

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors: yellow, orange, red, and then various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive

Cisco Webex App

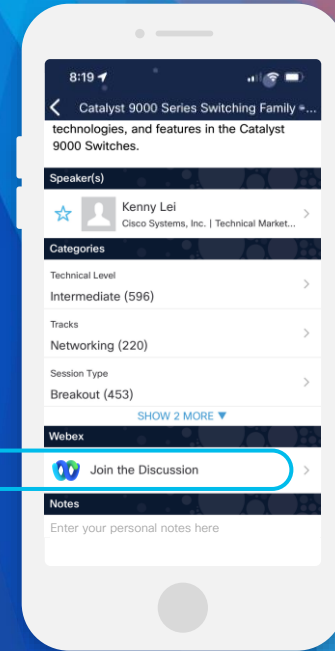
Questions?

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 June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#PSOSEC-1007>




The bridge to possible

Cisco XDR

Simplify Your Security Operations

Sana Yousuf
Product Marketing Leader

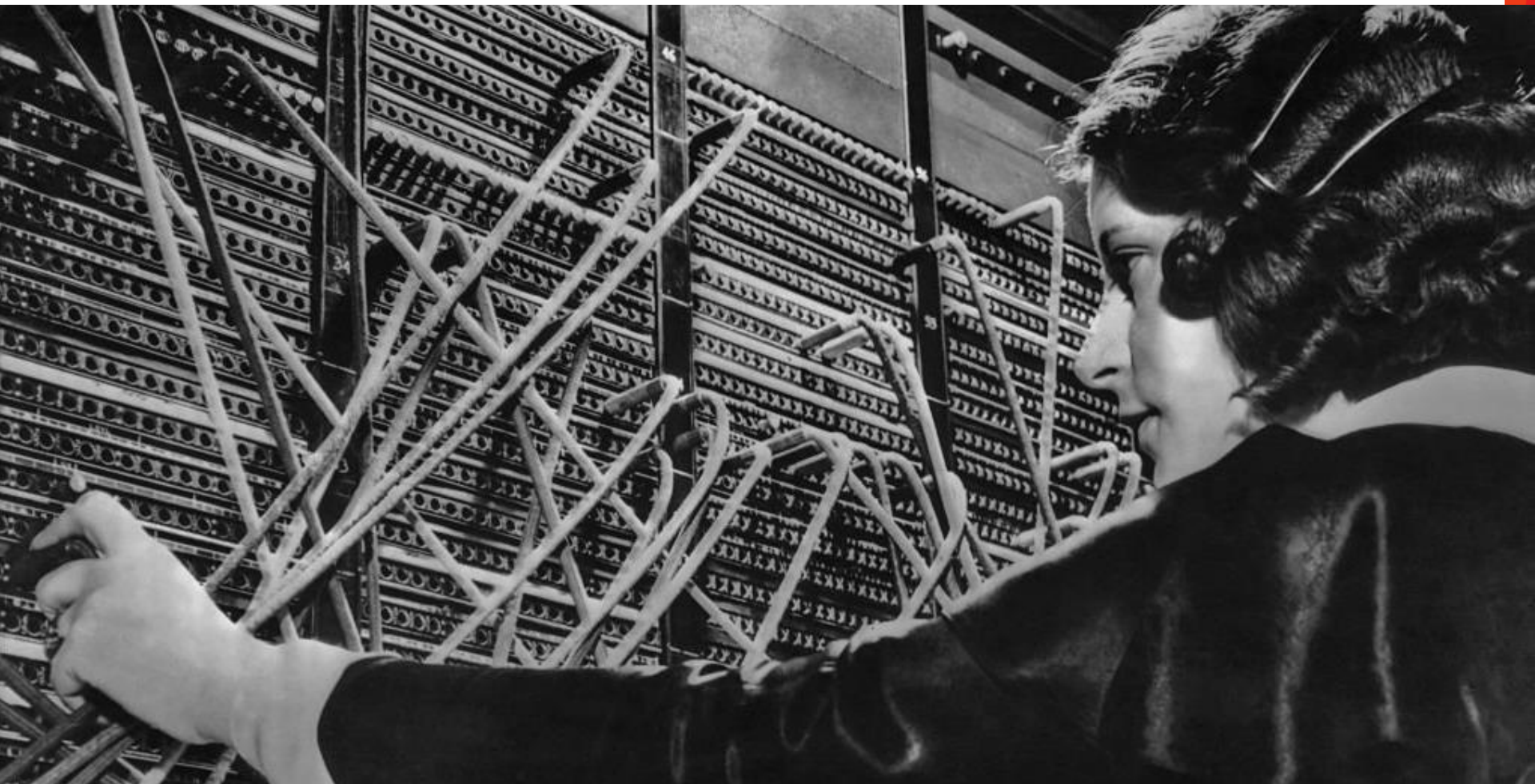
 [sana-yousuf-m/](#)

Session ID PSOSEC-1007

CISCO *Live!*


#CiscoLive







How we see
ourselves



How an adversary sees us

In a hybrid, multi-vendor, multi-vector universe

Everyone is
an insider

+30%

of all incidents
involved stolen
credentials or
malicious insiders

Attacks start
from anywhere

45%

of breaches occurred
in the cloud, and 19%
due to a compromise
at a business partner

Alert fatigue
is worse

37%

of IT and SecOps pros
say swelling alert
volume, complexity
increases job difficulty

Expanding
attack surface

22%

increase in the
average cost of a data
breach where hybrid
work was a factor

Tactics, Techniques and Procedures (TTPs) impacting nation states



Are everyone's
problem now



Once identifiable lures...

