The bridge to possible

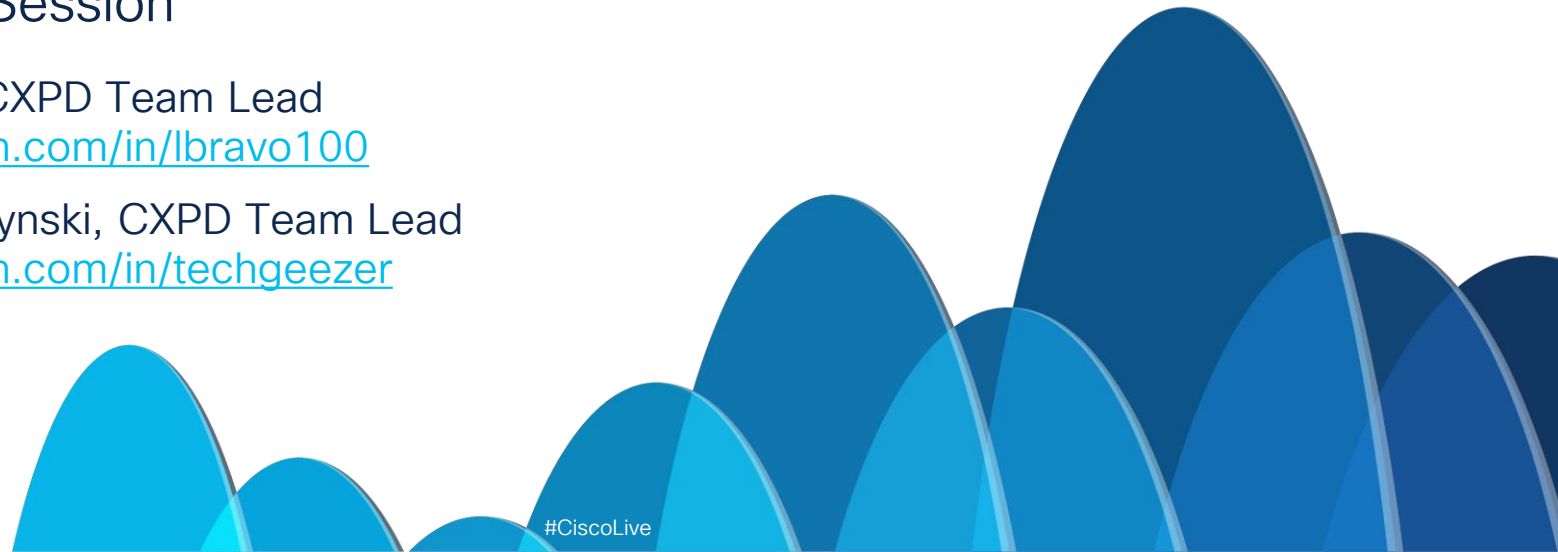
Using Full Stack Observability to align application security and lifecycle management

Breakout Session

Luis Bravo, CXPD Team Lead
www.linkedin.com/in/lbravo100

Marc Buraczynski, CXPD Team Lead
www.linkedin.com/in/techgeezer

BRKAPP-2004



cisco Live!

Cisco Webex App

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

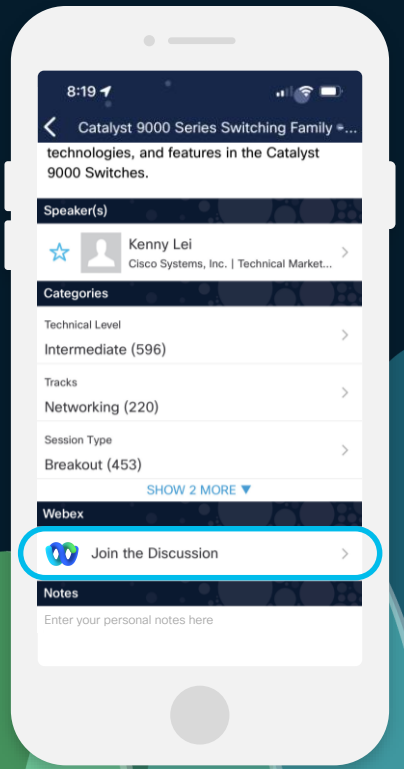
Questions?

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 7, 2024.



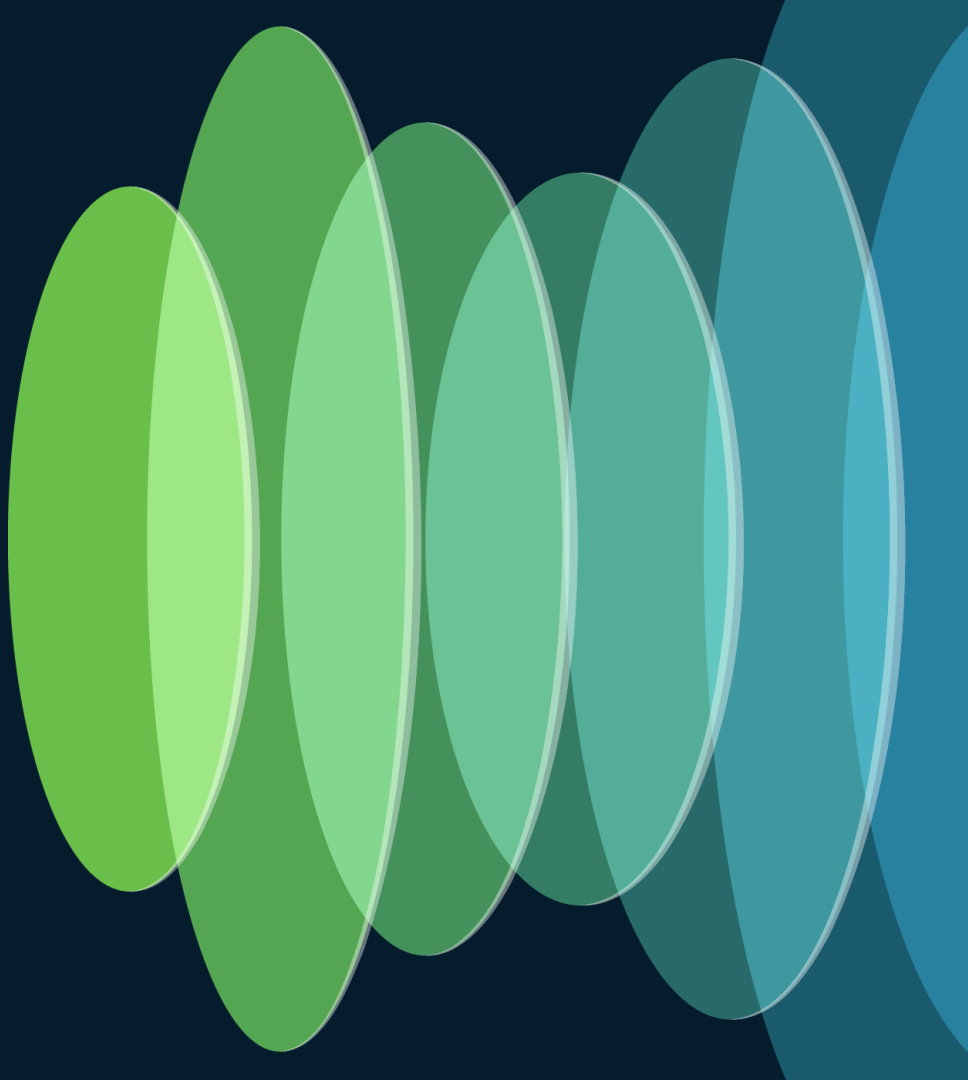
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

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

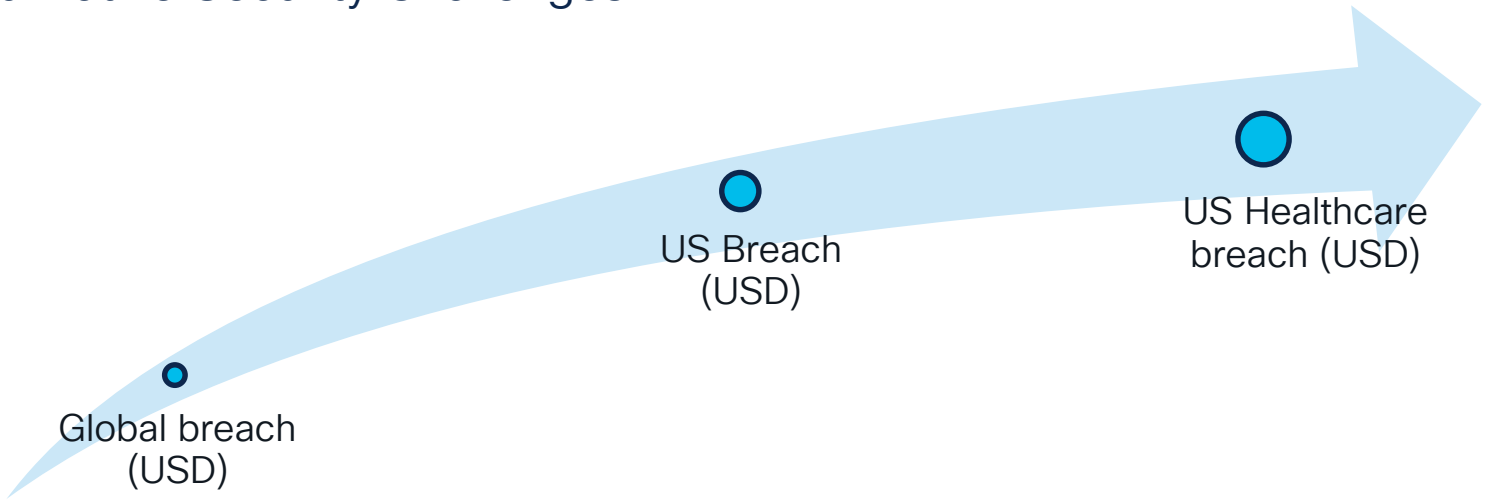
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why do we need application security?



