cisco *Live!*

Let’s go

#CiscoLive

The bridge to possible

Using Full Stack Observability to align application security and lifecycle management

Breakout Session

Luis Bravo CXPM Team Lead

www.linkedin.com/in/lbravo100

BRKAPP-2004

Cisco Webex App

Questions?

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

How

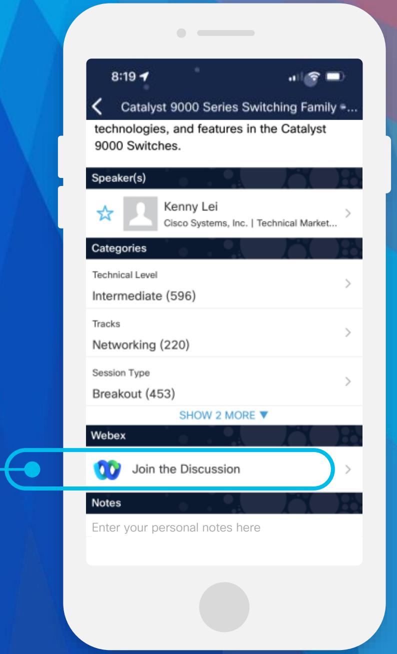
1 Find this session in the Cisco Live Mobile App

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.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKAPP-2004

Agenda

- Why do we need application security
- Securing on the left or the right
- Security Compliances
- Application security within Full Stack Observability
- Conclusion

Why do we need application security

The stakes are different for security

$6 Trillion

Global Impact of Cybercrime

Cost siphoned from beneficial investment to combat Cybercrime

Source: Herjavec Group 2021 Estimate

800%

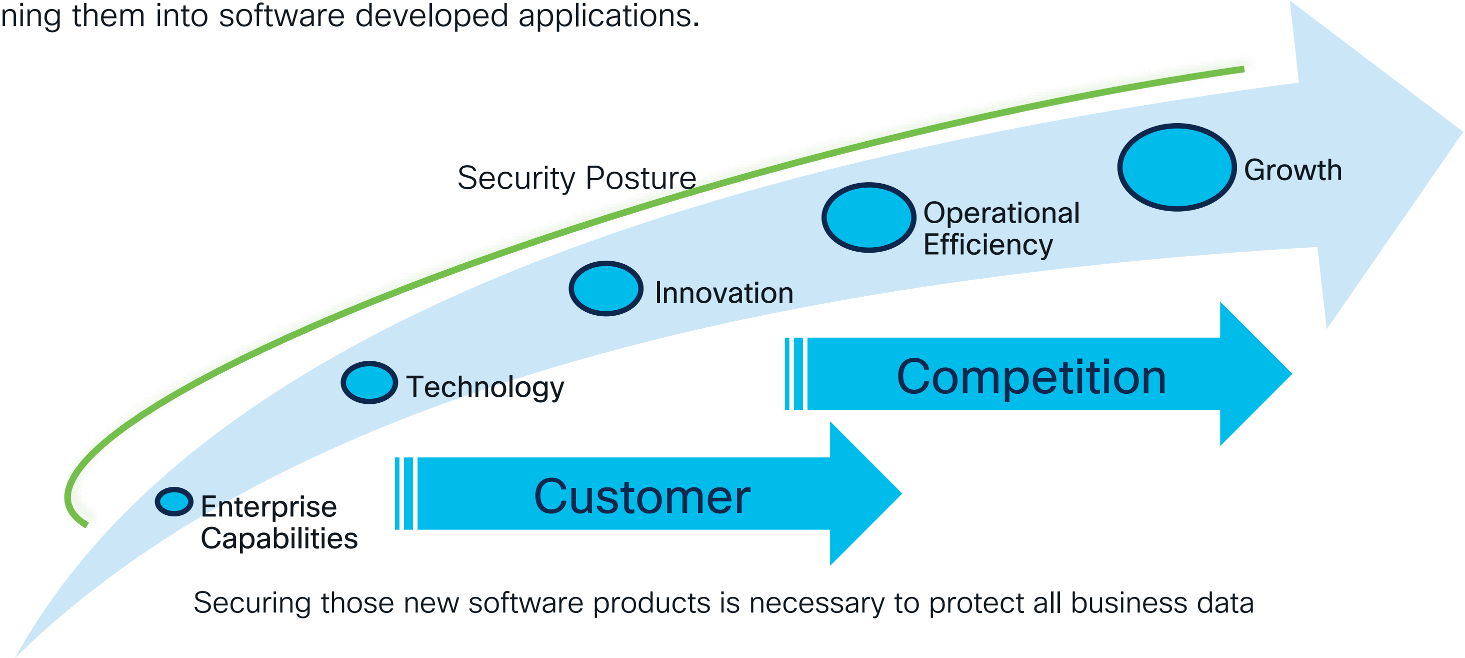
Increase in Nation-State initiated Cyber attacks

Since start of Russia-Ukraine War

The Register, Cyberattack Escalation, March 2022

Modern IT support operations must include Application Security

Organizations are now being challenged by their customers, partners and enterprise users to digitize their business processes turning them into software developed applications.



Securing those new software products is necessary to protect all business data

Security must be a priority when developing apps

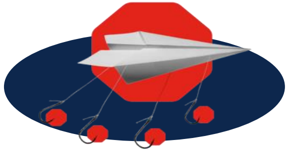
Maximizing Application Resiliency

- Secure Design Reviews
- Continuous Breach Resiliancy
- Technical Security Assessments
- Red Team & Penetration Testing

Cloud and Applications

Enterprise Networks

IoT Ecosystems



Operations

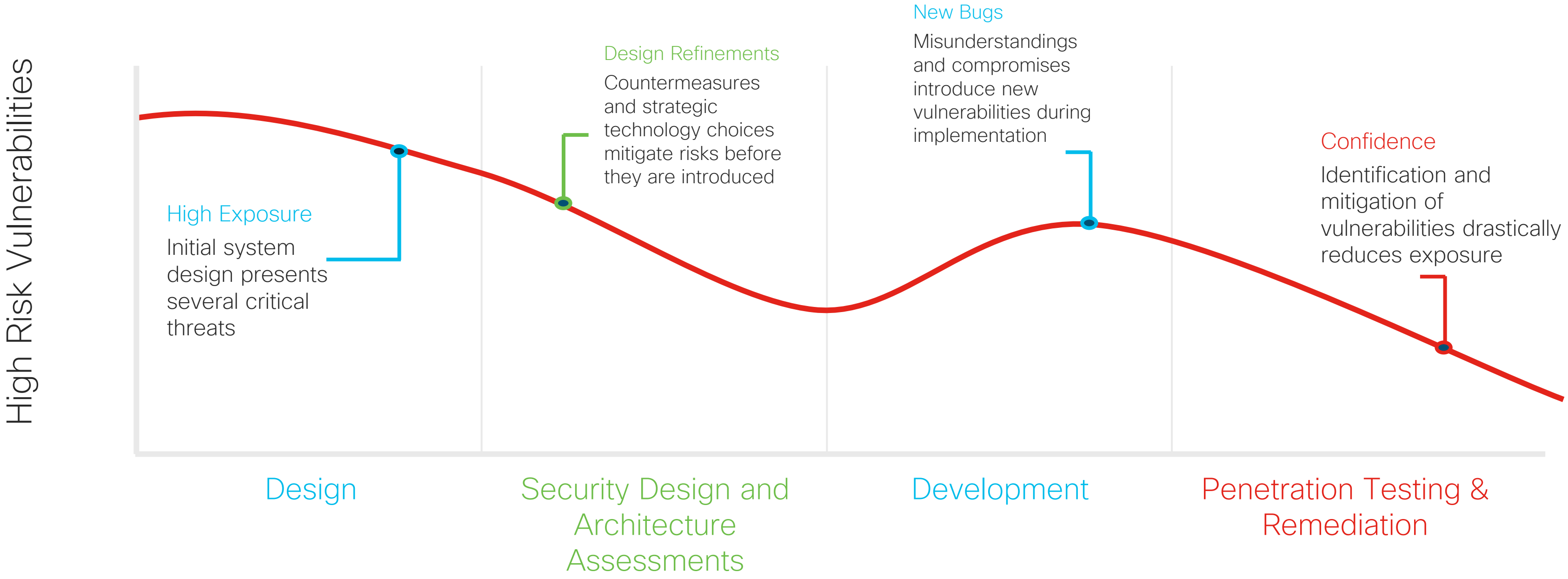
Develop an Application Security Framework