☑ bad grammar ☑ typos

Subject: "URGENT REPLY NEEDED"
From: princeofnigeria@zmail.com
To: majorie@hmail.com
DEAR FRIEND,
HAPPY NEW YEAR.
I KNOW THAT THIS MESSAGE WILL COME TO YOU AS A
SURPRISE.
I AM THE NEXT HEIR TO THE THRONE IN NIGERIA, THE CROWN
PRINCE, APARA KACHINPOPGORN. I HOPED THAT YOU WILL NOT
EXPOSE OR BETRAY THIS TRUST AND CONFIDENT THAT I AM
ABOUT TO REPOSE ON YOU FOR THE MUTUAL BENEFIT OF OUR
FAMILIES.

...are now indistinguishable

K

Describe an email using emotional tone, imagery, and language of a poor man, whose family suffered a tragic loss. Their father died in a car accident. The family was poor, destitute and in need of help. Joe offered to help, but Joe, your best friend, is no longer available. Write a convincing ad asking for a small donation



Dear friends and family,



I am writing to you with a heavy heart and a deep sense of grief. My family has suffered a tragic loss - my father was taken from us in a car accident just a few days ago. We are poor, destitute and in need of help.

As you may know, my best friend Joe has always been there for me and my family in times of need. He has always been willing to lend a helping hand and offer his support. Unfortunately, Joe is no longer with us and we are left to face this difficult time on our own.

I am reaching out to you today to ask for a small donation to help my family get through this tough time. Any amount, no matter how small, would be greatly appreciated. We are struggling to pay for basic necessities and the cost of my father's funeral is overwhelming.

I know that times are tough for everyone right now, but if you are able to spare anything, please consider making a donation to my family. Your kindness and generosity would mean the world to us and help us get through this difficult time.

Thank you for your understanding and support.

Sincerely,
[Your name]

Only an effective XDR solution can adapt to the changing nature of the threat



Security tools need to focus on the attacker



Turn potential false positives into validated incidents



Focus on initial compromise, lateral movement, privilege escalation and data exfiltration

The XDR promise



Collection of telemetry
from multiple security tools



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



Response and remediation
of that maliciousness





Adversary: Turla



// Nicknames

Snake

Venomous Bear

Uroburos

Group 88

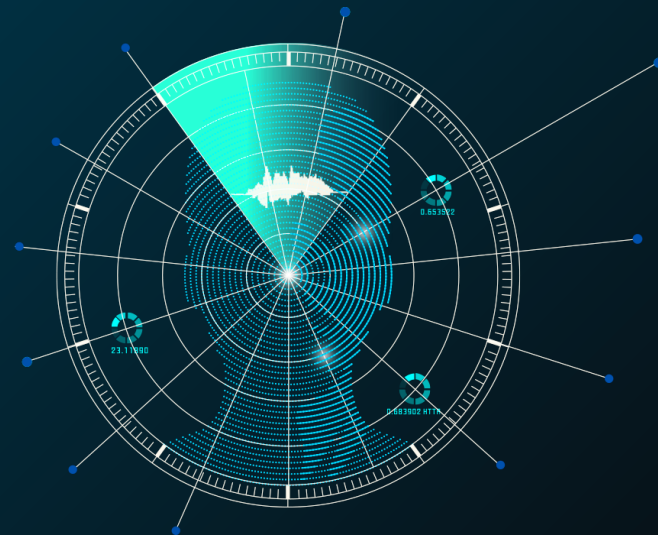
Waterbug

The adversary: What do we know?

- Estonian intelligence services associate this group with the Russian federal security service (FSB).
- Does NOT **deploy advanced tools unless necessary** to compromise the target

Method:

- Prefers watering holes and social engineering to manipulate victims
- Crafted lures are highly tailored to their targets
- Exploit themes related to current events
- First-stage malware typically acts as a filter











Without XDR, how can we detect and respond to all of this?