Threats Are Becoming More Expensive

Cloud Native Security Challenges



$4.4M

Global average cost of a breach in 2023

$9.8M

Average cost of a breach **in the US** in 2023

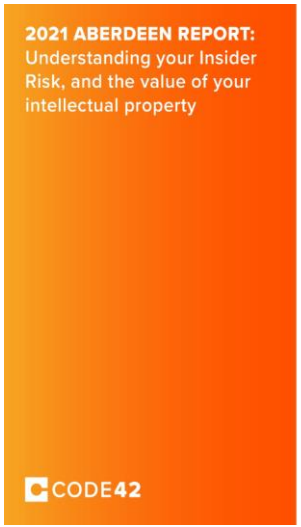
$10.9M

Average cost of a **healthcare** breach in the US in 2023

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Background...

- Security is the number one challenge your customers confront
- Bad actors primary motivation is profit: Disruption > Data (Cisco Ground School)
- Insider threats on the rise and often fueled by alternate currencies more powerful than cash....

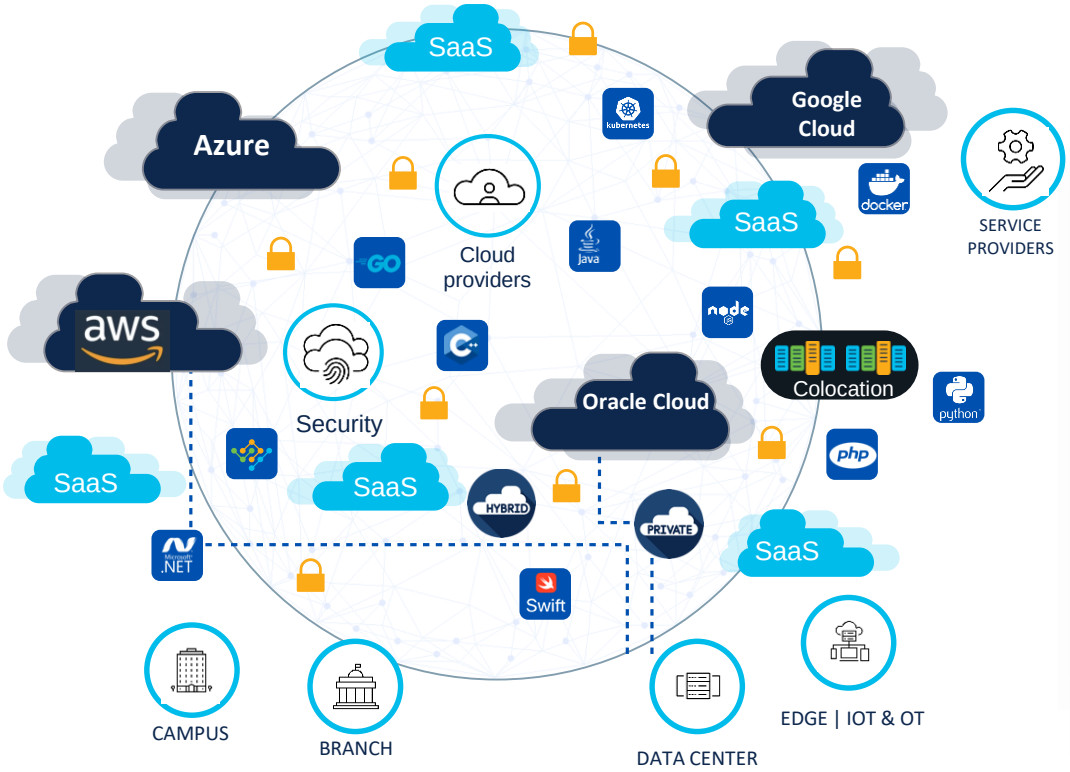


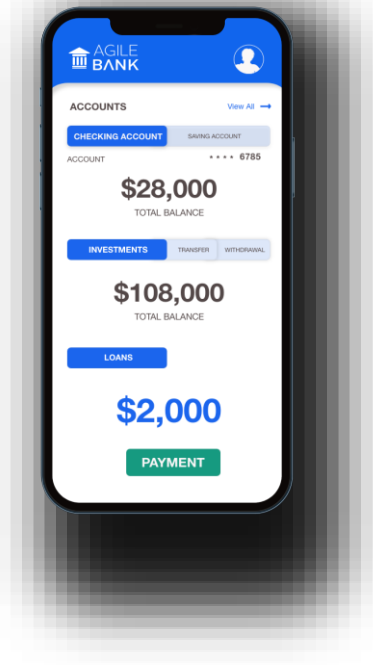
20%

- Annual revenue cost of data breaches from insiders.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Users expect simple, performant and secure experiences...





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Worsening trends confirm a capability struggle

1,108

2020
Cyber security breaches

1,862

2021
Cyber security breaches

Increase in reported breaches from 2020 to 2021

Source: CNET Data Breach 2021 Report, Jan. 2022

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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/

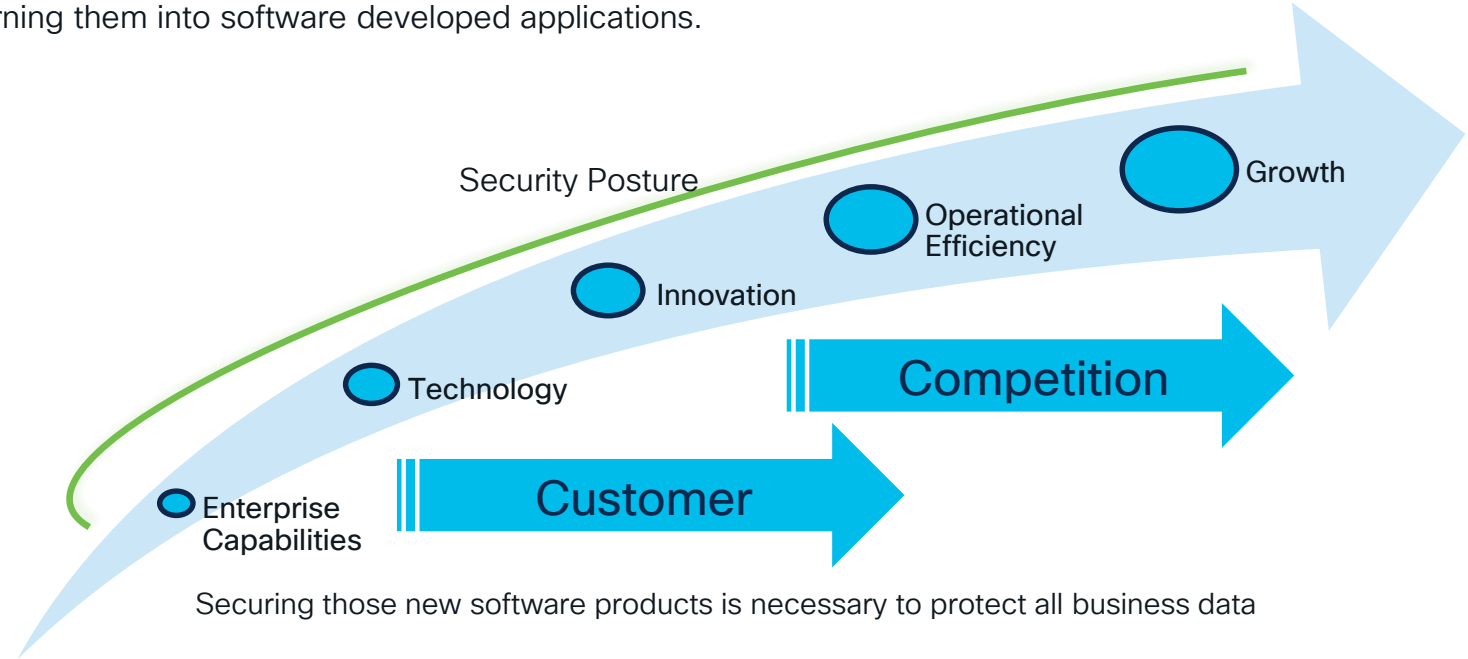
Breaches with data exfiltrated in the first 24-hours

Source: Cisco Security, 2020

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security must be a priority when developing apps