STRATEGY		EXECUTION		MANAGEMENT	
Compliance	Application Risk Criteria	Application Architecture	Application Security Tools & Solutions	Measurement & Metrics	Audit & Oversight
Secure Development Lifecycle	Contract Management	Threat Modeling	Awareness & Education	Configuration & Change Management	API Management
Requirements Definition	Roles Definition	Compliance Controls	Security Testing	Application Vulnerability Management	Profiling & Classification
Contingency Planning	3rd Party Portfolio Management	Data Security	Identity & Access Management	Incident Response & Forensics	Mobile Application Management

Securing on the left or the right

Shifting Left or Right

Minimizing Vulnerabilities Throughout the Lifecycle



High Risk Vulnerabilities
Design
Security Design and Architecture Assessments
Development
Penetration Testing & Remediation

High Exposure

Initial system design presents several critical threats

Design Refinements

Countermeasures and strategic technology choices mitigate risks before they are introduced

New Bugs

Misunderstandings and compromises introduce new vulnerabilities during implementation

Confidence

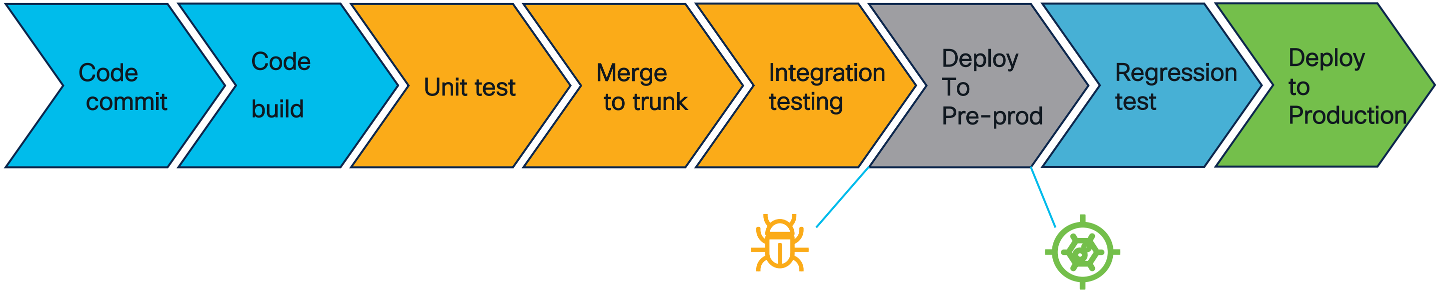
Identification and mitigation of vulnerabilities drastically reduces exposure

Managing and identifying vulnerability risks

How some organizations
Manage application security risks

Avoid	Accept	Mitigate	Transfer
Early remediation or alternative solution	Accept low risk and go live	Implement service or control mechanism	Hire external entity to own risk management

Identify vulnerabilities and security risks (example)



Code commit

Code build

Unit test

Merge to trunk

Integration testing

Deploy To Pre-prod

Regression test

Deploy to Production

SQL Injection identified

Application Risk identified

Specific Services

I want to know the security posture of my . . .

Applications and Systems

- Application Penetration Test and Security Assessments
- Application Design Assessment
- Code Review
- Software Development Lifecycle Assessment and Advisory
- Cloud Application Migration
- Threat Modelling

Networking & Infrastructure

- Network Design Assessment
- Network Penetration Test
- Network Vulnerability Assessment
- Host/Server/DB Build Review
- Cellular Radio Access Network Assessment
- Wireless Assessment/Penetration Test
- Breach Resiliency Subscription

Physical Components or Operations

- Physical Security Assessment
- Mobile Device Assessment
- Digital Profiling
- DevSecOps Assessment
- Phishing
- Physical Penetration Test
- OT Assessment - SCADA / ICS
- Hardware & Device Testing
- Connected Vehicle Testing

. . . and how to improve it.

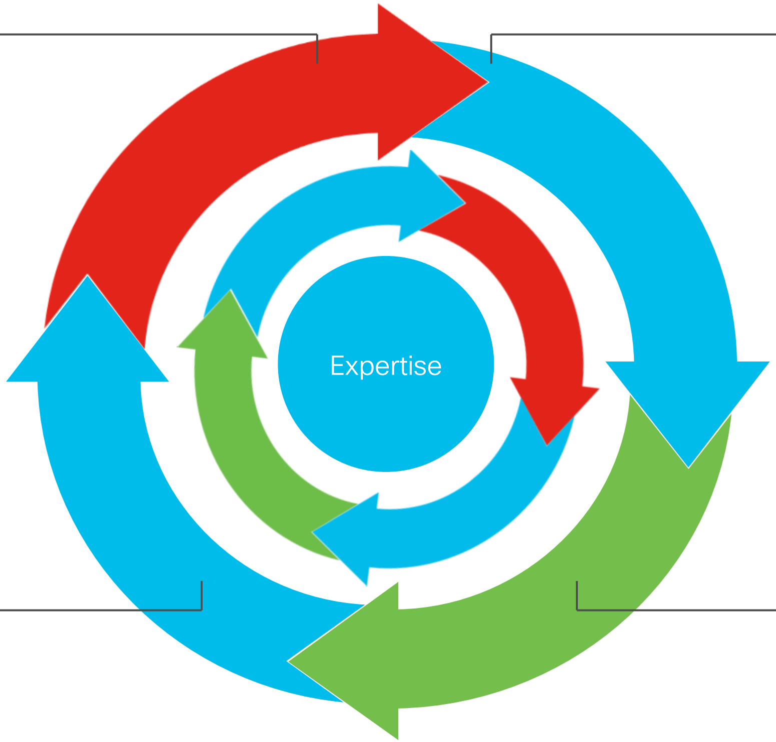
Process Fit

Penetration Test & Code Review

Testing and analysis of release. Verify countermeasures are effective.

Design

Create or modify system design. Produces product specifications.



Development

Produces new release.