TA0001: Initial Access		TA0002: Execution		TA0003: Persistence		TA0004: Privilege Escalation		TA0005: Defense Evasion		TA0006: Credential Access	
T1189: Drive-by Compromise		T1059: Command and Scripting Interpreter		T10598: Account Manipulation		T1548.001: Abuse Elevation Control Mechanism		T1548.002: Bypass User Account Control		T11557: Adversary-in-the-Middle	
T1190: Exploit Public-Facing Application		T1203: Exploitation for Client Execution		T1197: BITS Jobs		T1134: Access Token Manipulation		T1548.001: Setuid and Setgid		T1110: Weak Proxy	T1110.004: Credential Stuffing
T1133: External Remote Services		T1559: Inter-Process Communication		T1547: Boot or Logon Autostart Execution		T1037: Boot or Logon Autostart Execution		T1548.003: Sudo and Sudo Caching		T1110.002: Password Cracking	T1110.001: Password Guessing
T1200: Hardware Additions		T1106: Native API		T1037: Boot or Logon Initialization Scripts		T1037.001: Network Logon Script		T1134: Access Token Manipulation		T1134.001: Create Process with Token	T1134.002: Create Process with Token
T1566: Phishing	T1566.001: Spearphishing Attachment	T1053: Scheduled Task/Job		T1176: Browser Extensions		T1037.004: .NET Scripts		T1134.002: Parent PID Spoofing		T1134.003: Parent PID Spoofing	T11555.001: Credentials from Browser
	T1566.002: Spearphishing Link	T1129: Shared Modules		T1154: Compromise Client Software Binaries		T1543.002: Systemd Service		T1134.003: SID History Injection		T1134.004: Token Impersonation/Theft	T11555.002: Credentials from Browser
	T1566.003: Spearphishing via Service	T1072: Software Deployment Tools		T1136: Create Account		T1548.003: Windows Service		T1197: BITS Jobs		T1212: Exploitation for Credential Access	T11555.003: Password Managers
T1091: Replication Through Removable Media		T1569: System Services		T1136: Create Account		T1484: Domain Policy Modification		T1612: Debugger Evasion		T1187: Forced Authentication	T11555.004: Windows Credential Manager
T1195: Supply Chain Compromise		T1204: User Execution		T1543: Create or Modify System Process		T1613: Escape to Host		T1612: Debugger Evasion		T1187: Forced Authentication	
T1199: Trusted Relationship		T1047: Windows Management Instrumentation		T1546: Event Triggered Execution		T1546.001: Application Shim		T1006: Domain Policy Modification		T1606: Forge Web Credentials	
T1078: Valid Accounts	T1078.001: Default Accounts			T1133: External Remote Services		T1546.002: Accessibility Features		T1480: Execution Guardrails		T1056: Input Capture	T1056.004: Credential API Hooking
	T1078.002: Domain Accounts			T1574: Hijack Execution Flow		T1546.003: AppCert DLLs		T1221: Exploitation for Defense Evasion		T1056.002: GUI Input Capture	T1056.001: Keylogging
	T1078.003: Local Accounts			T1556: Modify Authentication Process		T1546.004: Applet DLLs		T1222: File and Directory Permissions Manipulation		T1056.003: Web Portal Capture	
				T1137: Office Application Startup		T1546.001: Application Shim					
				T1542: Pre-OS Boot		T1546.002: Change Default File Association					
				T1053: Scheduled Task/Job		T1546.003: Component Object Model					
				T1055: Server Software Component		T1546.002: Image File Execution Options					
				T1205: Traffic Signaling		T1546.007: Netsh Helper DLL					
				T1078: Valid Accounts		T1546.001: PowerShell Profile					
						T1546.002: Screensaver					
						T1546.003: Trap					
						T1546.004: User Shell Configuration Modification					
						T1566.003: Windows Management Instrumentation					
						T1068: Exploitation for Privilege Escalation					
						T1574: Hijack Execution Flow					
						T1574.012: CDR, PROFLER					
						T1574.001: DLL Search Order Hijacking					
						T1574.002: DLL Side-Loading					
						T1574.003: Dynamic Linker Hijacking					
						T1574.004: Executable Installer File Permissions					
						T1574.001: KernelCallback Table					
						T1574.002: Path Interception by PATH Environment Variable					
						T1574.003: Path Interception by PATH Environment Variable					
						T1574.004: Path Interception by PATH Environment Variable					
						T1574.005: Path Interception by PATH Environment Variable					
						T1574.006: Path Interception by PATH Environment Variable					
						T1574.007: Path Interception by PATH Environment Variable					
						T1574.008: Path Interception by PATH Environment Variable					
						T1574.009: Path Interception by PATH Environment Variable					
						T1574.010: Path Interception by PATH Environment Variable					
						T1574.011: Path Interception by PATH Environment Variable					
						T1574.012: Path Interception by PATH Environment Variable					
						T1574.013: Path Interception by PATH Environment Variable					
						T1574.014: Path Interception by PATH Environment Variable					
						T1574.015: Path Interception by PATH Environment Variable					
						T1574.016: Path Interception by PATH Environment Variable					
						T1574.017: Path Interception by PATH Environment Variable					
						T1574.018: Path Interception by PATH Environment Variable					
						T1574.019: Path Interception by PATH Environment Variable					
						T1574.020: Path Interception by PATH Environment Variable					
						T1574.021: Path Interception by PATH Environment Variable					
						T1574.022: Path Interception by PATH Environment Variable					
						T1574.023: Path Interception by PATH Environment Variable					
						T1574.024: Path Interception by PATH Environment Variable					
						T1574.025: Path Interception by PATH Environment Variable					
						T1574.026: Path Interception by PATH Environment Variable					
						T1574.027: Path Interception by PATH Environment Variable					
						T1574.028: Path Interception by PATH Environment Variable					
						T1574.029: Path Interception by PATH Environment Variable					
						T1574.030: Path Interception by PATH Environment Variable					
						T1574.031: Path Interception by PATH Environment Variable					
						T1574.032: Path Interception by PATH Environment Variable					
						T1574.033: Path Interception by PATH Environment Variable					
						T1574.034: Path Interception by PATH Environment Variable					
						T1574.035: Path Interception by PATH Environment Variable					
						T1574.036: Path Interception by PATH Environment Variable					
						T1574.037: Path Interception by PATH Environment Variable					
						T1574.038: Path Interception by PATH Environment Variable					
						T1574.039: Path Interception by PATH Environment Variable					
						T1574.040: Path Interception by PATH Environment Variable					
						T1574.041: Path Interception by PATH Environment Variable					