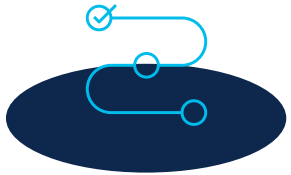
Maximizing Application Resiliency

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

Cloud and Applications

Enterprise Networks

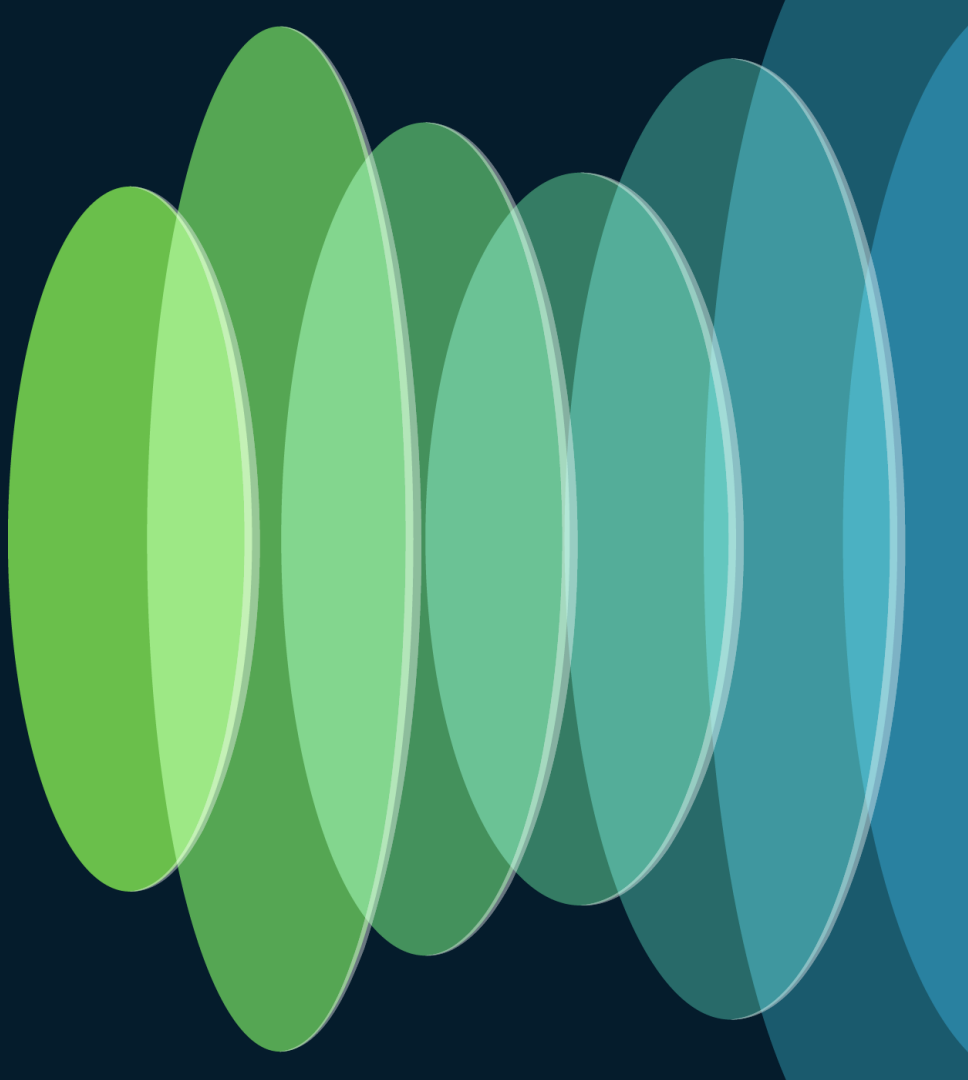
IoT Ecosystems



Operations

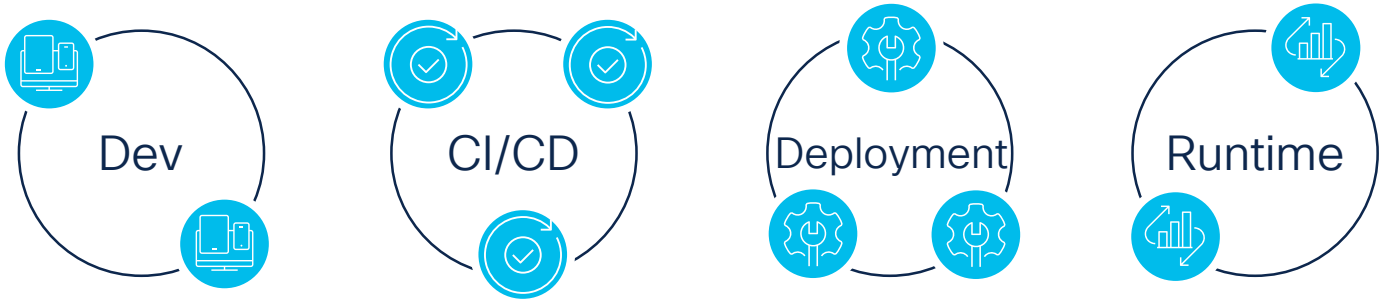
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Securing on the left or the right



Too Many Siloed Tools

Cloud Native Security Challenges



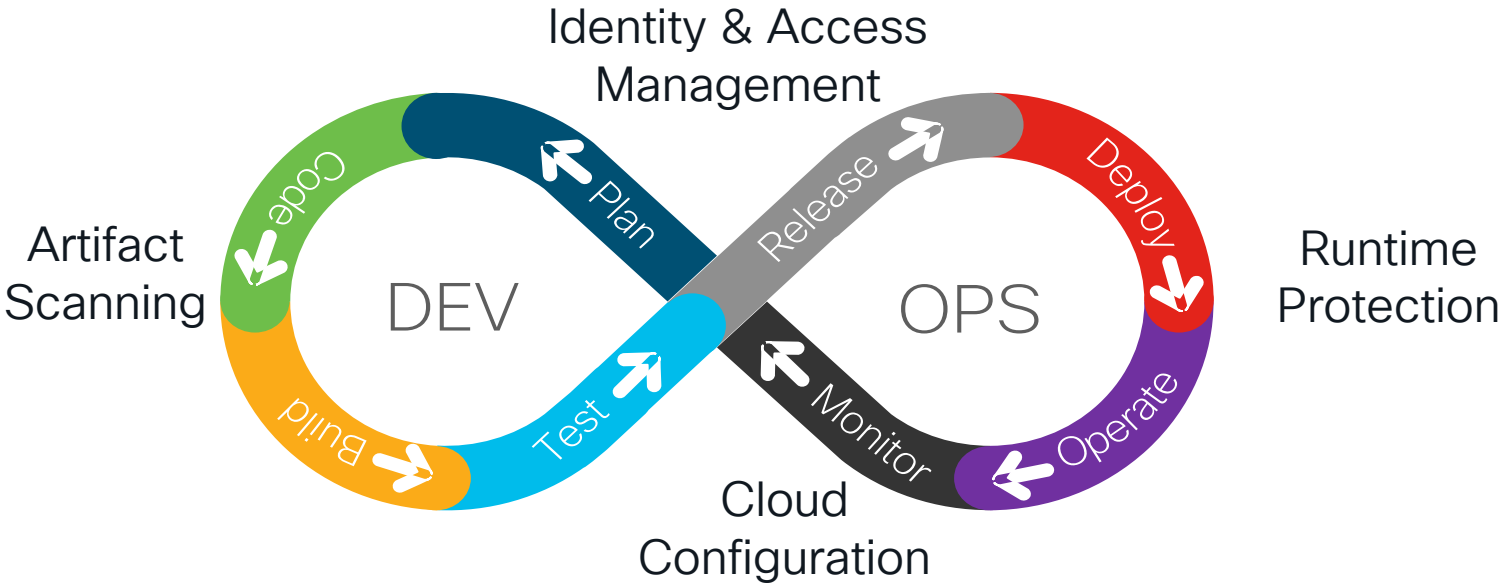
In 2022, enterprises used tools from **10 different vendors** for the life cycle protection of their cloud-native applications

-Gartner

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protecting Apps from Development to Runtime

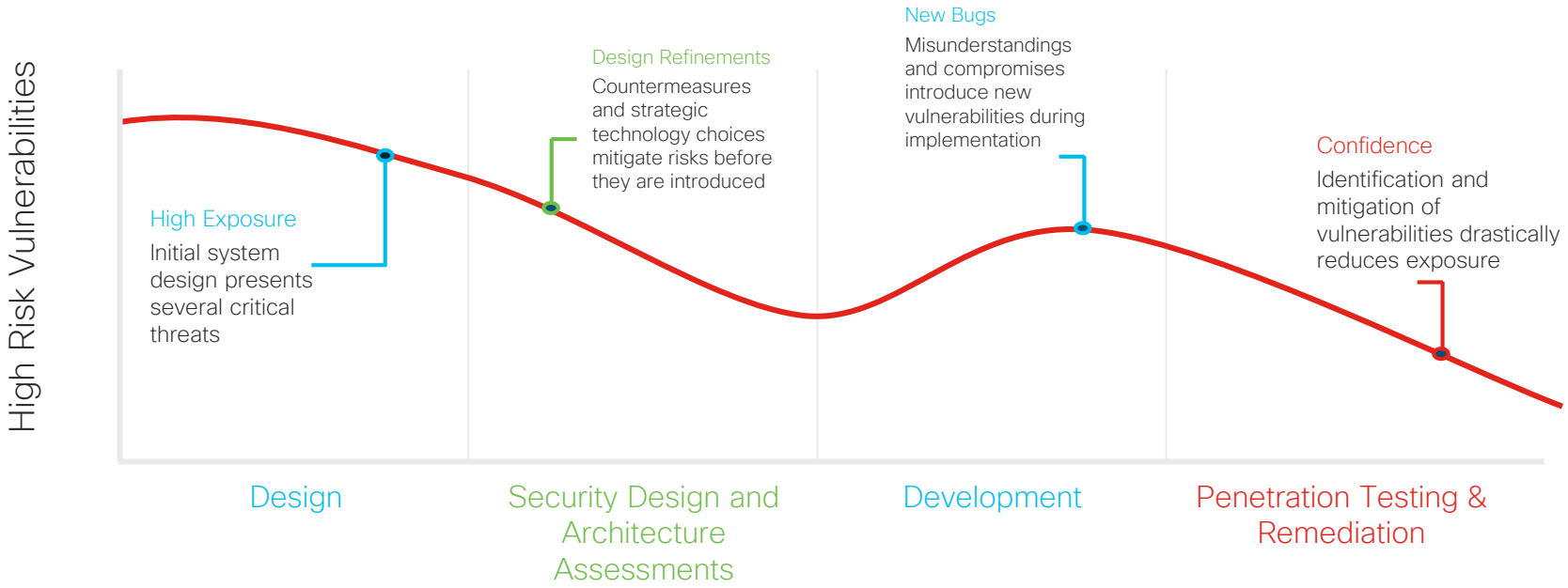
Cloud Native Application Security Requirements



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Shifting Left or Right

Minimizing Vulnerabilities Throughout the Lifecycle



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Specific Services

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

Applications and Systems	Networking & Infrastructure	Physical Components or Operations
• Application Penetration Test and Security Assessments • Application Design Assessment • Code Review • Software Development Lifecycle Assessment and Advisory • Cloud Application Migration • Threat Modelling	• 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 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.