Architecture Assessment & Threat Modeling

Identify threats, best practice gaps and countermeasures

Application Penetration Process Flow

Intelligence Gathering

- Define Targets
- Define Objectives
- Obtain Target Intelligence
- Identify Applicable Attack Vectors and Threat Agents
- Open Source Intelligence (OSINT) Gathering

Map Attack Surface

- Identify and map available functionality
- Perform scanning to identify hidden features
- Document different authorization levels and user types
- Research applicable threats to discovered system assets and software
- Prioritize attacks based on testing objectives

Vulnerability Scanning

- Fuzz known inputs and analyze responses
- Identify injection attacks
- Test for common misconfigurations
- Discover verbose errors or sensitive information
- Circumvent security controls

Manual Testing

- Manually verify scanner results
- Exploit vulnerabilities to gain additional access or bypass controls
- Chain exploits together to achieve further compromise
- Test authentication and authorization bypasses
- Exfiltrate sensitive data

Delivery and Closure

- Eliminate false positives, where possible
- Investigate potential business impact
- Investigate and develop remediation strategies
- Provide technical and strategic recommendations
- Additional Workshops

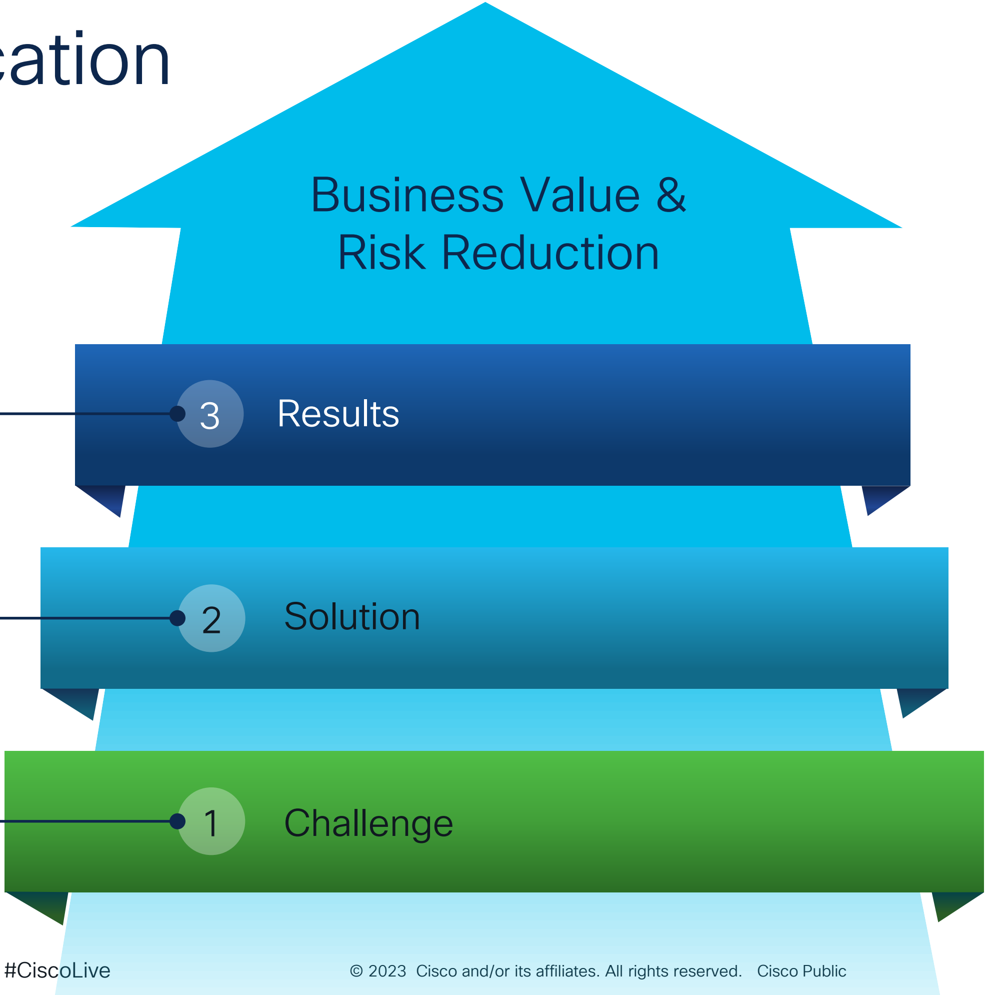
Example: Mobile Application

Securing mobile applications through penetration testing and application security

- **Securing user data** in transit and at rest against potential attackers
- **Securing the web service endpoints** against potential attackers
- Potentially adverse business impact of publishing insecure software

- **Security assessment** produces a prioritized list of must-fix issues along with remediation advice
- Executive presentation proving business impact
- Targeting specific concerns rather than the entire surface

- **Securing user data** in transit and at rest against potential attackers
- Securing the web service endpoints against potential attackers
- Potentially adverse business impact of publishing insecure software



Business Value & Risk Reduction

3 Results

2 Solution

1 Challenge

Common Web App Findings during penetration testing

Injection Attacks

- SQL Injection
- XML External Entity (XXE) Injection

Client Side Attacks

- Cross-Site Scripting -XSS (Reflected/Stored/DOM Based)
- Cross-Site Request Forgery (CSRF)
- Insecure Redirection

Controls Bypass

- Broken Authentication
- Horizontal / Vertical Authorization Bypass
- Business Logic Errors
- Timing Attacks

*OWASP Top 10 Vulnerabilities
1 – Injection
2 – Broken Authentication and Session Management
3 – XSS
4 – Insecure Direct Object References
5 – Security Misconfiguration
6 – Sensitive Data Exposure
7 – Missing Function Level Access Control
8 – CSRF
9 – Using Known Vulnerable Components
10 – Unvalidated Redirects and Forwards

*Open Web Application Security Project

Worsening trends confirm a capability struggle

1,108

2020 Cyber security breaches

1,862

2021 Cyber security breaches

68%

Increase in reported breaches from 2020 to 2021

Source: CNET Data Breach 2021 Report, Jan. 2022

Customer pain is real and similar to ITOps problems

$9.05M

Cost to Contain a Breach in the US

Average cost to contain a breach with 38% of this cost from lost business

“Cost of a Data Breach Report 2021,” Ponemon Institute, https://www.ponemon.org/

287 days

>200 Days to detect breach occurred!

Average time to identify and contain a data breach

“Cost of a Data Breach Report 2021,” Ponemon Institute, https://www.ponemon.org/

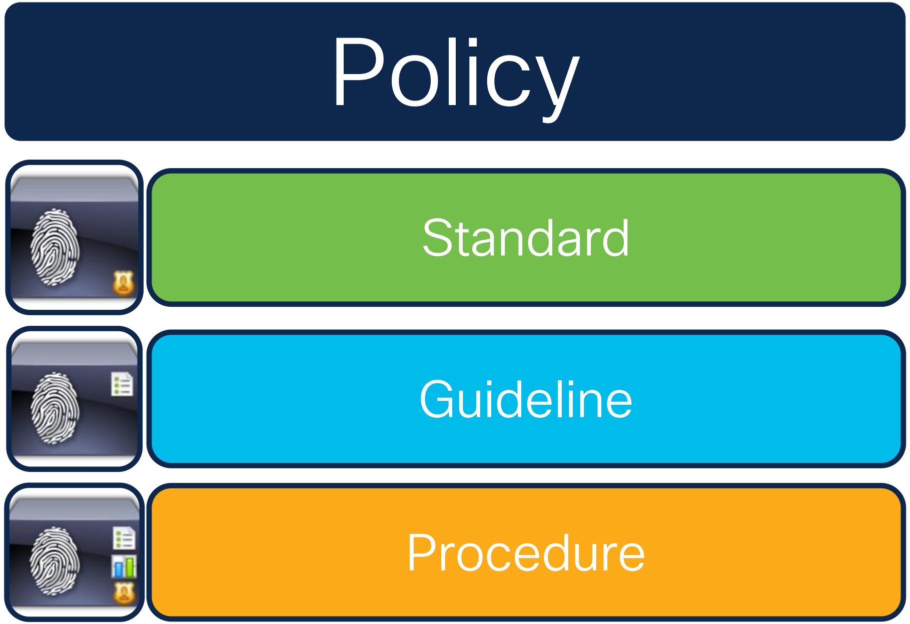
Breaches with data exfiltrated in the first 24-hours