						T1574.042: Path Interception by PATH Environment Variable					
						T1574.043: Path Interception by PATH Environment Variable					
						T1574.044: Path Interception by PATH Environment Variable					
						T1574.045: Path Interception by PATH Environment Variable					
						T1574.046: Path Interception by PATH Environment Variable					
						T1574.047: Path Interception by PATH Environment Variable					
						T1574.048: Path Interception by PATH Environment Variable					
						T1574.049: Path Interception by PATH Environment Variable					
						T1574.050: Path Interception by PATH Environment Variable					
						T1574.051: Path Interception by PATH Environment Variable					
						T1574.052: Path Interception by PATH Environment Variable					
						T1574.053: Path Interception by PATH Environment Variable					
						T1574.054: Path Interception by PATH Environment Variable					
						T1574.055: Path Interception by PATH Environment Variable					
						T1574.056: Path Interception by PATH Environment Variable					
						T1574.057: Path Interception by PATH Environment Variable					
						T1574.058: Path Interception by PATH Environment Variable					
						T1574.059: Path Interception by PATH Environment Variable					
						T1574.060: Path Interception by PATH Environment Variable					
						T1574.061: Path Interception by PATH Environment Variable					
						T1574.062: Path Interception by PATH Environment Variable					
						T1574.063: Path Interception by PATH Environment Variable					
						T1574.064: Path Interception by PATH Environment Variable					
						T1574.065: Path Interception by PATH Environment Variable					
						T1574.066: Path Interception by PATH Environment Variable					
						T1574.067: Path Interception by PATH Environment Variable					
						T1574.068: Path Interception by PATH Environment Variable					
						T1574.069: Path Interception by PATH Environment Variable					
						T1574.070: Path Interception by PATH Environment Variable					
						T1574.071: Path Interception by PATH Environment Variable					
						T1574.072: Path Interception by PATH Environment Variable					
						T1574.073: Path Interception by PATH Environment Variable					
						T1574.074: Path Interception by PATH Environment Variable					
						T1574.075: Path Interception by PATH Environment Variable					
						T1574.076: Path Interception by PATH Environment Variable					
						T1574.077: Path Interception by PATH Environment Variable					
						T1574.078: Path Interception by PATH Environment Variable					
						T1574.079: Path Interception by PATH Environment Variable					
						T1574.080: Path Interception by PATH Environment Variable					
						T1574.081: Path Interception by PATH Environment Variable					
						T1574.082: Path Interception by PATH Environment Variable					
						T1574.083: Path Interception by PATH Environment Variable					
						T1574.084: Path Interception by PATH Environment Variable					
						T1574.085: Path Interception by PATH Environment Variable					
						T1574.086: Path Interception by PATH Environment Variable					
						T1574.087: Path Interception by PATH Environment Variable					
						T1574.088: Path Interception by PATH Environment Variable					
						T1574.089: Path Interception by PATH Environment Variable					
						T1574.090: Path Interception by PATH Environment Variable					
						T1574.091: Path Interception by PATH Environment Variable					
						T1574.092: Path Interception by PATH Environment Variable					
						T1574.093: Path Interception by PATH Environment Variable					
						T1574.094: Path Interception by PATH Environment Variable					
						T1574.095: Path Interception by PATH Environment Variable					
						T1574.096: Path Interception by PATH Environment Variable					
						T1574.097: Path Interception by PATH Environment Variable					
						T1574.098: Path Interception by PATH Environment Variable					
						T1574.099: Path Interception by PATH Environment Variable					
						T1574.100: Path Interception by PATH Environment Variable					
						T1574.101: Path Interception by PATH Environment Variable					
						T1574.102: Path Interception by PATH Environment Variable					
						T1574.103: Path Interception by PATH Environment Variable					
						T1574.104: Path Interception by PATH Environment Variable					
						T1574.105: Path Interception by PATH Environment Variable					
						T1574.106: Path Interception by PATH Environment Variable					
						T1574.107: Path Interception by PATH Environment Variable					
						T1574.108: Path Interception by PATH Environment Variable					
						T1574.109: Path Interception by PATH Environment Variable					
						T1574.110: Path Interception by PATH Environment Variable					
						T1574.111: Path Interception by PATH Environment Variable					
						T1574.112: Path Interception by PATH Environment Variable					
						T1574.113: Path Interception by PATH Environment Variable					
						T1574.114: Path Interception by PATH Environment Variable					
						T1574.115: Path Interception by PATH Environment Variable					
						T1574.116: Path Interception by PATH Environment Variable					
						T1574.117: Path Interception by PATH Environment Variable					
						T1574.118: Path Interception by PATH Environment Variable					
						T1574.119: Path Interception by PATH Environment Variable					
						T1574.120: Path Interception by PATH Environment Variable					
						T1574.121: Path Interception by PATH Environment Variable					
						T1574.122: Path Interception by PATH Environment Variable					
						T1574.123: Path Interception by PATH Environment Variable					
						T1574.124: Path Interception by PATH Environment Variable					
						T1574.125: Path Interception by PATH Environment Variable					
						T1574.126: Path Interception by PATH Environment Variable					
						T1574.127: Path Interception by PATH Environment Variable					
						T1574.128: Path Interception by PATH Environment Variable					
						T1574.129: Path Interception by PATH Environment Variable					
						T1574.130: Path Interception by PATH Environment Variable					
						T1574.131: Path Interception by PATH Environment Variable					
						T1574.132: Path Interception by PATH Environment Variable					
						T1574.133: Path Interception by PATH Environment Variable					
						T1574.134: Path Interception by PATH Environment Variable					
						T1574.135: Path Interception by PATH Environment Variable					
						T1574.136: Path Interception by PATH Environment Variable					
						T1574.137: Path Interception by PATH Environment Variable					

Telemetry data source importance

The top six data sources that customers believe are essential for an XDR are
Endpoint, Network, Firewall, Identity, Email, and DNS

Essential		
	Count	Share
 Endpoint	255	85.0%
 Network	226	75.3%
 Firewall	207	69.0%
 Identity	191	63.7%
 Email	179	59.7%
 DNS	140	46.7%
 Public Cloud	137	45.7%
 Non-Security Sources	36	12.0%



Cisco Secure
Client



Cisco / Meraki
(Networking)



Firewall Threat
Defense (FTD)



Duo

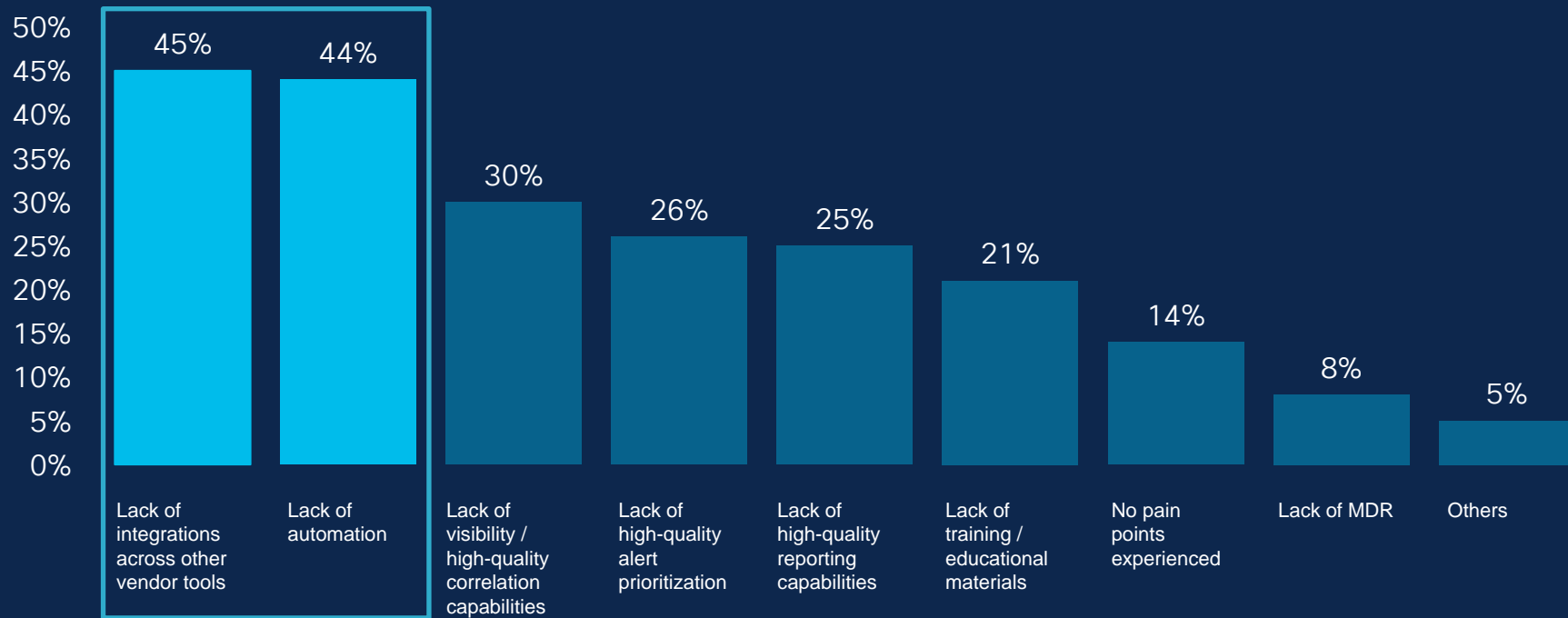


Email Threat
Defense (ETD)

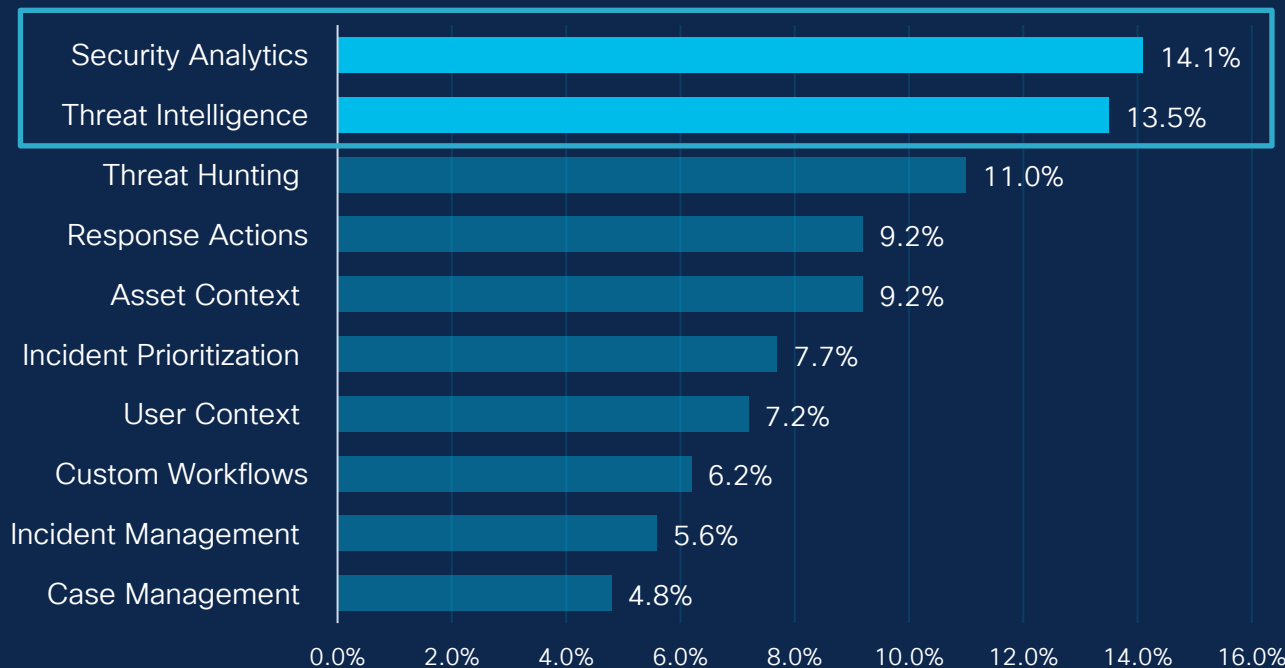


Umbrella

Lack of integration and automation are the most widespread pain points for existing XDR solutions



Security Analytics and Threat Intelligence are the top two features by revealed preferences among the overall sample



N+307 Total
Respondents

44 Fortune 500
Respondents

106 Global 2000
Respondents

Stop advanced threats like ransomware

Most attacks use a sequence like this...



Email



DNS



010110
110010
001011

A well-tailored and personalized email causes a user to click...

Which goes to a questionable web site...

Which leads to a strange process being created locally on the user's device...