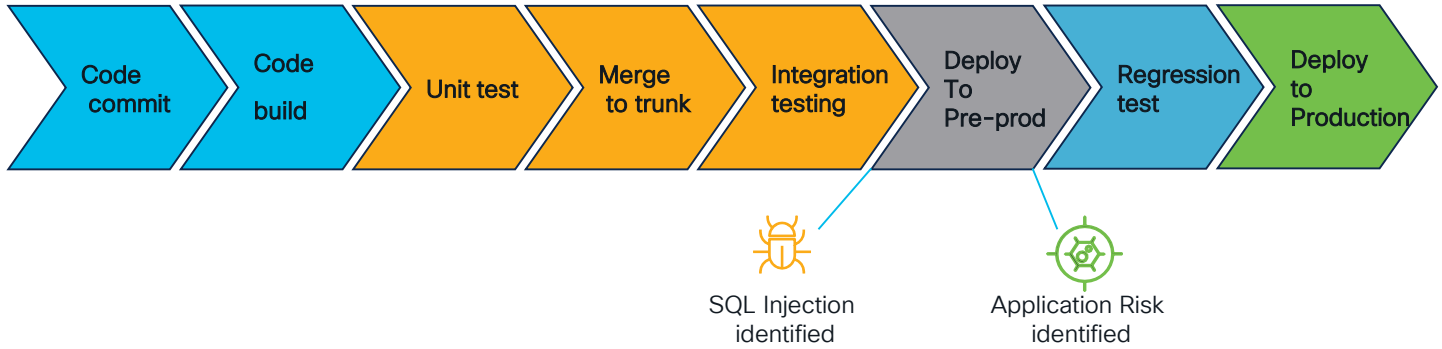
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 & security risks (example)

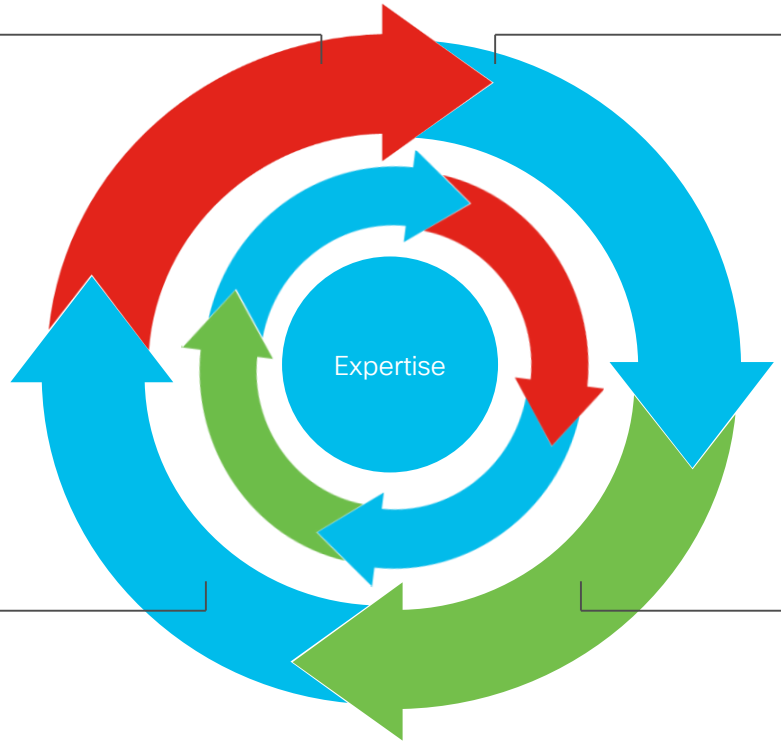


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

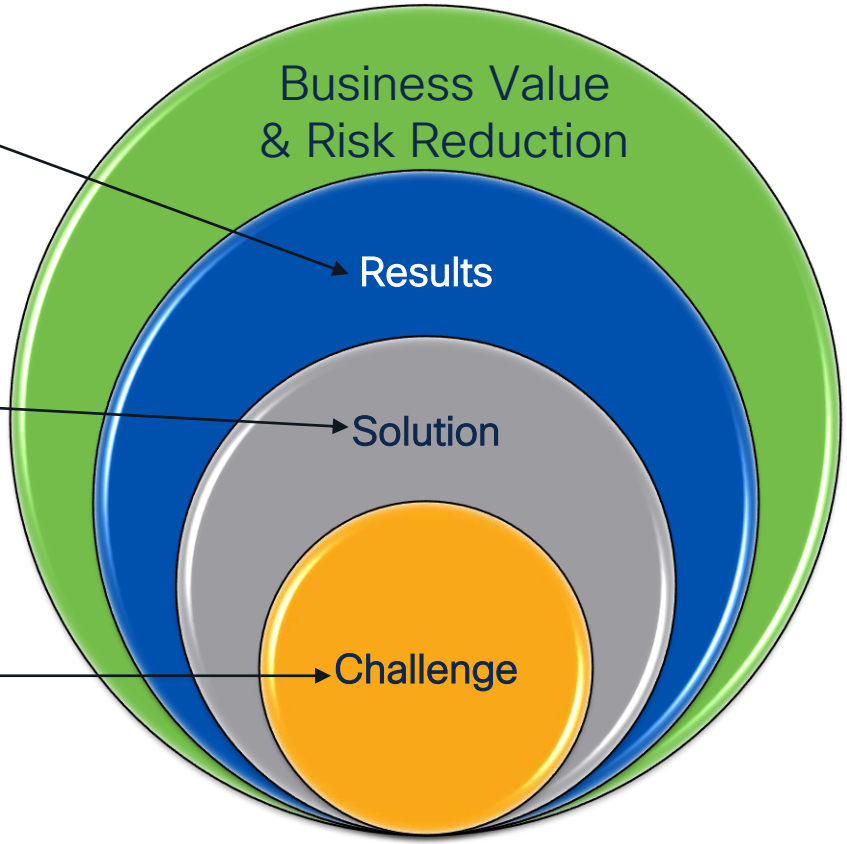
Example: Mobile Application

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



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Global Cybersecurity Talent Shortage

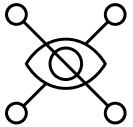
Cloud Native Security Challenges

#1

Barrier to Cloud Adoption: Insufficient Training

3.4M

Global shortage of cybersecurity professionals



50%

Percentage of cybersecurity incidents that will be due to lack of talent or human failure by 2025

- Exponential Growth of Threats
- Security as a Mainstream Need

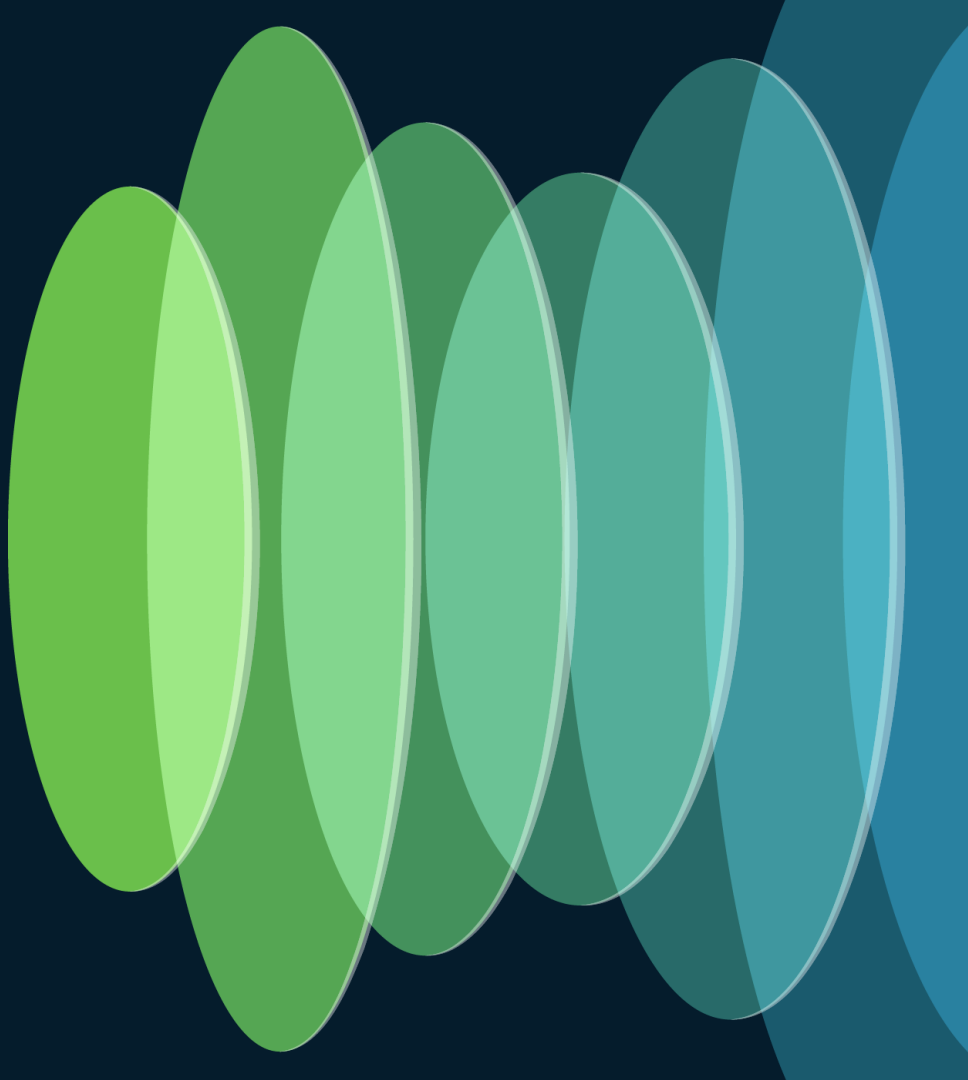
- Specialized Skills
- Dynamic Field

- Limited Training Programs
- "Experience Paradox"