Source: Cisco Security, 2020

Security Compliances

Meeting internal and external security policies

- Governance, risk and compliance
- Security roadmaps
- Define security standards (i.e. encryption)
- Security Guidance are non mandatory
- Procedural steps to implement standards or guidelines



Policy

Standard

Guideline

Procedure

Legal and Regulatory Compliance

International & Local

Information Security + Privacy

- ISO 2700X i.e ISO 27001 / 27017 / 27018 / 27701
- SOC 2 Type II and SOC 3
- Cloud Computing Compliance Controls Catalog (C5)
- FedRAMP
- Cisco's Quality Management System
- ISO 9001
- CSA STAR L2

Regulatory

- HIPAA
- GDPR
- FERPA
- COPPA
- PIPEDA
- PHIPA
- CCPA
- PCI
- Continually assessing regs

Cross-Border Transfers

- Binding Corporate Rules
- APEC cross-border privacy rules
- EU Standard Contractual Clauses

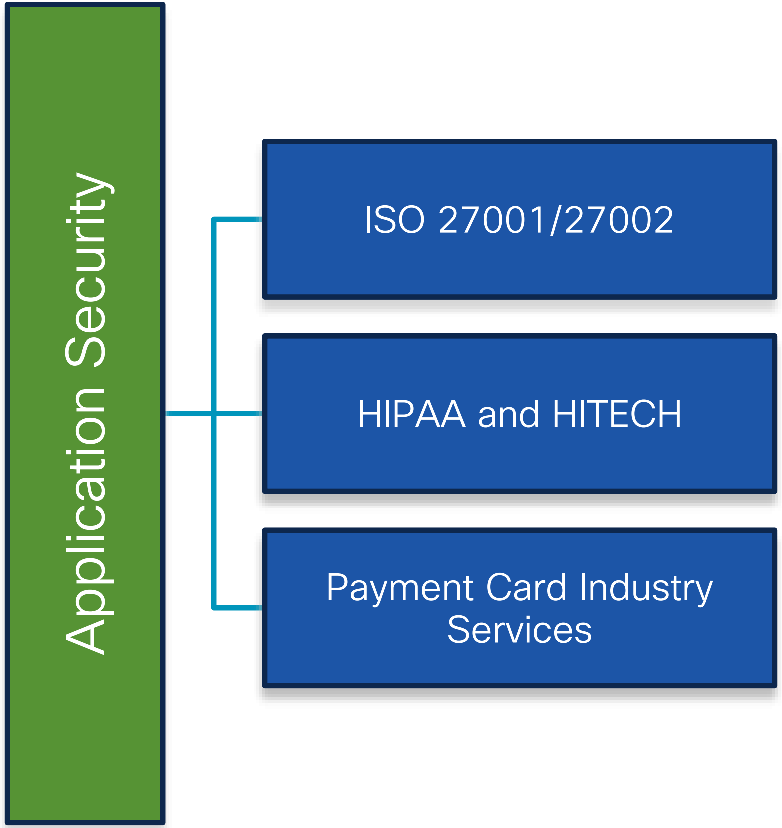
Business applications with highest security risk

42%	Customer facing web apps
40%	Legacy applications
30%	Mobile applications
28%	Desktop applications
26%	Internal-facing applications
26%	Business applications

Source: Cybersecurity insiders, Application Security Report 2022

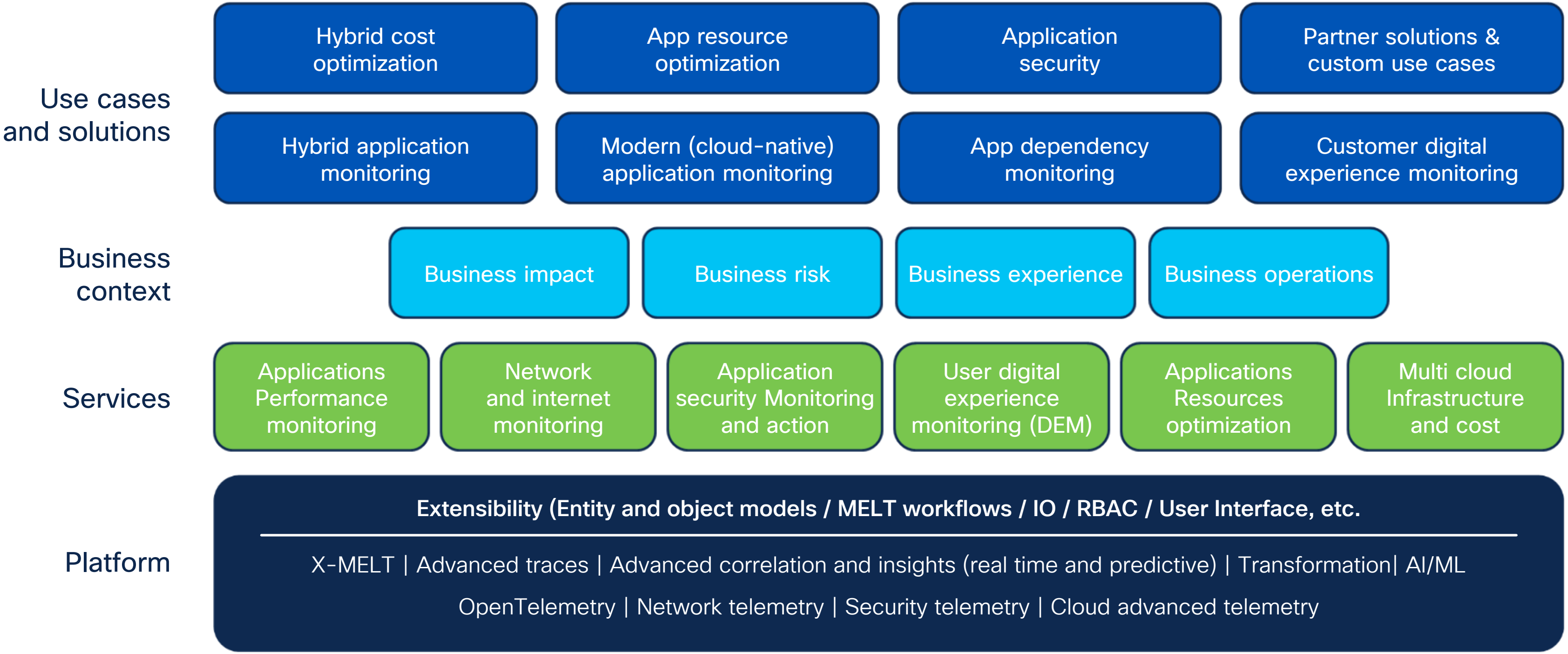
Application alignment with compliances

- **Expertise** is needed for the following:
  - Understand and satisfy regulatory requirements.
  - Build a compliance roadmap that bridges existing practices and certification goals.
  - Take advantage of the knowledge gained for broader security maturity.
- **Reduce costs** by avoiding penalties imposed when you are not in alignment with regulations.
- **Faster adoption.**
- **Align audit cycles.**
- **Improve agility** to keep up with constantly changing business models.