That process will connect to another machine or directly to their data

T1055: Process Injection

T1566: Spear phishing

T1189: Drive-by Compromise

T1570: Lateral Tool Transfer

T1087: Account Discovery: Domain Account

T1048: System Network Connections Discovery

Vendor A

Vendor C

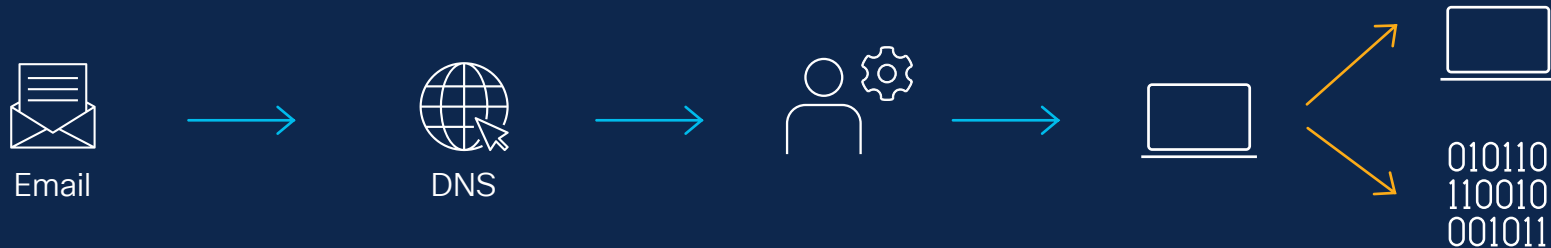
Vendor E

Vendor G

Vendor D

Anatomy of a real attack (Turla)

Most attacks use a sequence like this...



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



Built on the Cisco Security Cloud platform

Simplify with Cisco XDR



The Cisco approach to XDR

Detect more, act faster, elevate productivity, build resilience

Detect
the most
sophisticated
threats



- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimized for multi-vendor environments

Act on
what truly
matters, faster



- Prioritize threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations

Elevate
productivity



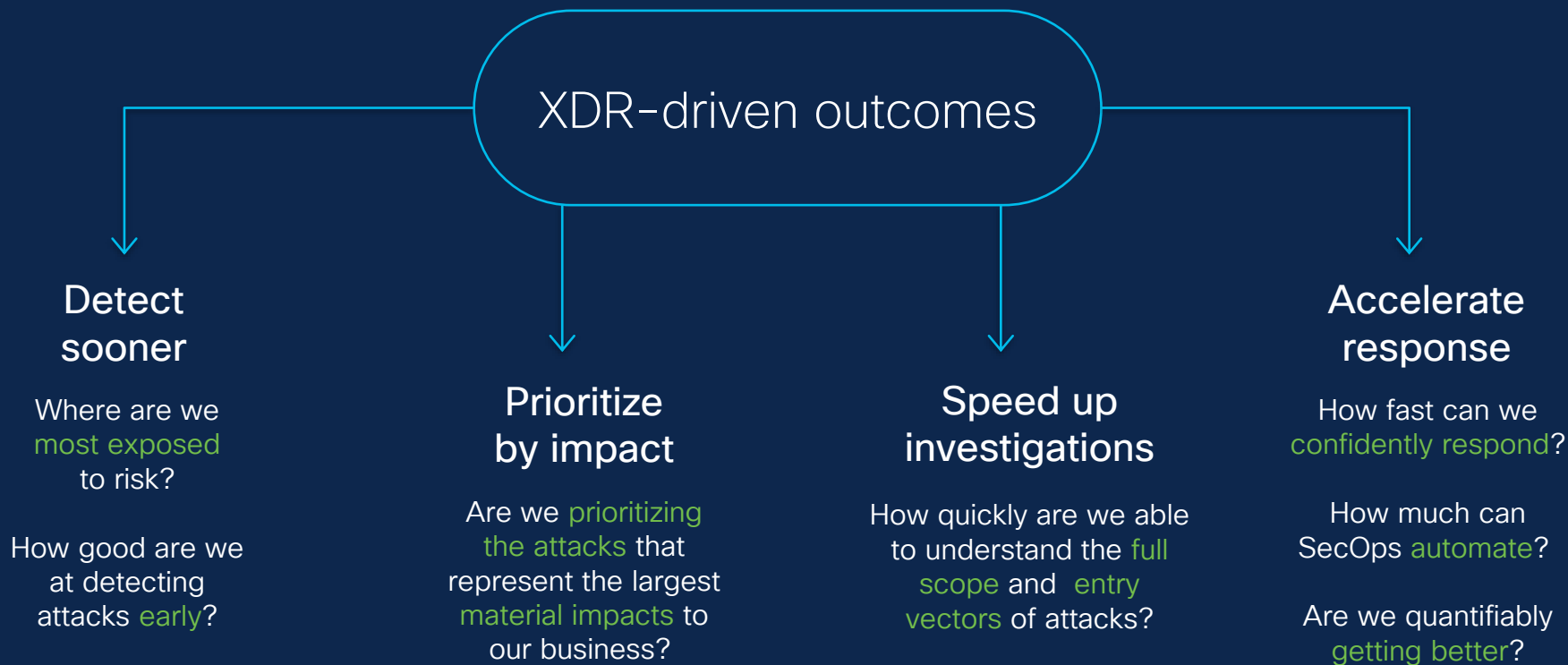
- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks

Build
resilience

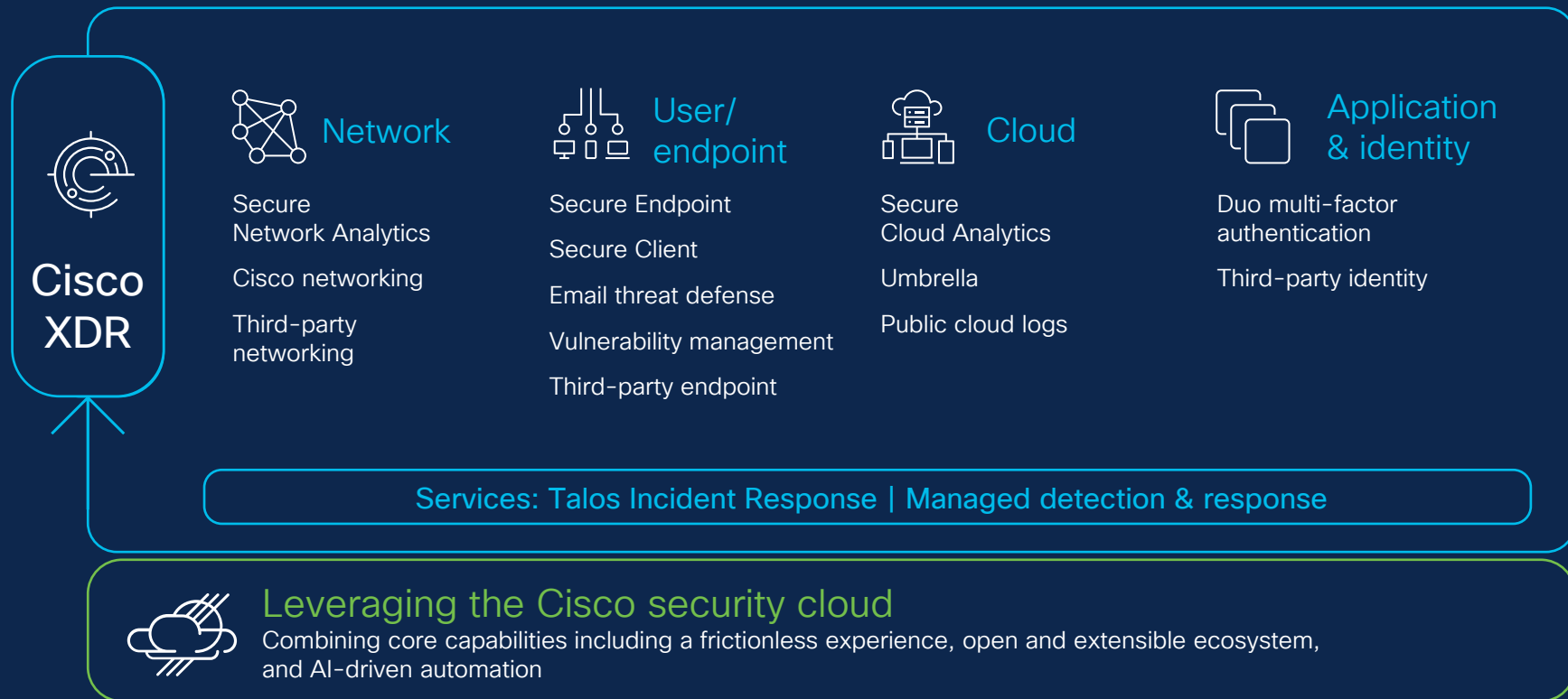


- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, everyday with continuous, quantifiable improvement

Shift the focus to outcomes



Delivering XDR to meet you where you are



Quickly position teams to achieve incremental XDR milestones

Integrate

Consolidate solutions and technology with an integrated platform



Orchestrate

Enable prioritized detection and response using AI & ML



Optimize

Evolve, and fine tune security by proactively executing against that baseline



Unify

Build an ecosystem that aggregates, enriches data and telemetry from all part of your environment



Automate

Automate detection and response workflows that require minimal human intervention



Easy to buy tiers for Cisco XDR

Cisco XDR
Essentials

Full Featured
XDR

Cisco XDR
Advantage

Full Featured
XDR

+Third-Party Telemetry

Cisco XDR
Premier

Full Featured
XDR

+Third-Party Telemetry

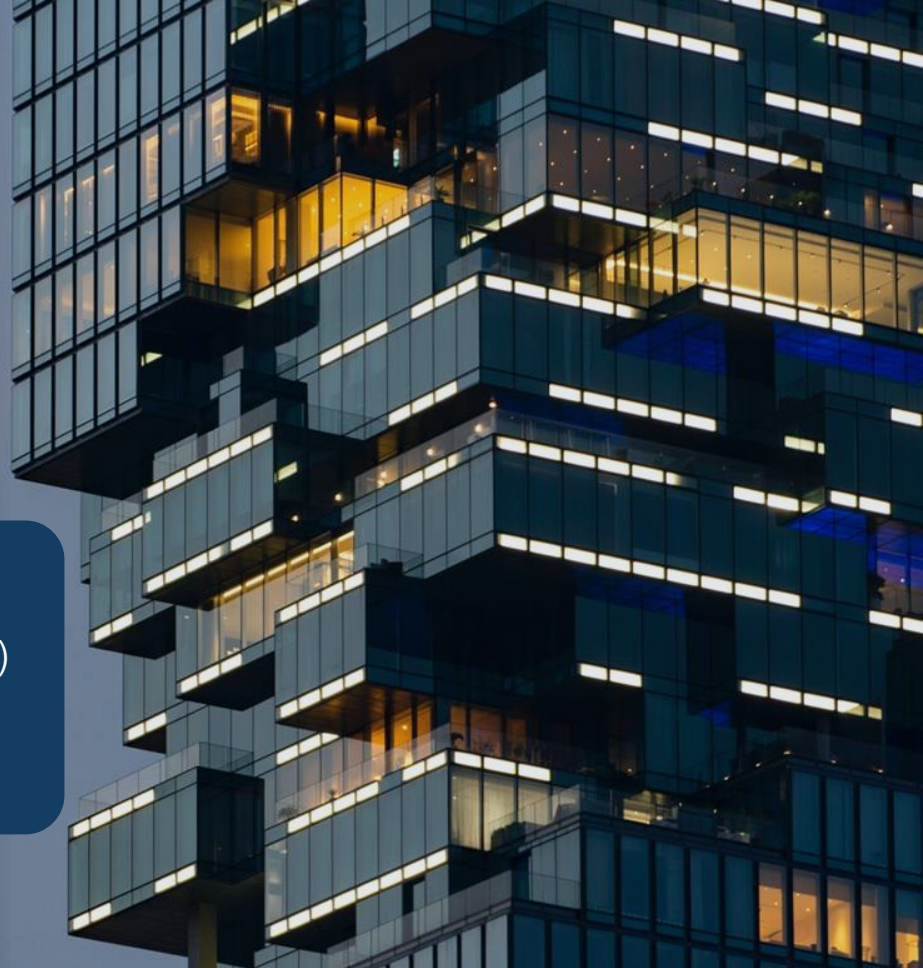
+Managed Services

Take the Attack to the Attackers

Learn more at cisco.com/go/xdr

Come check out Cisco XDR

- 'The Brew Pub' at the 'World of Solution' (#2421)
- Security zone of the [Cisco Showcase](#)
- Sign up to [meet an expert](#)



Discover how security services accelerate outcomes

CX delivers the outcomes that matter most, faster. We optimize for emerging security challenges, activate threat visibility, and provide rapid incident response.



Visit CX Security
to learn more

How we can help

- Secure cloud
- Secure datacenter
- Zero Trust Networking
- DevSecOps
- Secure Range
- Security Reference Architecture
- SecureX Automation
- Secure Access Service Edge (SASE)
- Incident Response
- Learning
- Certifications

You don't have to do it alone.

For more insight, visit the Cisco CX Booth (#3310) in the World of Solutions for Lightning Talks and Demos

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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

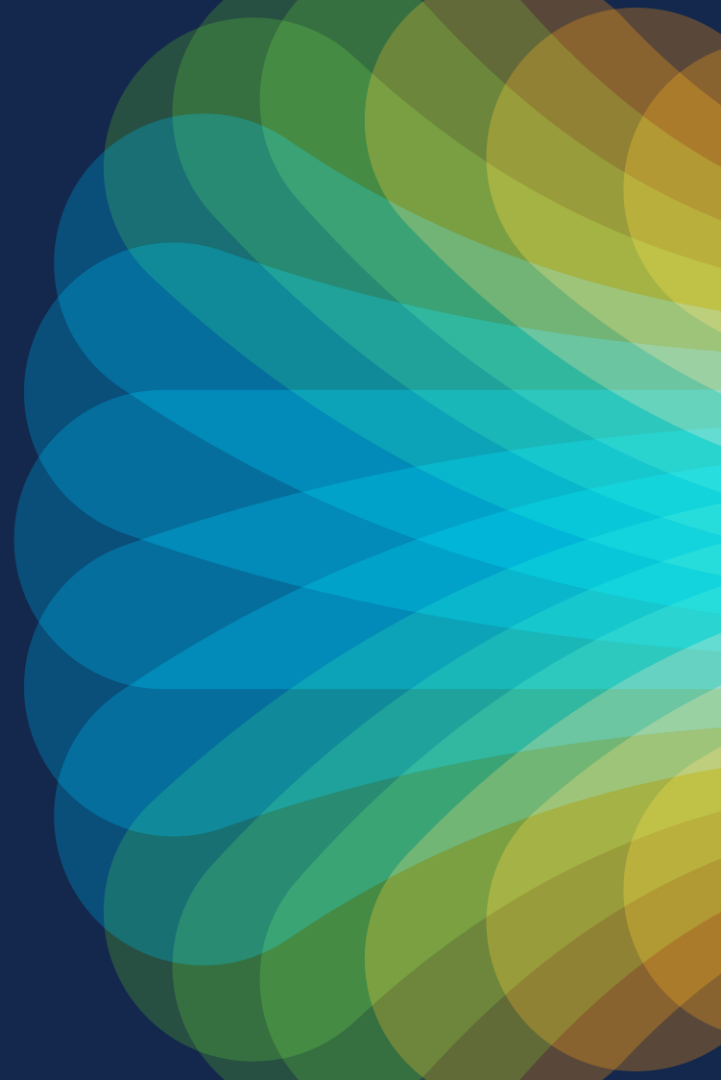


The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

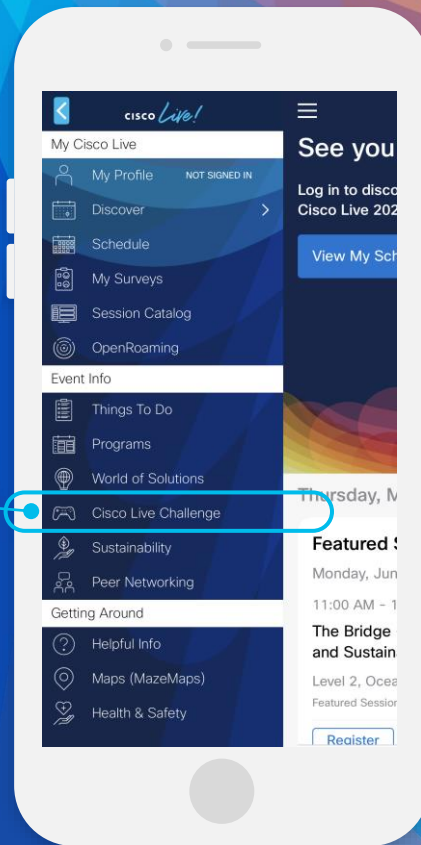


Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background features a vibrant, multi-colored abstract design. On the left, there are overlapping, wavy, organic shapes in shades of red, orange, and yellow. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, including blue, green, and yellow, creating a sunburst or starburst effect. The overall color palette is a spectrum of rainbow colors.

cisco *Live!*

Let's go

#CiscoLive