- Burnout
- Perception of Cybersecurity

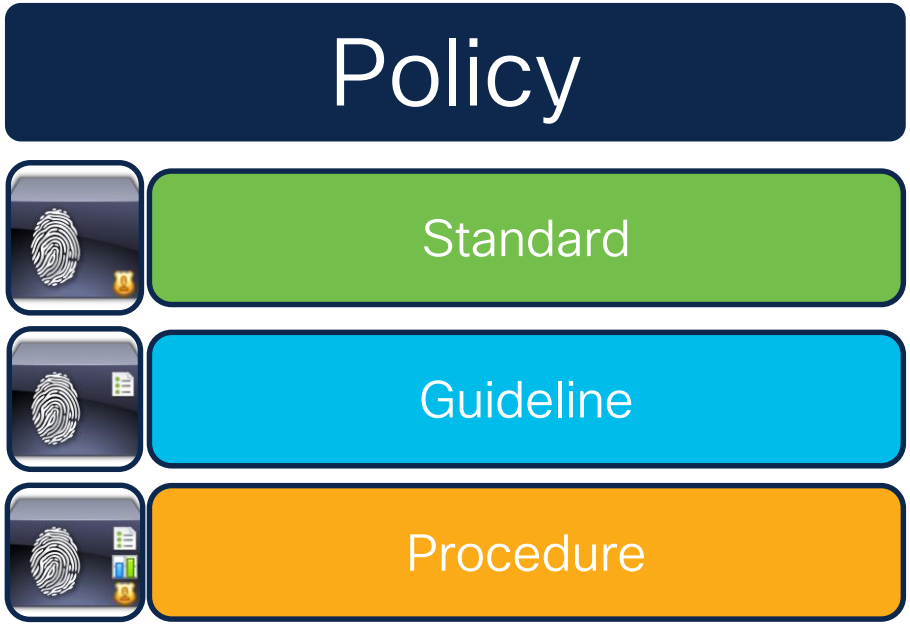
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

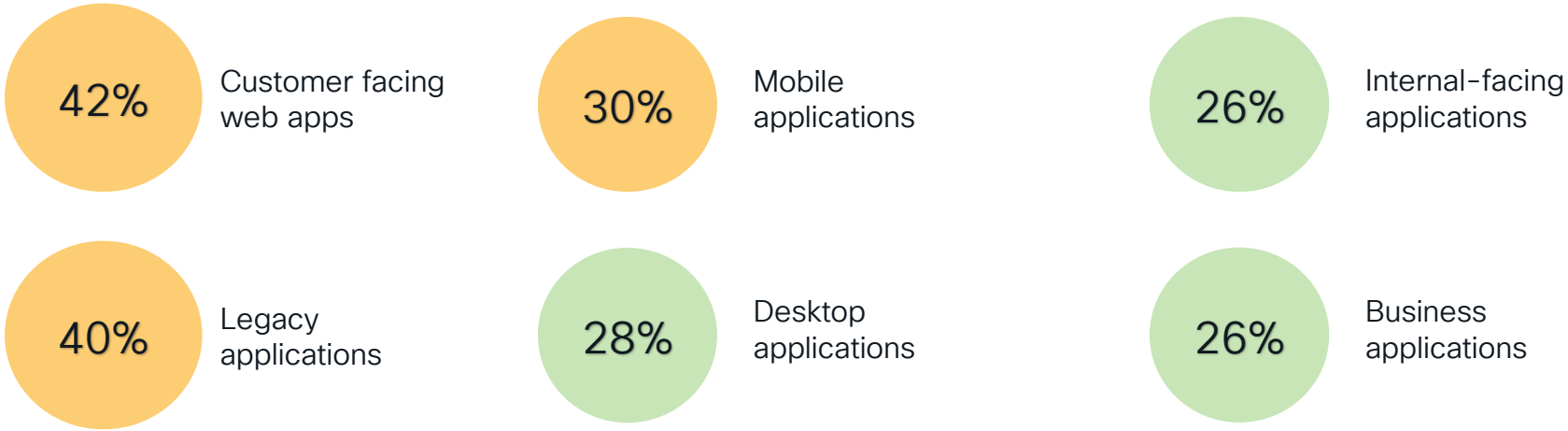
- HIPAA
- GDPR
- FERPA
- COPPA
- PIPEDA
- PHIPA
- CCPA
- PCI
- Continually assessing regs

Cross-Border Transfers

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Business applications with highest security risk

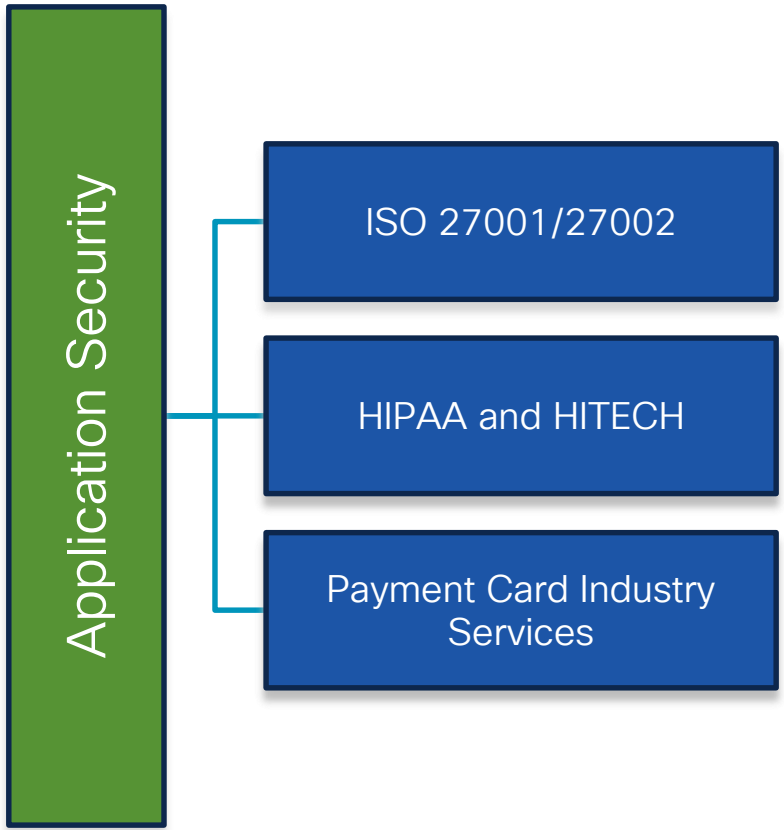


Source: Cybersecurity insiders, Application Security Report 2022

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

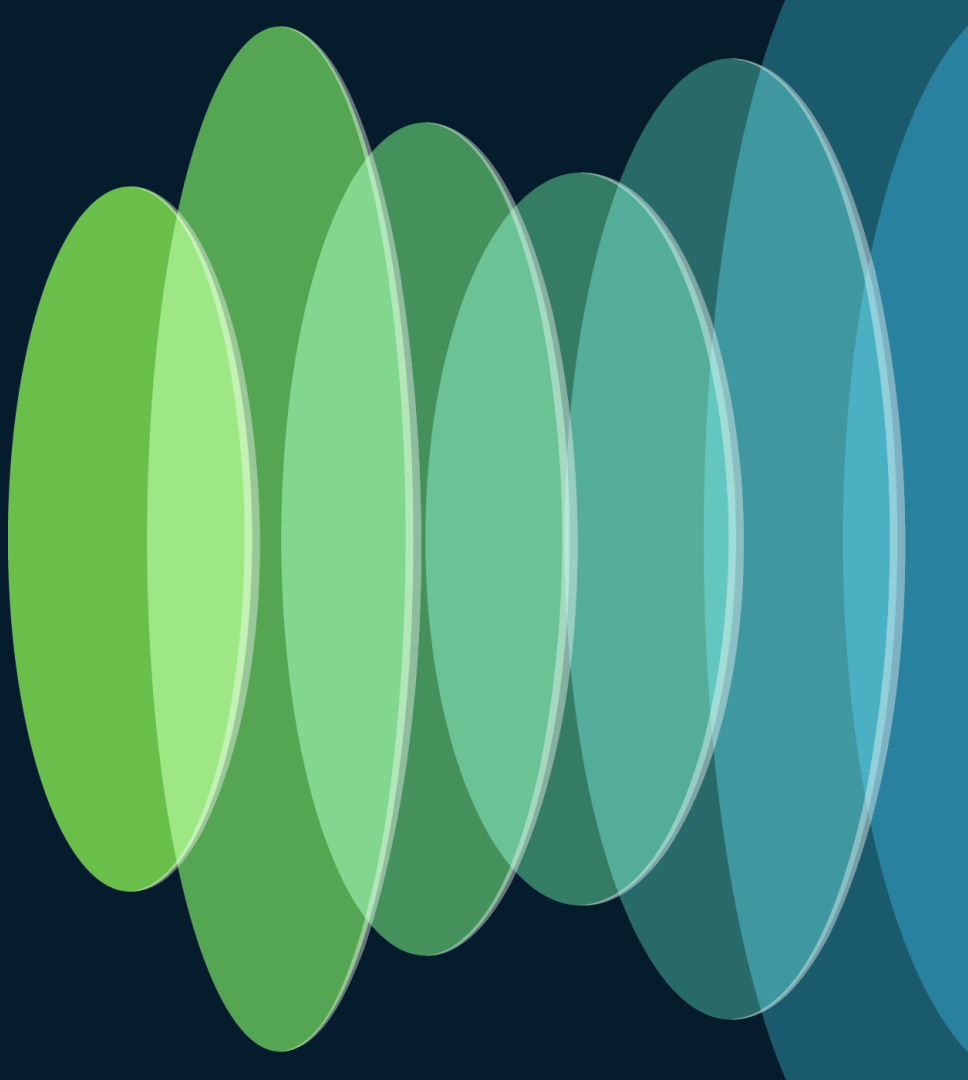
Application alignment with compliances

- **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.



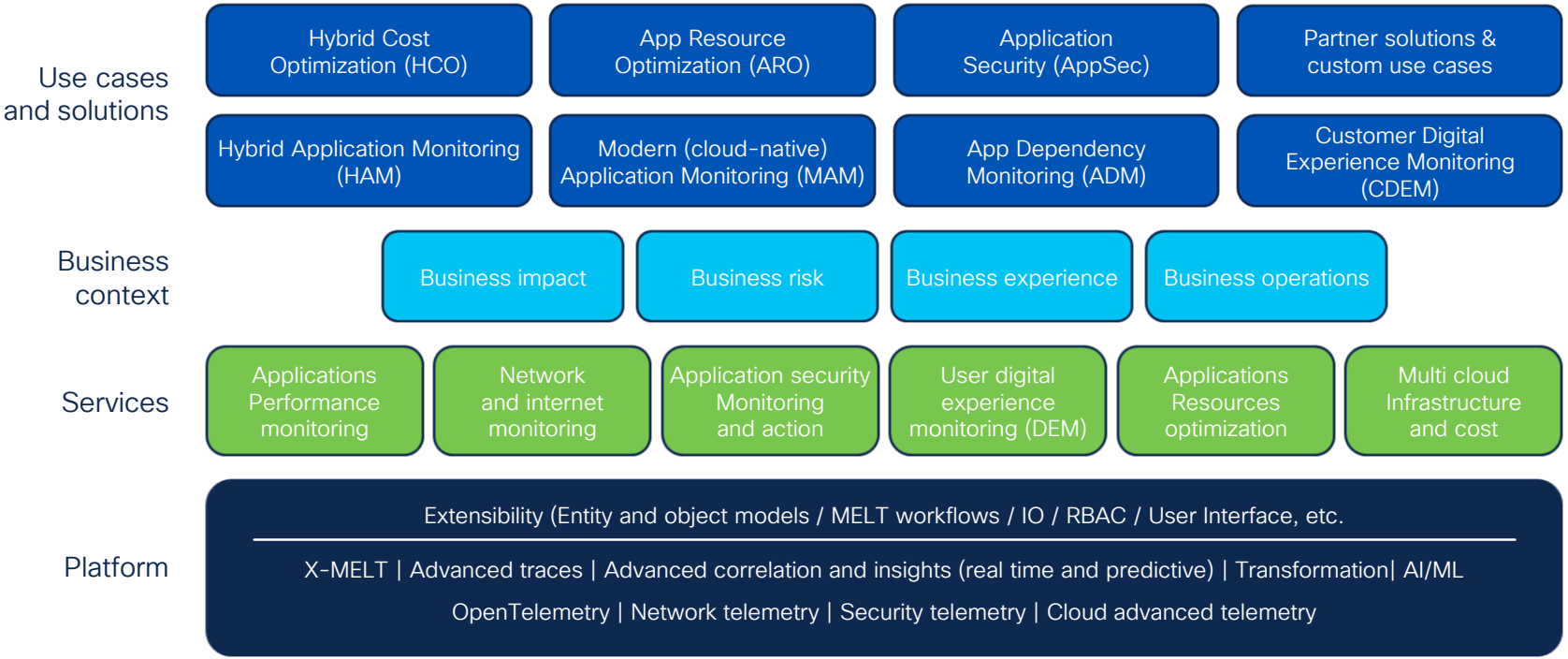
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

App security within Full Stack Observability



cisco Live!

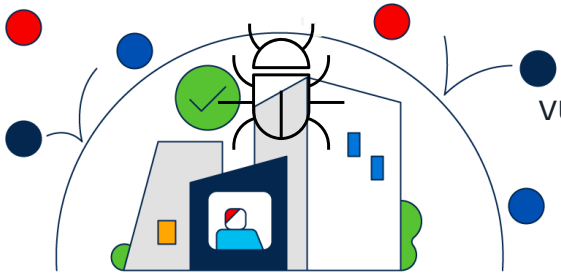
Cisco Full-Stack Observability Architecture Foundation



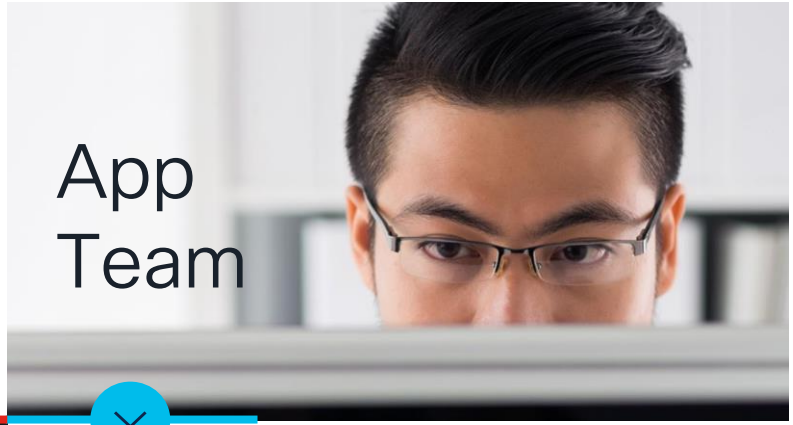
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Full Stack Observability

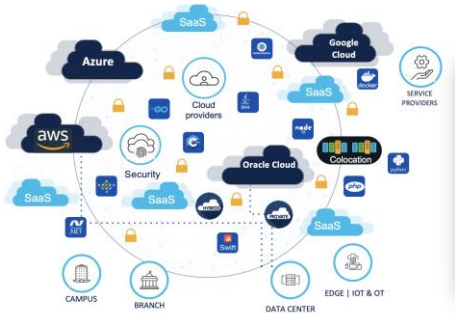
With focus on Application Security



Focused on vulnerabilities & threats



Focused on velocity & user experience

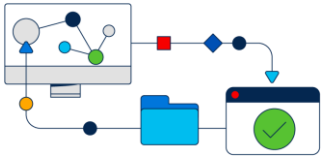


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Application Use Cases at Runtime

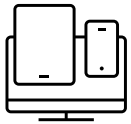
Fast to deploy, immediate time to value, and performant for all environments

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

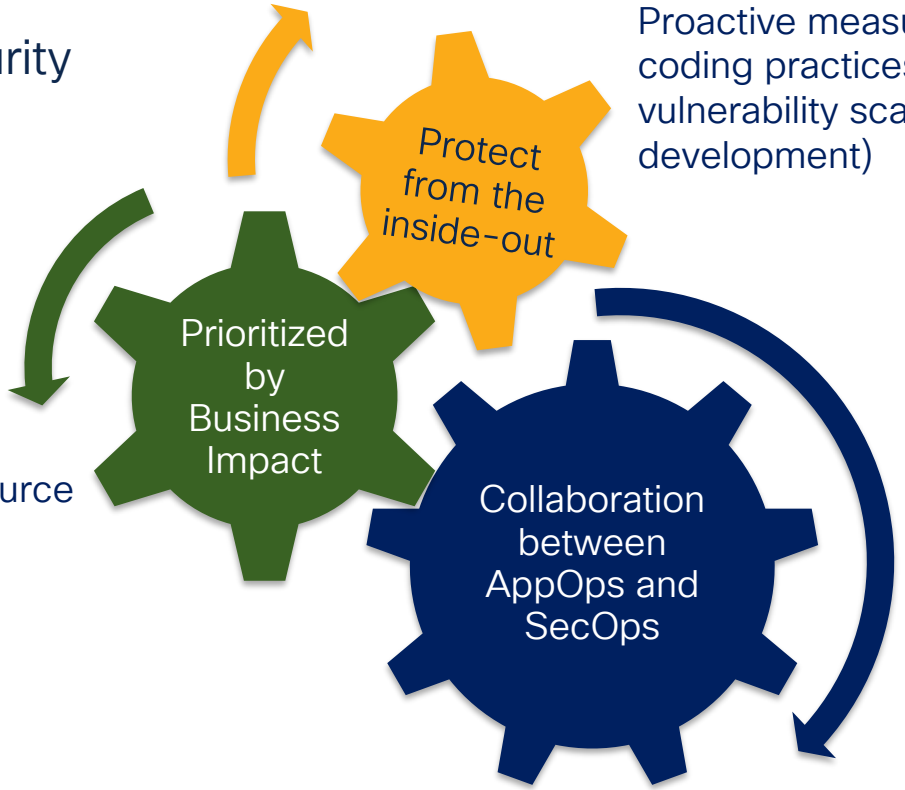
Policy level blocking that stops bad actors… even if vulnerabilities exist

Security insights provided with Application and Business context

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Security at the center of business

Application Security



Proactive measures (secure coding practices, vulnerability scanning during development)

Focus on highest risk areas for efficient resource allocation.

Bridging the gap between development agility and secure deployment.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

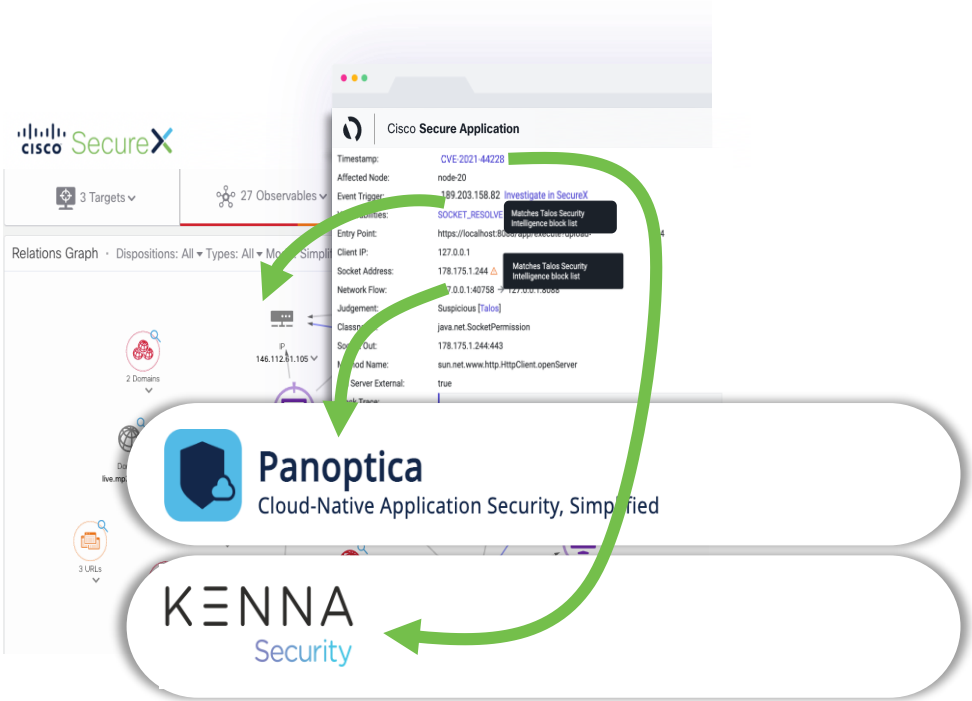
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco FSO Security solution

Extended detection and response to boost productivity

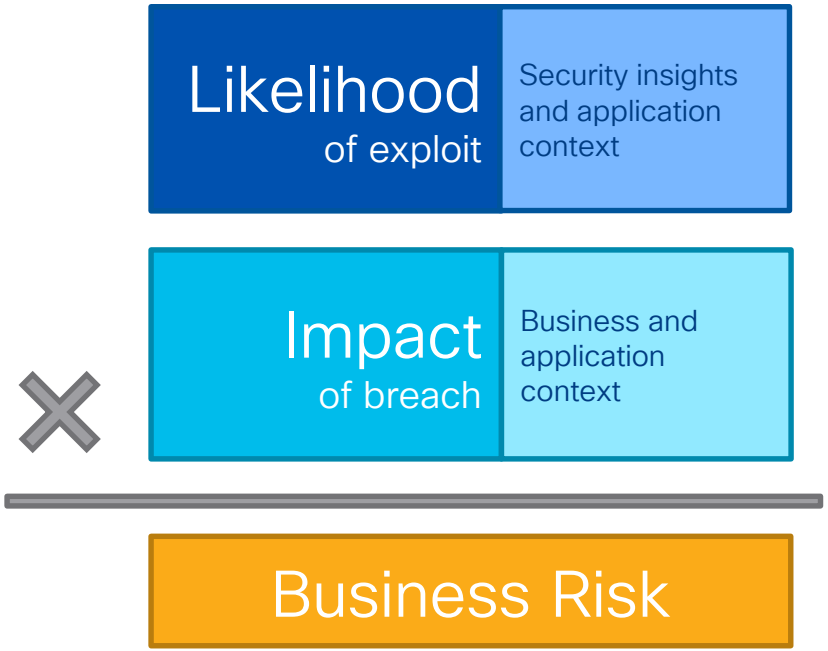
- Integrated with Kenna Security
- Detailed vulnerabilities insights to prioritize right vulnerabilities to address
- Integrated with Panoptica
- Expose 3rd-party API security issues (Vulnerabilities, *TLS issues..)
- Integrated with Talos Intelligence
- Identify bad actors
- Hunt for threats in SecureX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

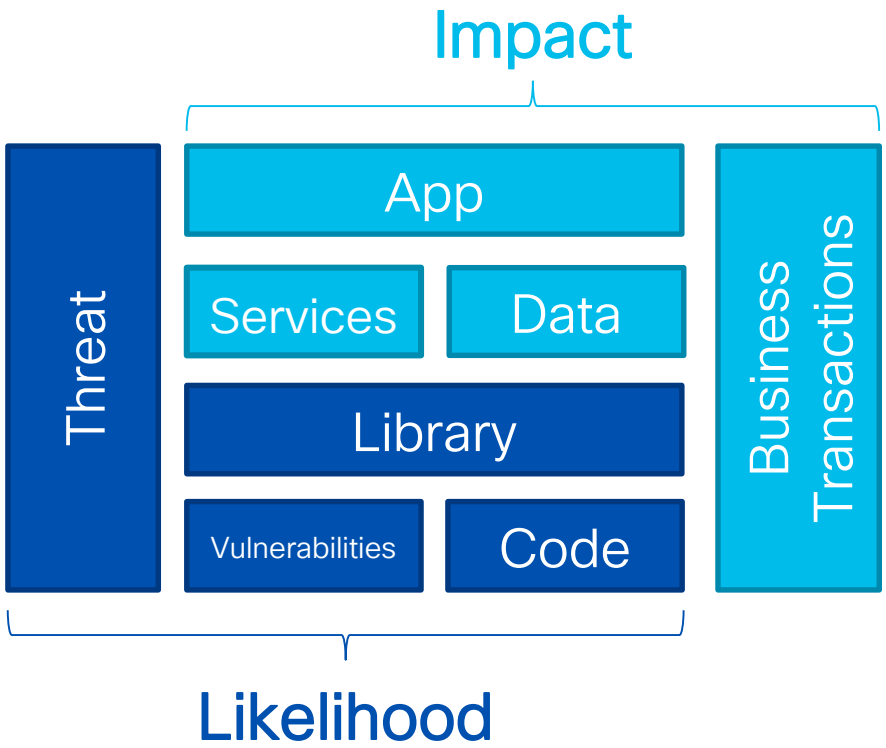
*Transport Layer Security



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is Business Risk Observability?





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

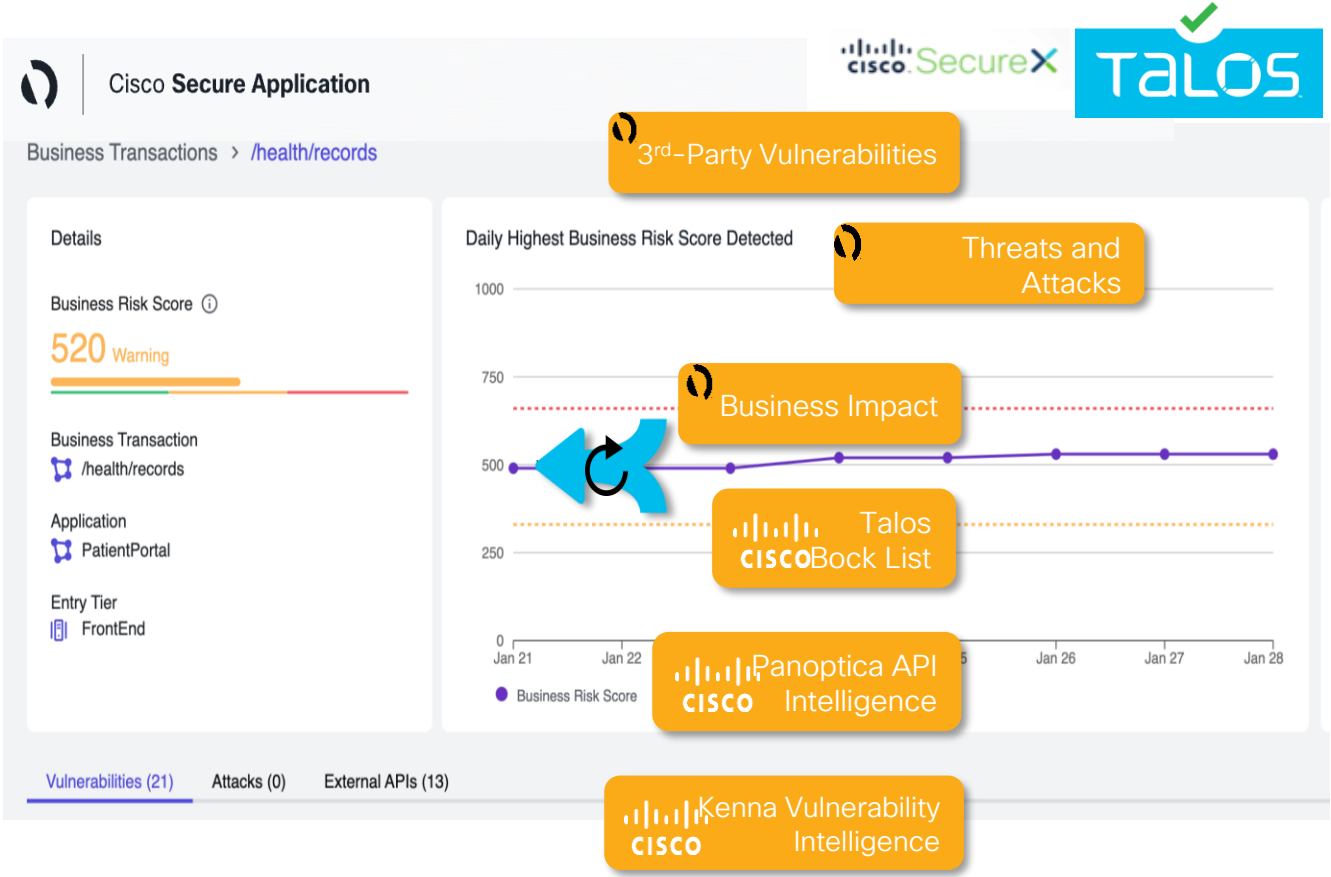
Vulnerability Classification (example)

Security Impact Rating (SIR)	Classification Tag	Operational Mitigation Target	Response Type
1	Critical	48 Hours	Drop Everything / Impacting or High Exposure
2	High	48 Hours	Top of List / Impact or Exposure Highly Likely
3	Medium	Standard Patch Management Lifecycle	Vulnerabilities that are unlikely to be exploited and therefore do not justify unplanned remediation activities. In most cases, the fix is implemented during a routine OS or application upgrade, system/application decom, or patch cycle.
4	Informational	Standard Patch Management Lifecycle	The vulnerability poses little risk and does not require action.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

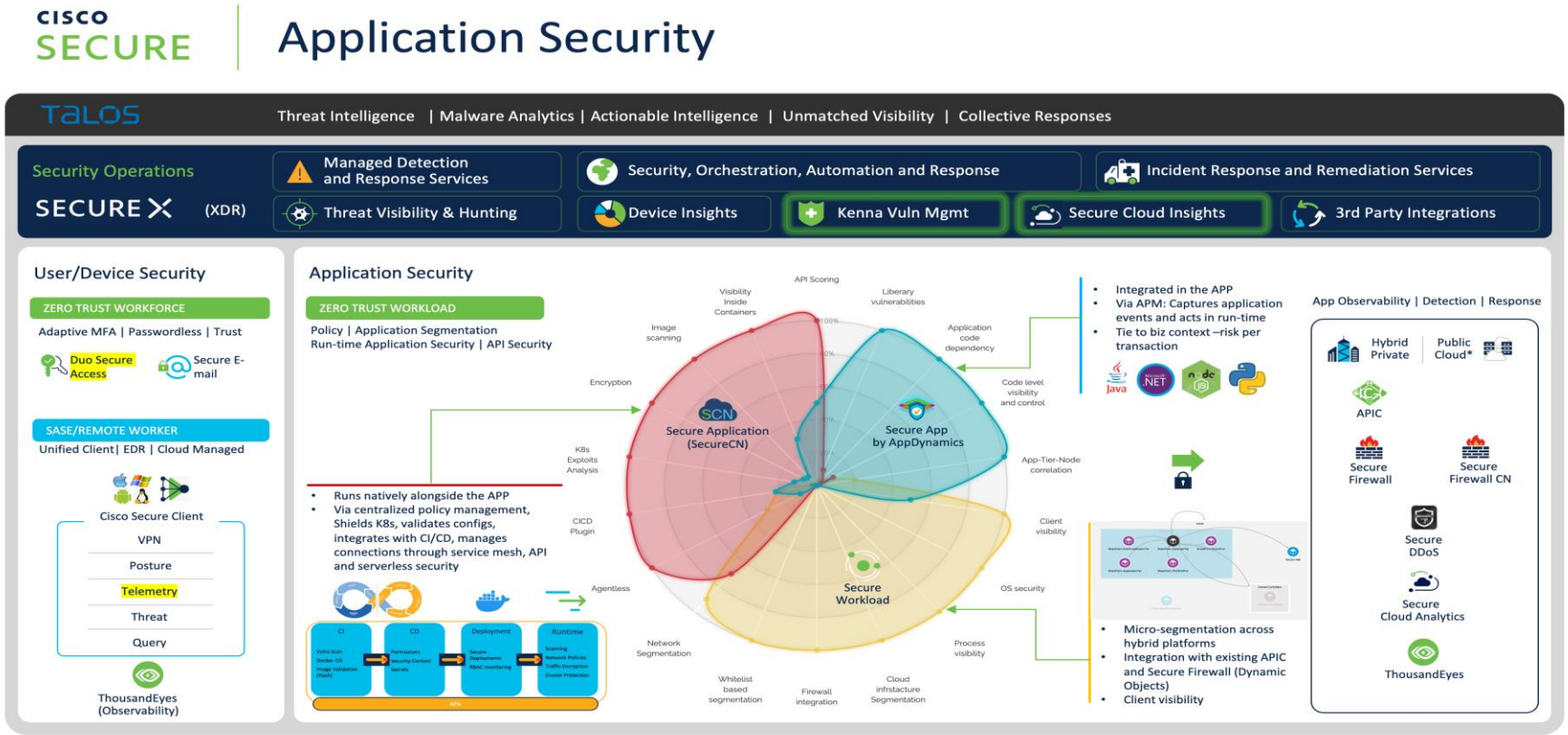
Risk Scoring

- 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

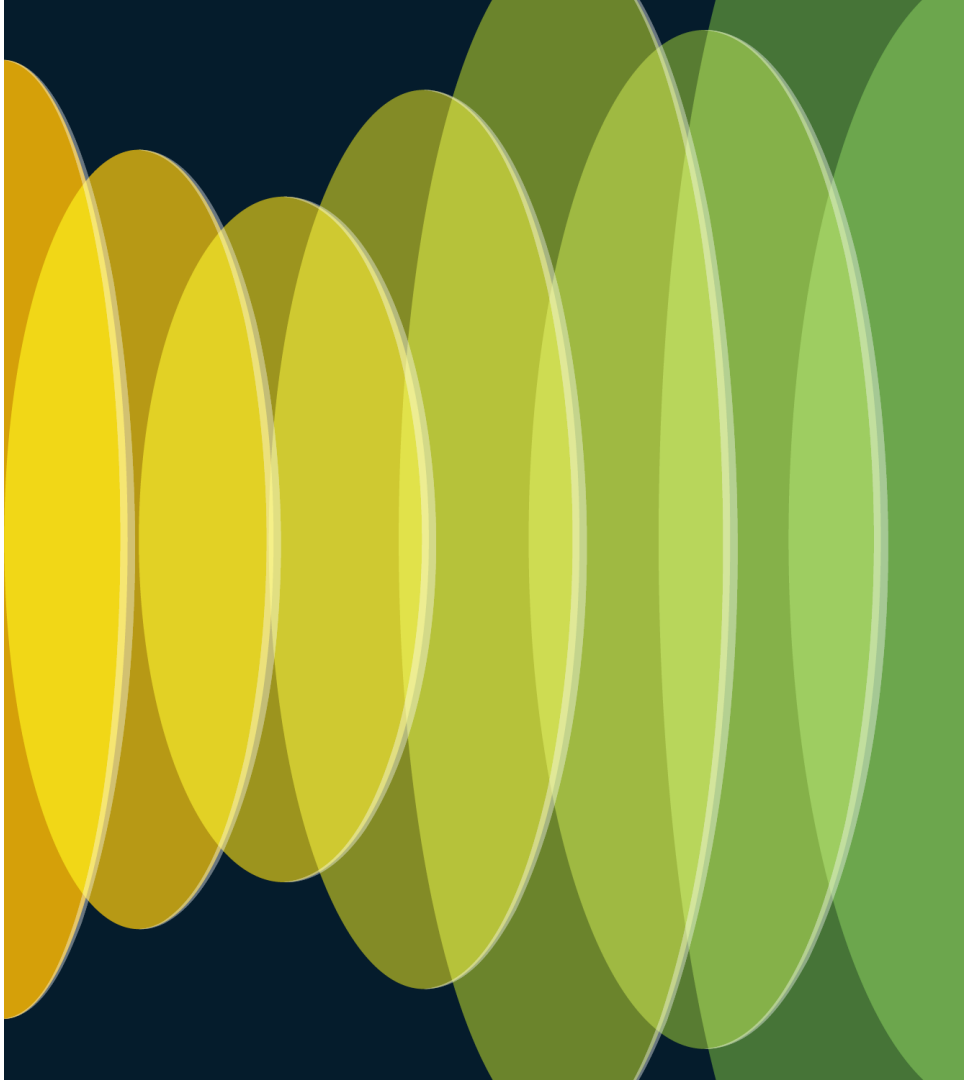


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco approach to Application Security



Demo



Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

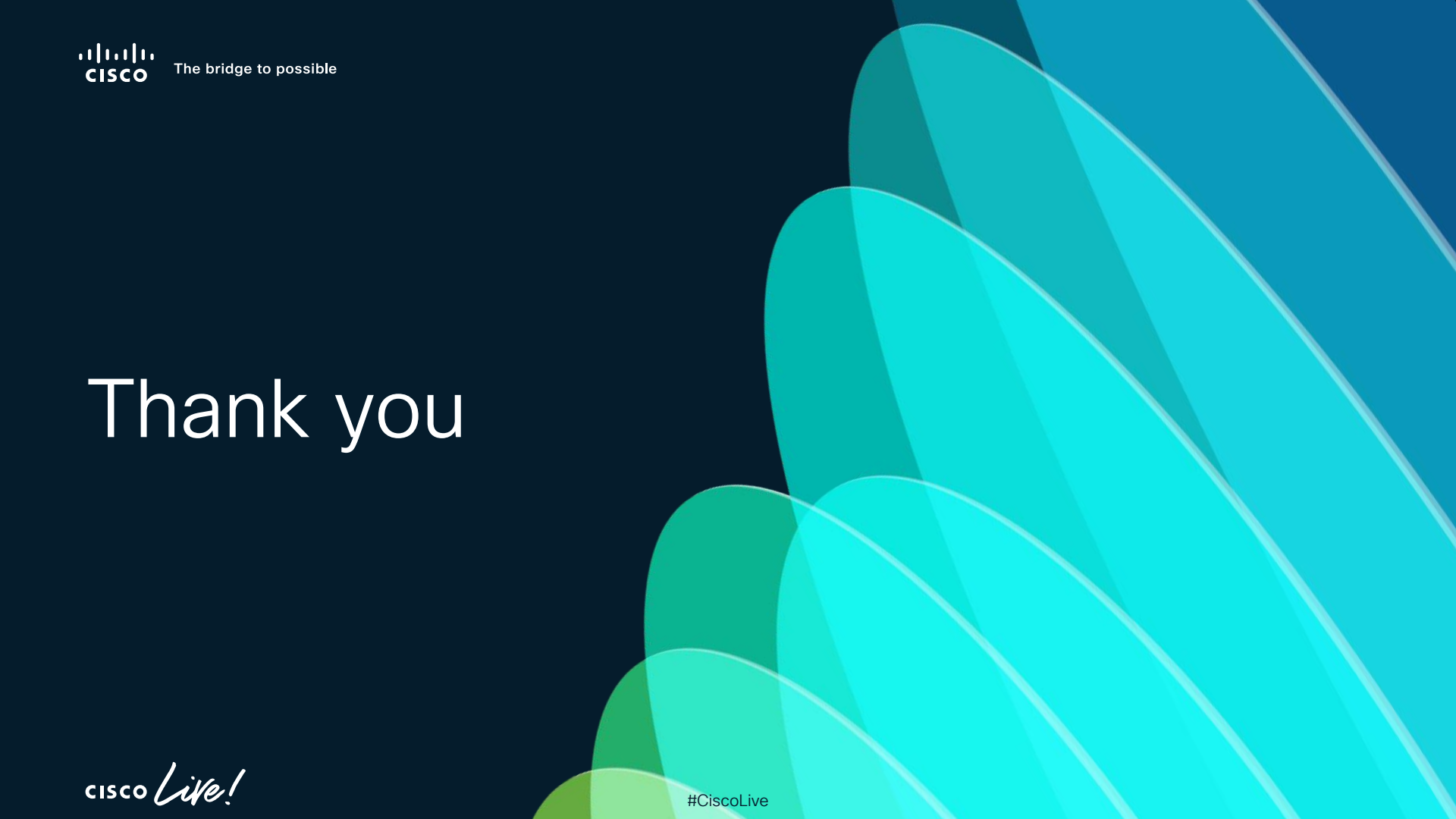
Continue your education

- 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

Contact us at:

Luis Bravo (lubravo@cisco.com)
Marc Buraczynski (maburacz@cisco.com)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public


The bridge to possible
Thank you
cisco Live!
#CiscoLive