App security within Full Stack Observability

Cisco Full-Stack Observability Architecture Foundation



Use cases and solutions

- Hybrid cost optimization
- App resource optimization
- Application security
- Partner solutions & custom use cases
- Hybrid application monitoring
- Modern (cloud-native) application monitoring
- App dependency monitoring
- Customer digital experience monitoring

Business context

- Business impact
- Business risk
- Business experience
- Business operations

Services

- Applications Performance monitoring
- Network and internet monitoring
- Application security Monitoring and action
- User digital experience monitoring (DEM)
- Applications Resources optimization
- Multi cloud Infrastructure and cost

Platform

Extensibility (Entity and object models / MELT workflows / IO / RBAC / User Interface, etc.

X-MELT | Advanced traces | Advanced correlation and insights (real time and predictive) | Transformation| AI/ML

OpenTelemetry | Network telemetry | Security telemetry | Cloud advanced telemetry

Full Stack Observability

With focus on Application Security

Focused on vulnerabilities & threats

App Team

Security Team

Focused on velocity & user experience

docker
Azure
kubernetes
amazon web services
serverless
IBM
SAP
Google Cloud
kubernetes
docker
kubernetes
serverless
PRIVATE

Secure Application Use Cases at Runtime

Fast to deploy, immediate time to value, and performant for all environments

Detect Vulnerabilities

Common Vulnerabilities and Exceptions with Code Level correlation

Detect Attacks

Spot Common Vulnerabilities correlated runtime exploits and Zero Day attacks (like Log4j)

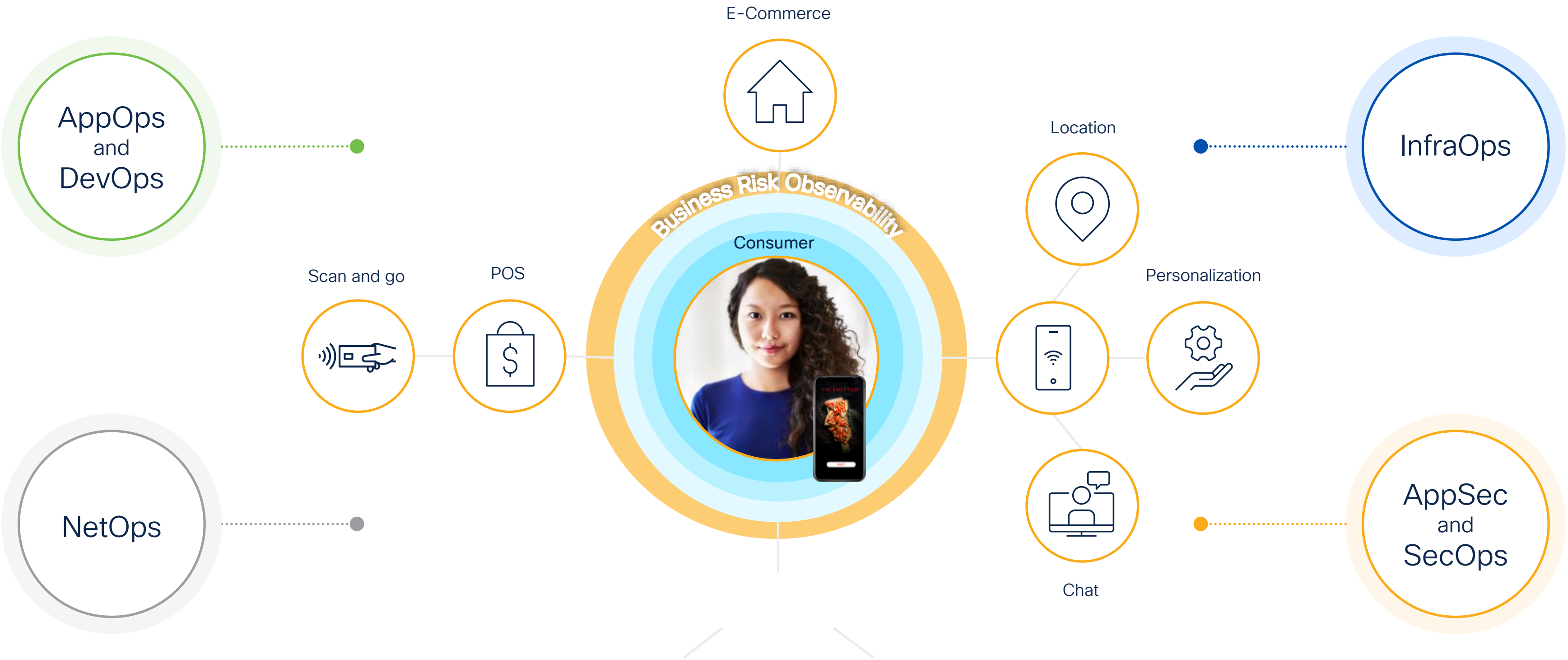
Block Attacks

Policy level blocking that stops bad actors… even if vulnerabilities exist

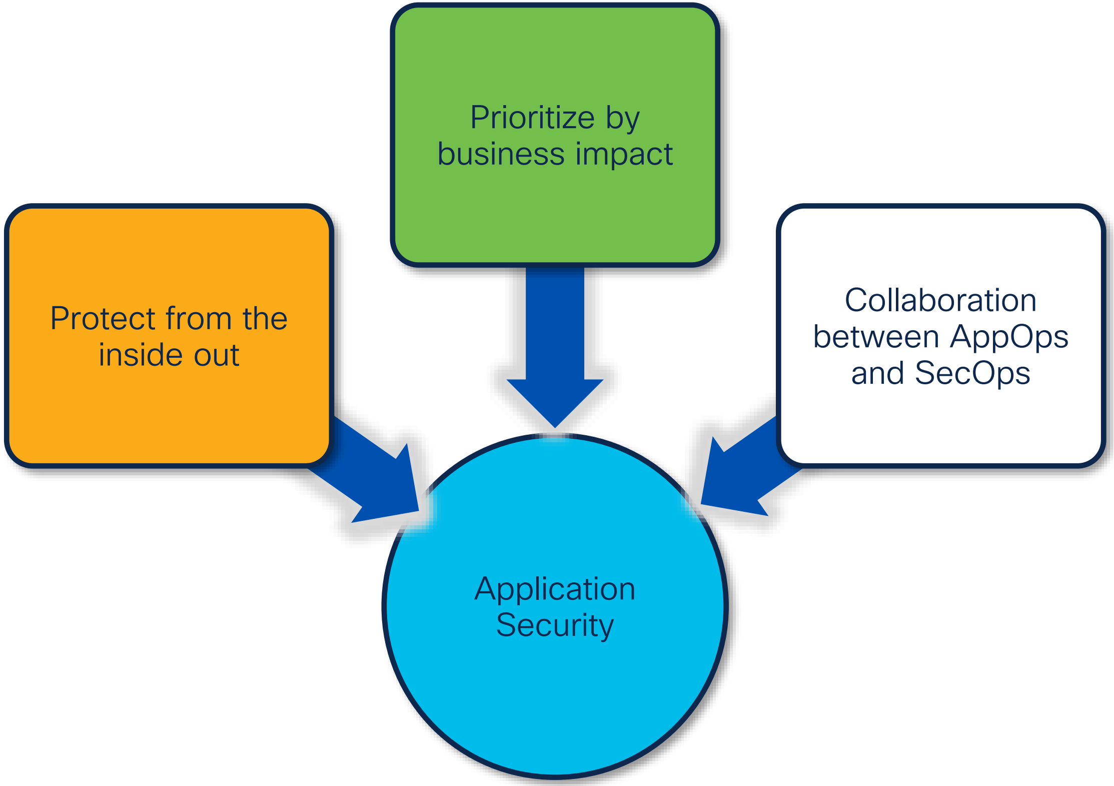
Security insights provided with Application and Business context

Your teams need to see the full stack of available data

Fast to deploy, immediate time to value, and performant for all environments



Application Security at the center of business



Prioritize by business impact

Protect from the inside out

Collaboration between AppOps and SecOps

Application Security

Applications require a new security approach

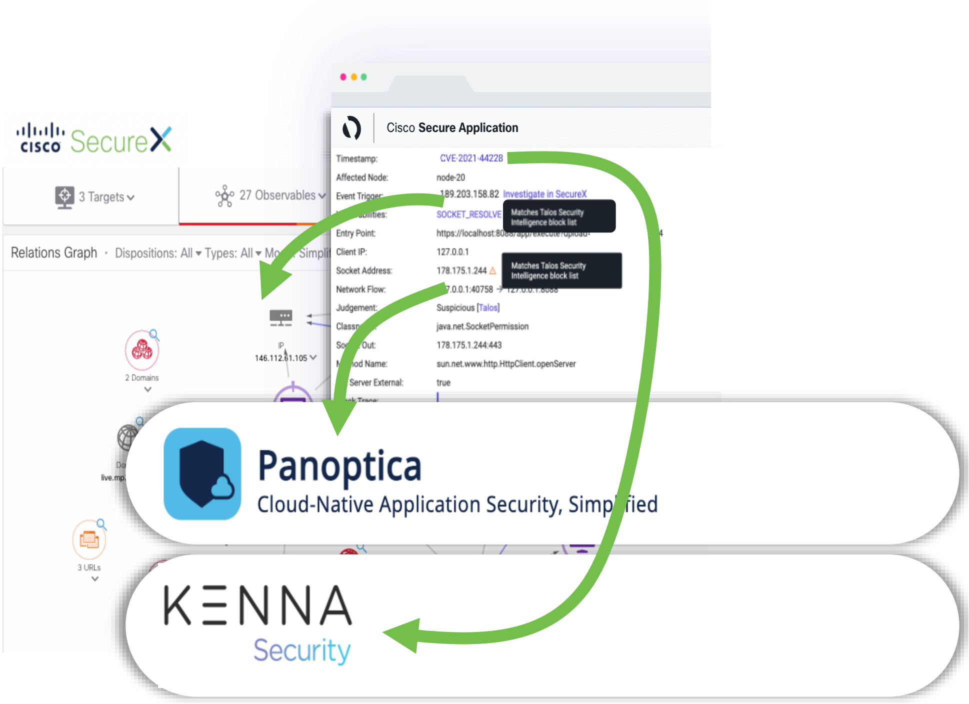
Empowering the digital enterprise to operate with speed and security

New applications	Require new protections
Run anywhere	CLOSER to the application
Change constantly	CONTINUOUSLY automates security
Are unique	ADAPTIVE for the application

Cisco FSO Security solution

Extended detection and response to boost productivity

- Integrated with Kenna Security
- Detailed vulnerabilities insights to prioritize right vulnerabilities to address
- Integrated with Panoptica
- Expose 3rd-party API security issues (Vulnerabilities, *TLS issues..)
- Integrated with Talos Intelligence
- Identify bad actors
- Hunt for threats in SecureX
  Give a more complete picture of an incident



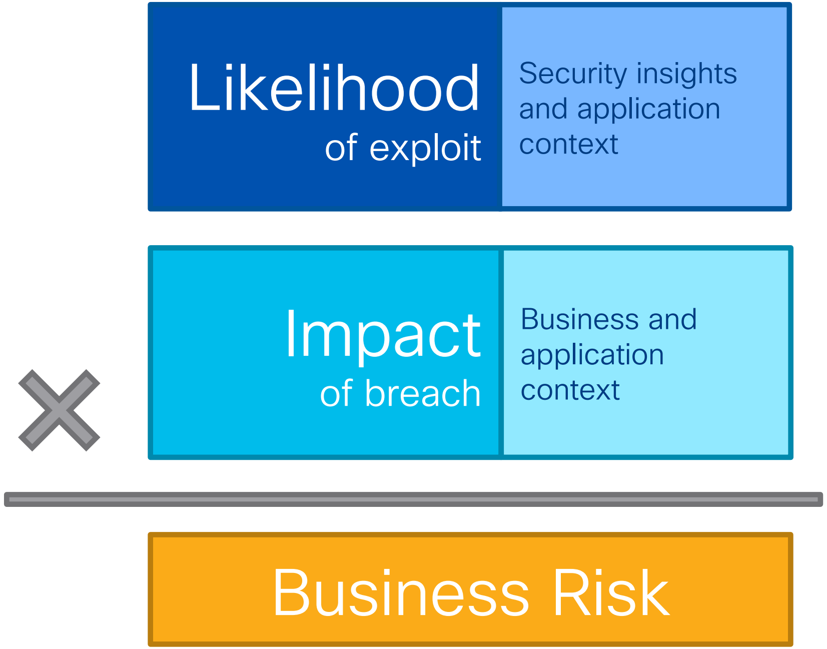
SecureX
3 Targets
27 Observables
Relations Graph · Dispositions: All ▾ Types: All ▾ Mo… Simplif…
2 Domains
IP
146.112.61.105
Do…
live.mp…
3 URLs
Panoptica
Cloud-Native Application Security, Simplified
KENNA
Security

Cisco **Secure Application**

Timestamp: CVE-2021-44228
Affected Node: node-20
Event Trigger: 189.203.158.82 Investigate in SecureX
…abilities: SOCKET_RESOLVE
Matches Talos Security Intelligence block list
Entry Point: https://localhost:8088/app/execute?upload-
Client IP: 127.0.0.1
Socket Address: 178.175.1.244 ⚠
Matches Talos Security Intelligence block list
Network Flow: …7.0.0.1:40758 → 127.0.0.1:8088
Judgement: Suspicious [Talos]
Classn…: java.net.SocketPermission
So… Out: 178.175.1.244:443
M…od Name: sun.net.www.http.HttpClient.openServer
… Server External: true
…k Trace:

*Transport Layer Security

What is Business Risk Observability?



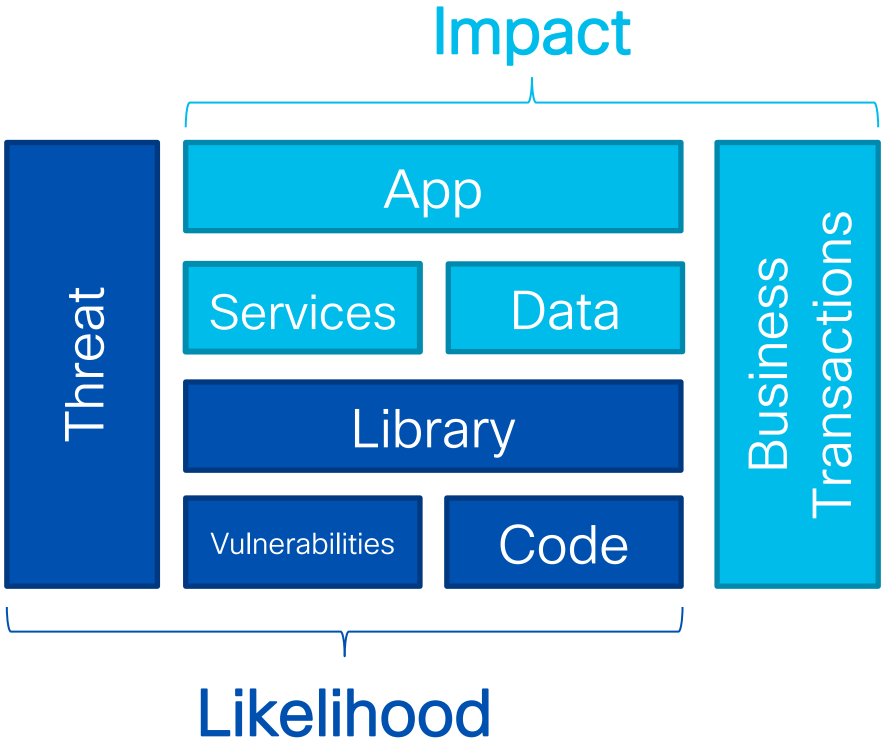
Likelihood of exploit

Security insights and application context

Impact of breach

Business and application context

Business Risk



Impact

App

Services

Data

Library

Vulnerabilities

Code

Threat

Business Transactions

Likelihood

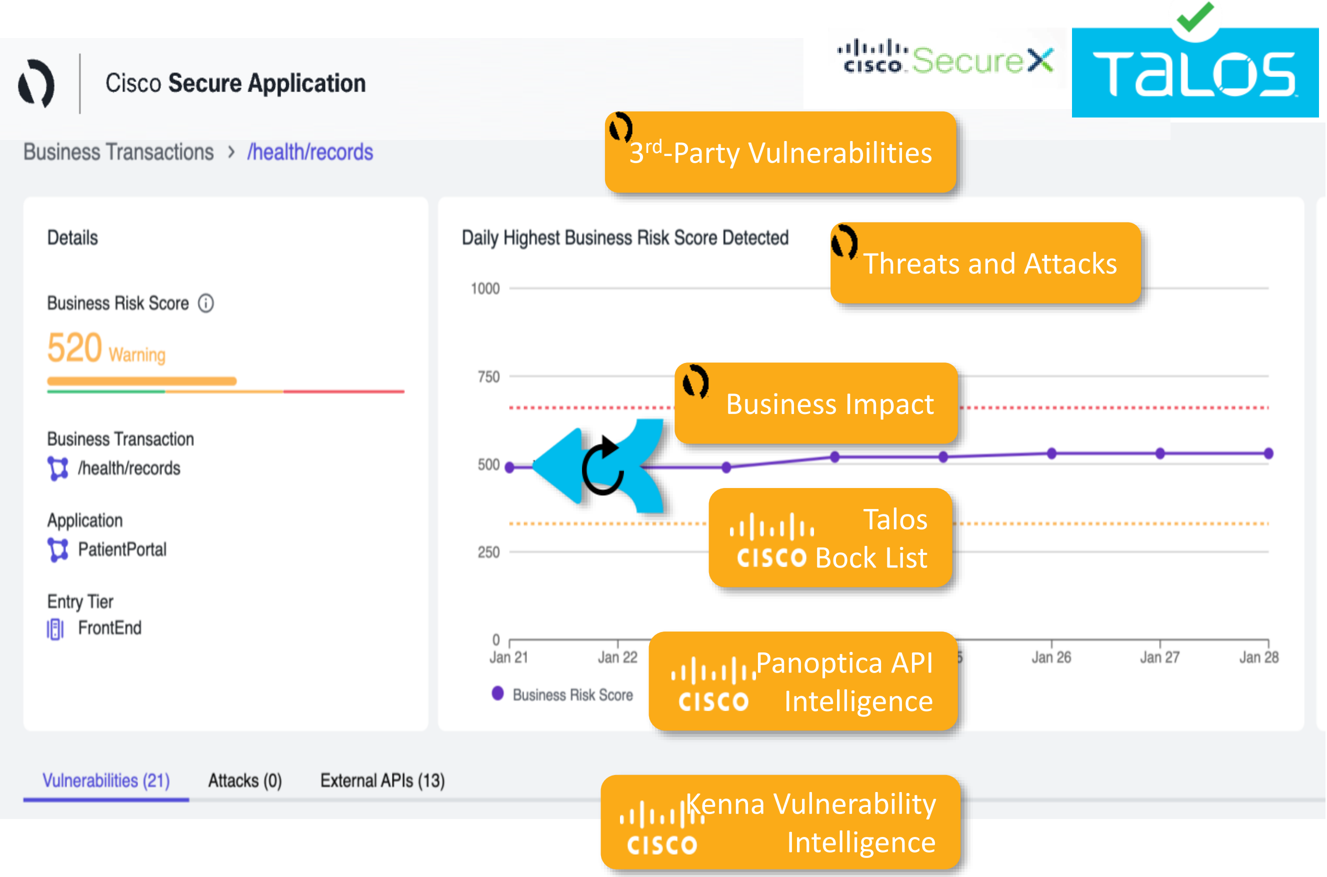
Risk Scoring

- Leverage app and biz data
  Create a customer-specific view of security risk

- Security insights in transactions
  Merge findings and intel from Cisco Talos, Panoptica, Kenna, *Snyk

- Continuously assess score
  Evaluate all changes to reflect real-time risk

- Stack-ranked risk
  Prioritize remediation and mitigation efforts by what matters to the biz



Cisco Secure Application

Business Transactions › /health/records

Details

Business Risk Score ⓘ

520 Warning

Business Transaction
/health/records

Application
PatientPortal

Entry Tier
FrontEnd

Daily Highest Business Risk Score Detected

Vulnerabilities (21) Attacks (0) External APIs (13)

Demo

Cisco Secure App

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 Game** 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

Discover how full-stack observability services accelerate outcomes

Cisco **Customer Experience**

CX helps you identify and deliver exceptional digital experiences. We assess your use cases, implement KPIs, and deliver recommendations for optimizing your application and networking experience.

How we can help

Strategy and solution discovery
Discover and document business and technical use cases, identify sources of information and drive observability roadmap

Planning, design, implementation
Accelerate success implementing unified dashboards and correlating available information for business related KPIs

Assessments
Assess application and networking environment readiness to gather necessary metrics

Knowledge transfer
Receive consulting support with dedicated advisors driving recommendations

Optimization and monitoring support
Unleash the full power of full-stack observability tools

Learning | Certifications
Empower your workforce with efficiency and innovation

Optimize the user experience with the power of FSO

Innovate with Cisco® certified application experts

Stay agile to resolve application issues with predictable analytics

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

Agenda

Where Partner Managed and as-a-Service Sales is showing up at Cisco Live

- 11 Sessions (1 Customer Success, 2 PSO's, 6 Breakouts, 2 Dev)
- Partner Day – Tuesday, June 6th 10:00 am – 1:00 pm. Alexandra Zagury Presentation.
- Partner Managed Services Booth (#2217) in the World of Solutions
- Meet the Executive – Alexandra Zagury
- Meet the Engineer – Sanjit Aiyappa
- Private Meeting Room for PMaaS & APO partner/customer meetings (location TBD)

Partner Managed and as-a-Service Sales Sessions

Session	Monday June 5	Tuesday June 6	Wednesday June 7	Thursday June 8
Partner Day		10:00 – 1:00		
BRKNWT-2208 - Driving network automation through application visibility and event correlation (Russ, Aleksas)	10:30 – 11:30			
DEVWKS-2768 - Demystifying Cisco FSO Stack APIs (Anuj)	12:00 Noon			
PSOGEN-1033 – Unlock business outcomes from connectivity with a Private 5G solution (PK)	2:30 – 3:00 WOS			
CSSMER-1008 – TBD (Hector)	4:00 – 5:00			
BRKIOT-1127 – Build pervasive wireless mobility in industrial environment (Karan)	4:00 – 5:00			
PSOGEN – 1044 – How to generate new revenue streams while enhancing customer experiences and engagement: A use case story (Sanjit)	New time: 1:00 or 2:30 WOS			
BRKGEN-1366 - From Zero to Managed Campus using Cisco DNAC (Hector)			2:30 – 3:30	
BRKGEN-2000 - Demystifying Cisco FSO Stack APIs- Building a secure code pipeline with Concourse CI and Vault Integration (Anuj)			4:00 – 5:00	
BRKGEN-2001 - Cisco P5G - A Robust and Secure Architecture (Rajneesh)				1:00 – 2:00
BRKXAR-2014 - Managed Service Provider - Creating Single Touch-Point for Multiple Cisco Architecture using API's and increasing their operational efficiency (Sunil)				1:00 – 2:00
DevNet-2278 – Using IOT + Collab + Meraki API’s for a safer return to school (Hector)		2:00 – 2:45 DeNet Classroom 2		

Partner Managed and as-a-Service CLUS FSO-related Sessions

Session ID	Title	Speaker	Session Date/Time	Abstract
BRKNWT-2208	Driving network automation through application visibility and event correlation	Russ Atkin, Aleksas Vitenas	6/5 10:30 - 11:30	The trend is clear: automation and machine learning are helping IT teams support more strategic initiatives for the business. AIOps tools, are accelerating this trend by shrinking mean time to resolution (MTTR) and helping IT leaders better support user experience. We will discuss how Cisco can help you enhance observability across the network and cloud native environments. By augmenting observability with AIOps tools, a vast improvement in operational efficiency is quickly becoming a reality. In this session, we will illustrate how Cisco is supporting our partners with programs that provide a blueprint to deploy observability-driven operations, by leveraging best-in-class Cisco infrastructure with observability innovations into AIOps platforms with open extensible APIs. This Full-Stack Observability use case improves overall Customer Experience and will significantly lower Mean-Time-to-Isolation (MTTI) in complex multi-domain environments. Discuss a functional Architecture for AIOps
BRKGEN-2000	Demystifying Cisco FSO Stack APIs - Building a secure code pipeline with Concourse CI and Vault Integration	Anuj Modi	6/7 4:00 - 5:00	The DevOps culture brings a new change to the IT industry by collaborating developers and operations teams to build better products using automation, CI/CD, and APIs. This session will walk through modern cloud-native development methodology to make the code pipeline for testing & development with Cisco FSO APIs. This session will cover the fundamentals of CISCO FSO APIs stack including all of its components like AppDynamics, ThousandEyes, and Intersight to integrate with their own products or third-party products. The takeaway would be detailed information on building lab using AWS cloud provider, Hashicorp Vault, container repositories, source code repo, Kubernetes, AWS APIs, to create a pipeline for the entire infrastructure as a code
DEVWKS-2768	Demystifying Cisco FSO Stack APIs	Anuj Modi	6/5 12:00 Noon	The DevOps culture brings a new change to the IT industry by collaborating developers and operations teams to build better products using automation, CI/CD, and APIs. This session will walk through modern cloud-native development methodology to make the code pipeline for testing & development with Cisco FSO APIs. This session will cover the fundamentals of CISCO FSO APIs stack including all of its components like AppDynamics, ThousandEyes, and Intersight to integrate with their own products or third-party products. The takeaway would be detailed information on building lab using AWS cloud provider, Hashicorp Vault, container repositories, source code repo, Kubernetes, AWS APIs, to create a pipeline for the entire infrastructure as a code. New this year DevNet workshop seating is pre-registered attendees are seated first. There are only 20 laptops available for this session. This is a hands-on DevNet Workshop where you code along with an instructor.

Partner Managed and as-a-Service CLUS FSO Related Complementary Sessions. Cross Promotion (CTA to PMaaS Booth, promote our sessions)

Session ID	Title	Speaker
BRKAPP-2007	Cisco FSO Platform and 2 partner use cases	Ben Haddox
LTRAPP-2682	Building Observability Solutions on the FSO Platform	Renato Quedas
PSOAPP-1009	Extend observability with Cisco FSO Platform	Yogesh Ranjan
BRKAPP-1013	Empower a new observability ecosystem with an open and extensible Cisco FSO Platform	Sunder Parameswaran, Renato Quedas
BRKAPP-2008	Cisco FSO Platform and partner use cases	Luca Relandini
BRKAPP-2632	Adopt Cisco Full-Stack Observability to Accelerate Cloud Migration	Subarno Mukherjee
IBOCLD-2020	An Interactive Discussion on Why Organizations Need an FSO Platform	Luis Bravo

The bridge to possible

Thank you

#CiscoLive

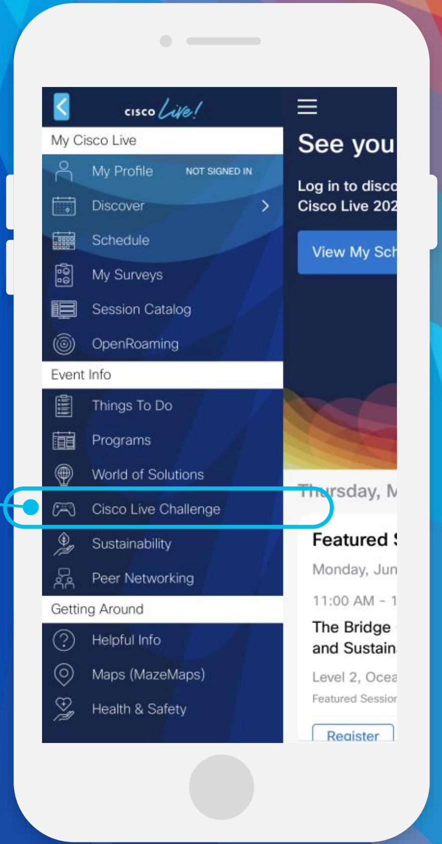
Cisco Live **Challenge**

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:



cisco Live!

Let's go

#CiscoLive