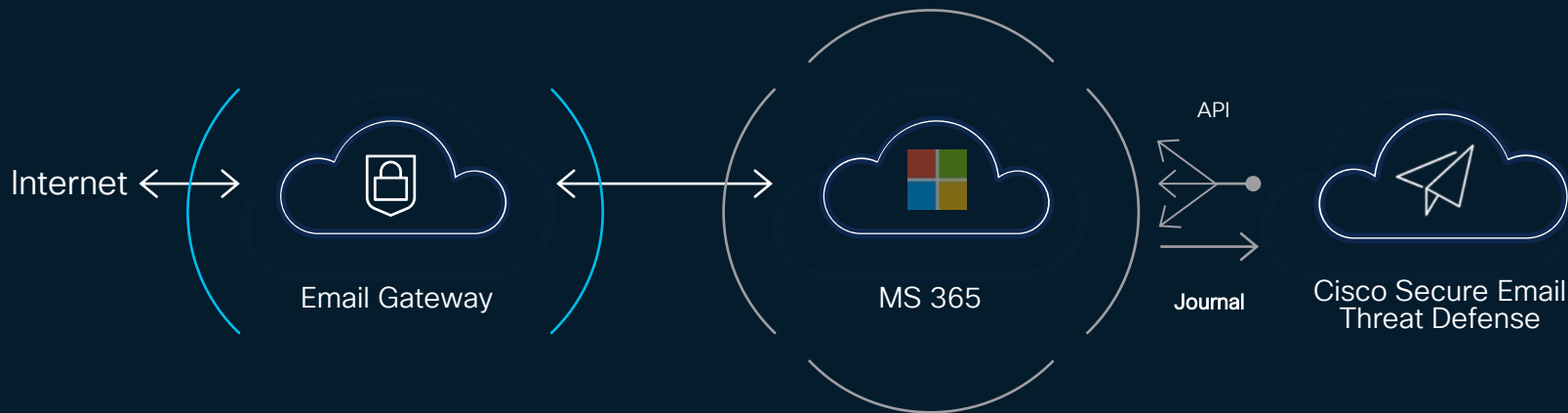
Completes Visibility & Protection for all messages

Traditional Email Gateway

Only sees **inbound** and **outbound** messages that cross the perimeter – **excludes internal**

Cisco Secure Email Threat Defense

Has complete visibility of **all messages**, including **internal**, in addition to **inbound** and **outbound** messages



Signal Generation

What are signals and how do they lead to a conviction



The final verdict is then given
by aggregating the signals

Full Email Analysis – Always on, all inclusive

Type	Engine
Header Analysis (IP, Domain, Sender)	<ul style="list-style-type: none">• Sender IP Reputation• Sender Domain Reputation
File Analysis	<ul style="list-style-type: none">• Advanced Malware Reputation• Secure Malware Analytics File Analysis
URL Analysis	<ul style="list-style-type: none">• URL Reputation• Cloud URL Analysis (crawling)
Content Analysis (Potentially Unwanted)	<ul style="list-style-type: none">• Anti-Spam & Graymail
Context Analysis (Threat)	<ul style="list-style-type: none">• BEC / Scam (Giftcard, Wire Transfer, QR Code, other)• Phishing (URL and no payload)• Artificial Intelligence• Machine Learning• Natural Language Understanding

Use-case example

A phishing link has been reported by a user

Common Scenario:

What do I want to know?

Who else received
this link?



From **additional senders**?
With the **same subject**?

What do I want to do?

Remove the link
from all inboxes



Regardless of **sender**
Regardless of **subject**

A phishing link has been reported by a user

Microsoft workflow

Message Trace query

- Cannot search by subject, URL, IP Address SHA 256
- Slow to return results
- Generates a report only

Cannot take any action from the results

- Writing a PowerShell script is the next step to remediate.

New message trace

Find all messages or find specific messages sent by senders and/or recipients. Refine further by selecting a date range or adjusting the advanced settings.

Senders

All

Recipients

All

Time range (UTC-05:00)

Last 2 day(s)

[Custom time range](#)

Detailed search options

Report type

All reports include essential information with more detailed reporting in the Enhanced and Extended report, which are only downloadable.

☒ Summary report
Instant online access

☐ Enhanced summary report
Downloadable CSV file only

☐ Extended report
Downloadable CSV file only

Total time is in minutes or hours

A phishing link has been reported by a user

Email Threat Defense workflow

Search for **any message detail**

- Sender, Recipient, URL, etc.
- Rapid results in seconds



Select and remediate **instantly**

- One or multiple messages at once
- Actions taken directly from the results



Total time is in seconds

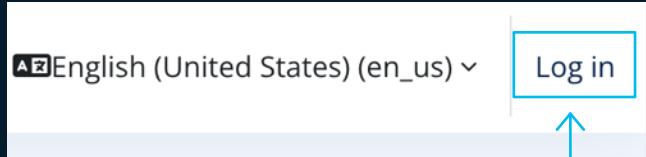
Hands on Lab



Accessing the Lab

Sign-up time!

<http://www.ciscosecurityworkshop.com>



1 Log in (upper right-hand corner)

2 Create new account

Sign-up time!

<http://www.ciscosecurityworkshop.com>

3

Enter info, including enrollment key

EmailCLMeI2024!



(case-sensitive)

New account

Username ⓘ

The password must have at least 8 characters, at least 1 digit(s), at least 1 lower case letter(s), at least 1 upper case letter(s), at least 1 special character(s) such as *, -, or #

Password ⓘ

Enrollment key ⓘ

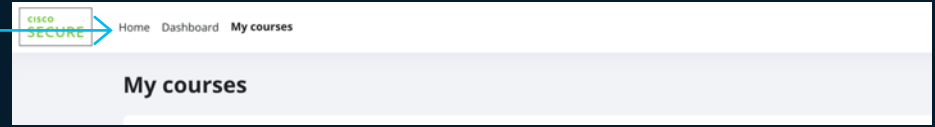
Email address ⓘ

Email (again) ⓘ

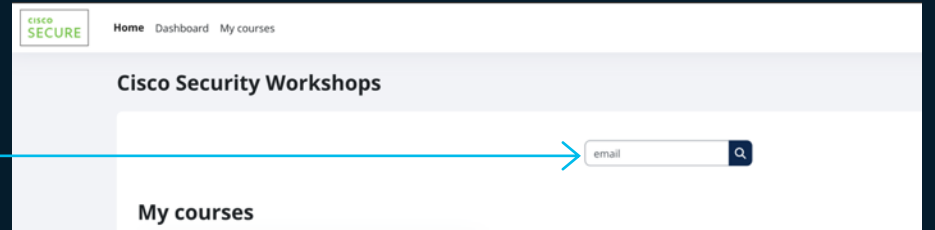
First name ⓘ

Existing Accounts

1 Click Home



2 Search for "email"



3 Click on the ETD Workshop and enter enrolment key



Session Details

dCloud session: <https://dcloud2-rtp.cisco.com/event/405317/access>

Workshop URL: <https://www.ciscosecurityworkshop.com/>

Enrollment key: EmailCLMel2024!



(case-sensitive)

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC