RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **DSO-W09**

Product Security at Scale: Lessons from Comcast

Sandra Cavazos

Vice President, Product Security and Privacy
Comcast

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

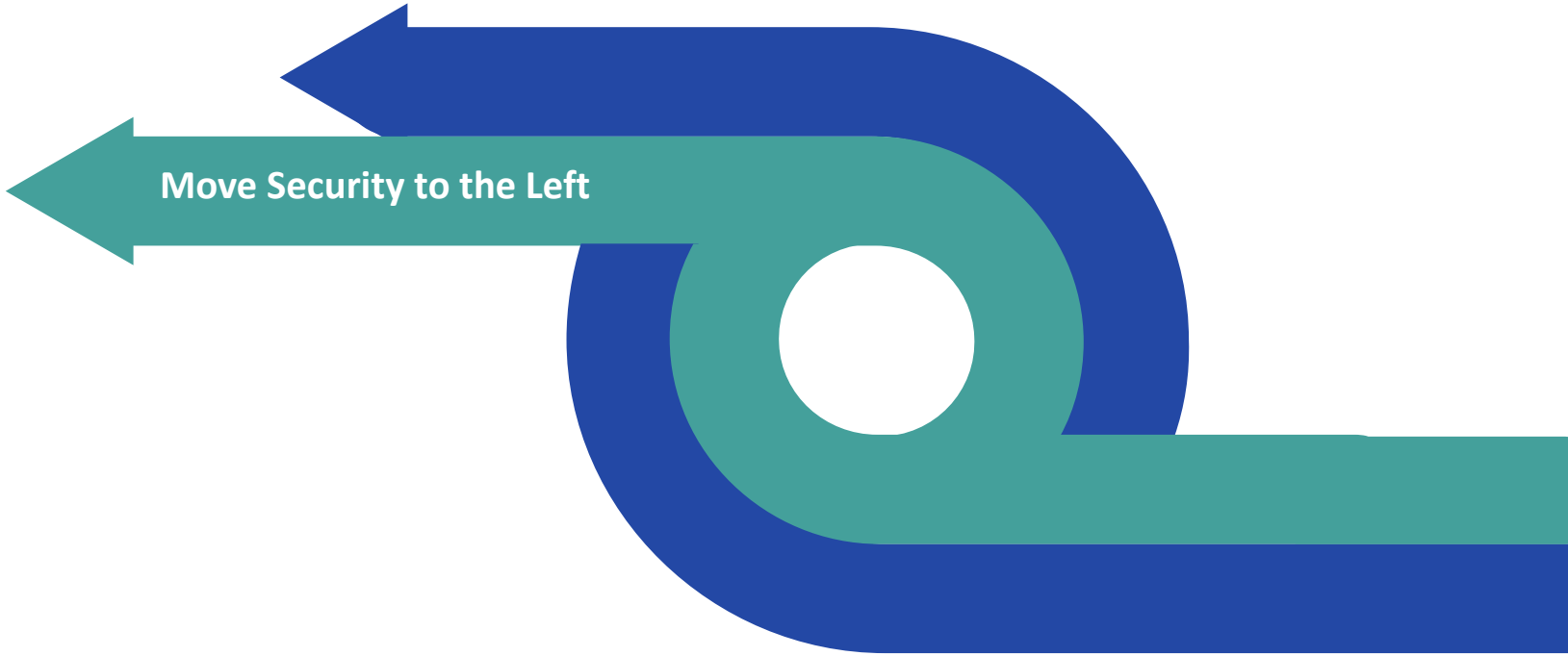
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Goal of the Secure Development Lifecycle

Reduce risk of incidents

Resolve vulnerabilities early

Reduce development cost



COMCAST

Priority of the Secure Development Lifecycle

Business Drivers

Brand reputation and future business growth rely on having and providing secure products and services

Threats

Attacks are growing in sophistication, with an increased focus on espionage and monetary gain (e.g., ransomware), but occasionally with the simple intent of causing disruption

Technology

Sophisticated hacking tools are being developed and deployed by a wide variety of entities, from individuals to organized groups to nation states

Compliance Concerns

Government, industry, and customer contracts require security assurances that meet both general and domain-specific regulations

COMCAST

Comcast SDL Guiding Principles

Building security in
over bolting it on

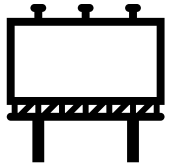
Implementing features securely
over adding security features

Iterating and learning continuously
over gating decisions

Empowering development teams
over relying on security specialists

Growing a culture of secure practices
over policing enforcement

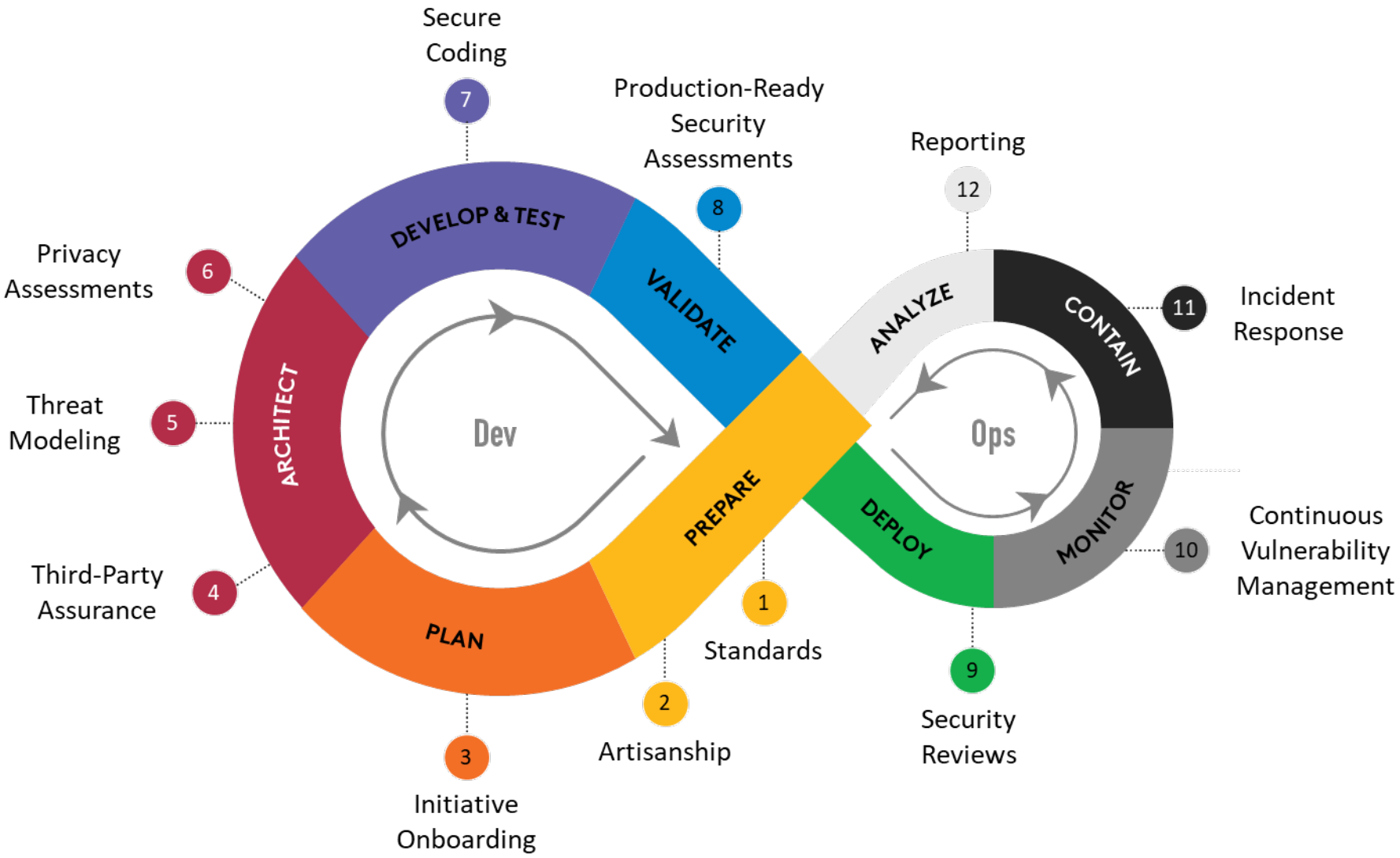
Lesson #1



Branding a company-wide SDL program and presenting consistent taxonomy drives alignment and measured progress.

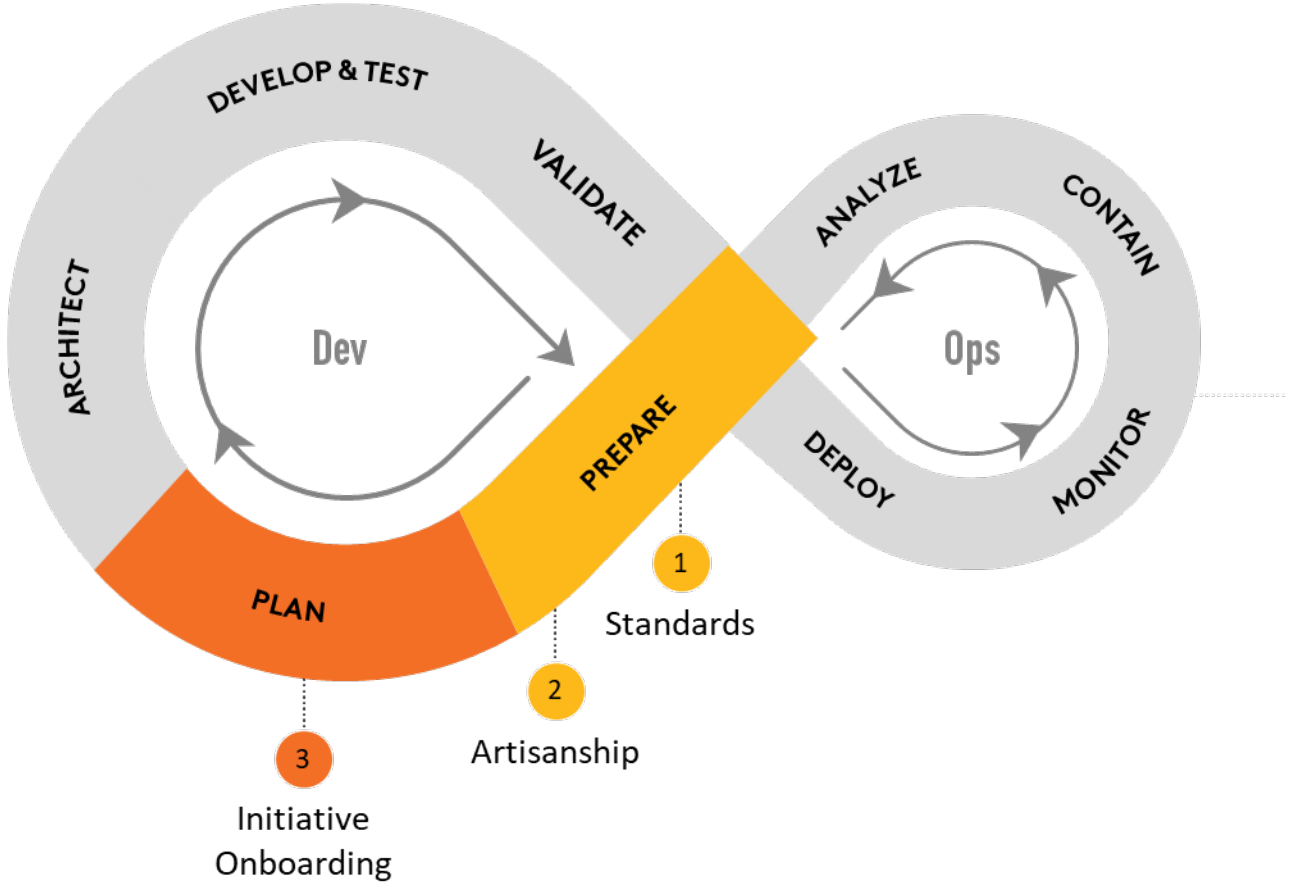
COMCAST

Secure Development Lifecycle Practices



COMCAST

Prepare and Plan (Practices 1-3)

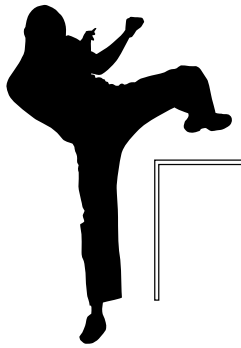


COMCAST

Practice 1: Security Policies, Standards, and Guidelines

COMCAST

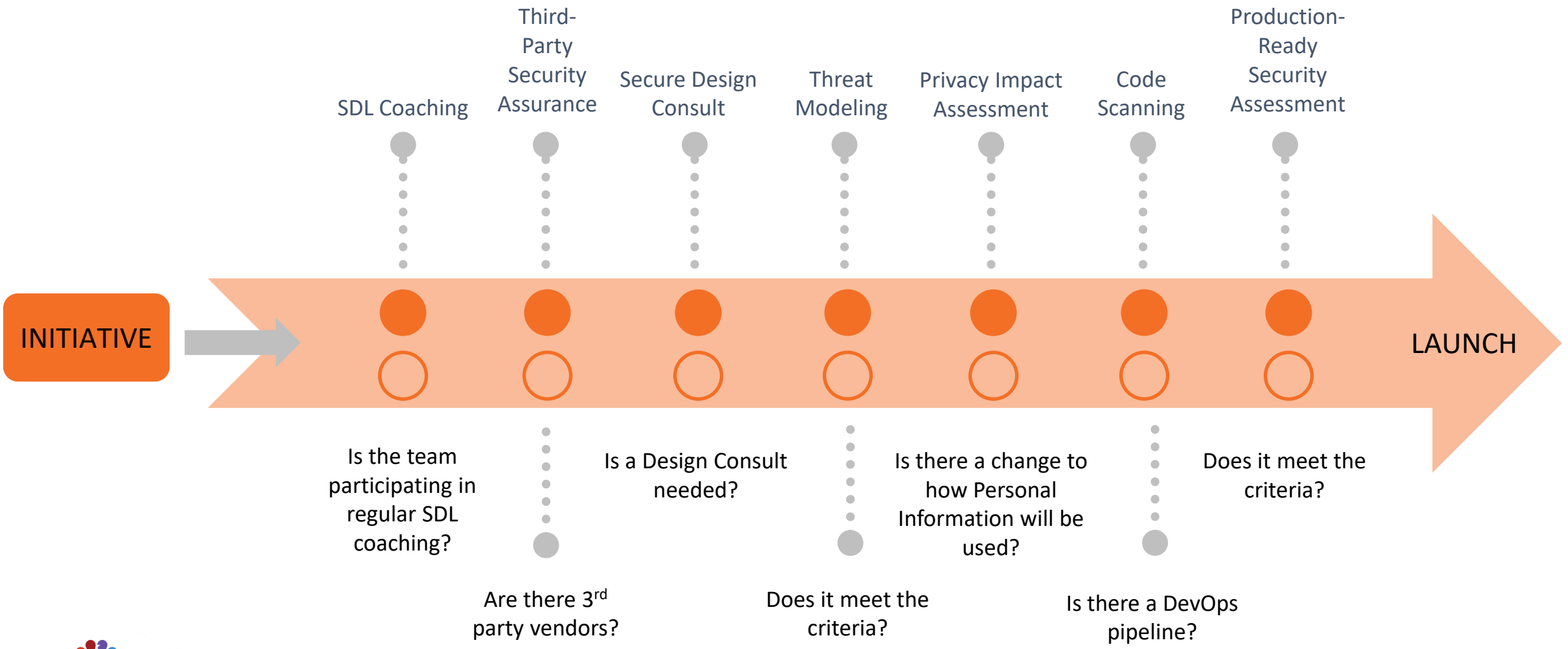
Practice 2: Artisanship



LEVEL 01	LEVEL 02	LEVEL 03	LEVEL 04	LEVEL 05	LEVEL 06
WHITE BELT	YELLOW BELT	ORANGE BELT	GREEN BELT	BROWN BELT	BLACK BELT
Required training for all employees covering topics such as phishing, email compromise, passwords, secure Wi-Fi use and URL hygiene	Gain an understanding of Comcast's security philosophy, typical threats, and the ways to protect our customer's security and privacy.	Technical security training for specialized areas of product development.	Practitioner-level training that increases a learner's security knowledge by providing skill-based training for specialized areas of product development.	Technical mastery of security that fosters and recognizes sustained improvements in security practices that have Comcast-wide impact.	Recognizes individuals that acquire expert and/or specialized security knowledge that make significant contributions to Comcast and the industry.

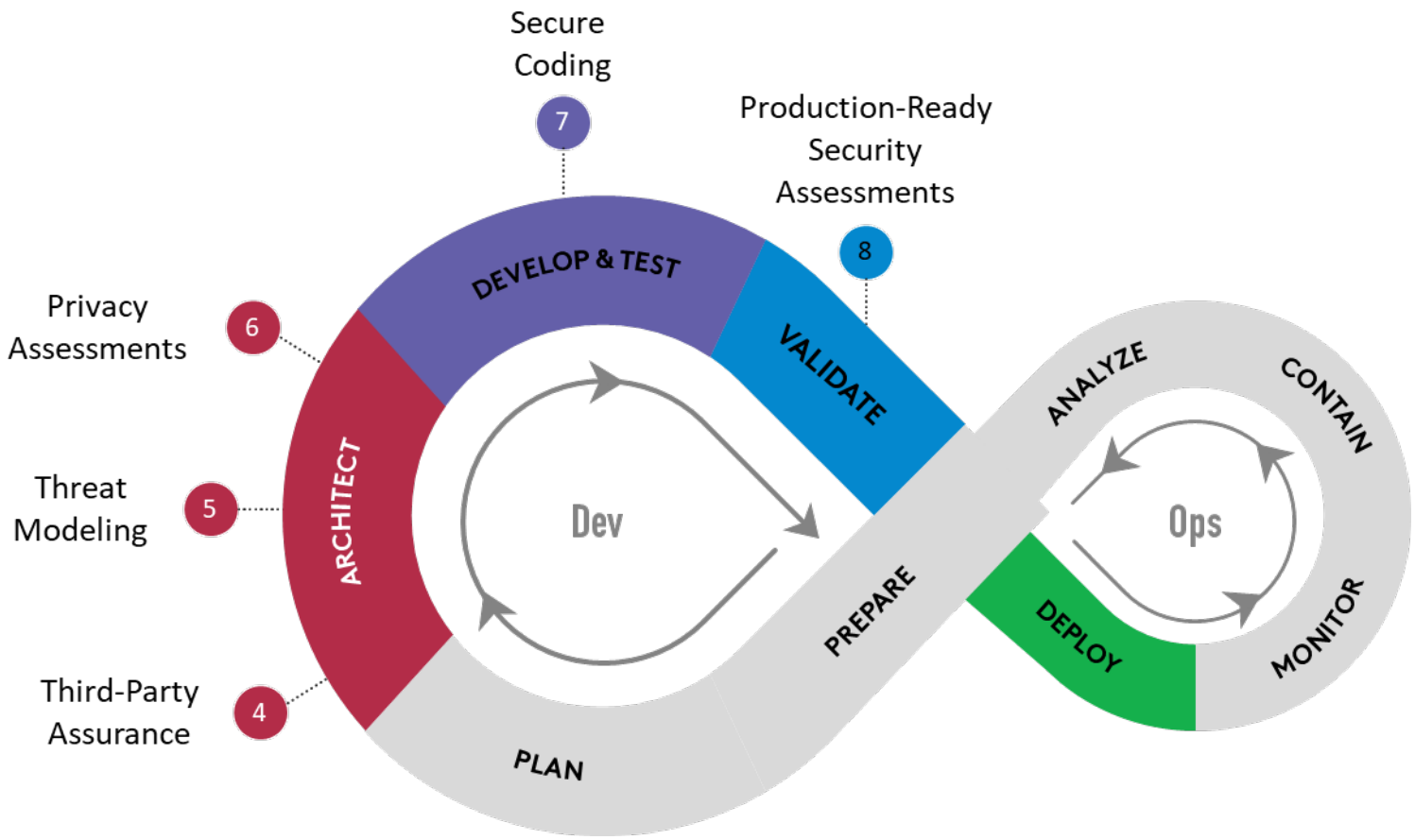
COMCAST

Practice 3: Initiative Onboarding



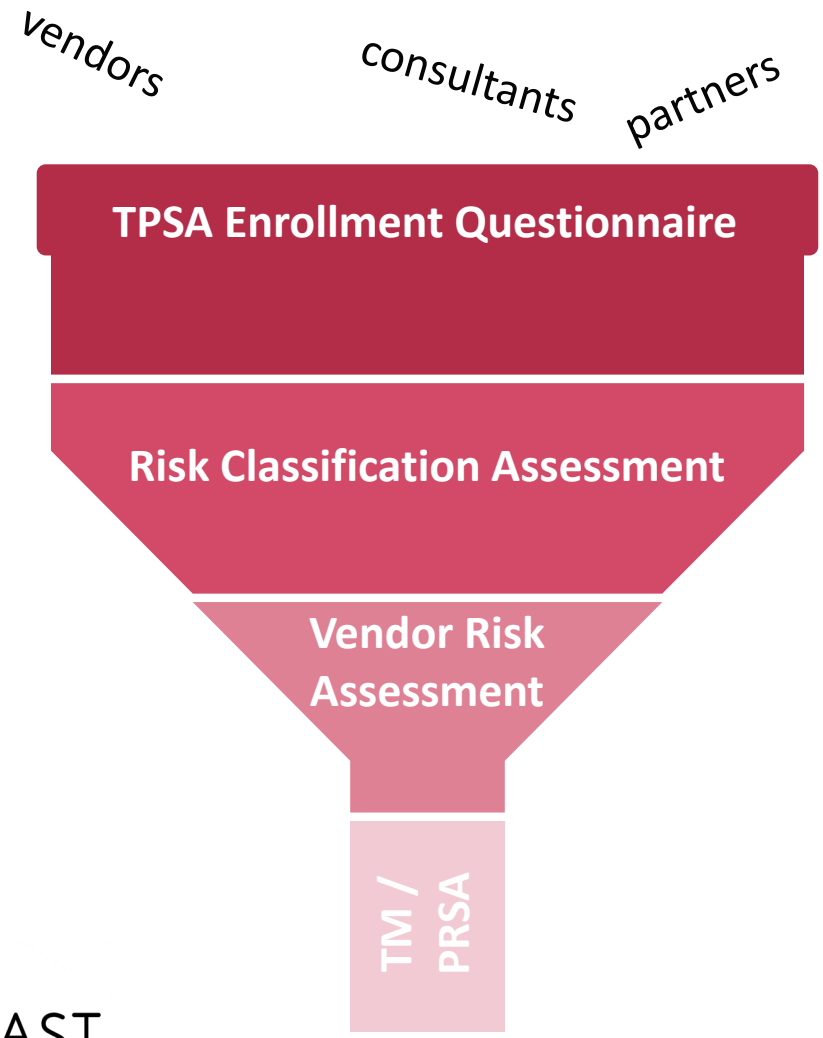
COMCAST

Building in Security (Practices 4-9)



COMCAST

Practice 4: Third-Party Security Assurance



Three question survey covering data sharing, access to Comcast systems and software development

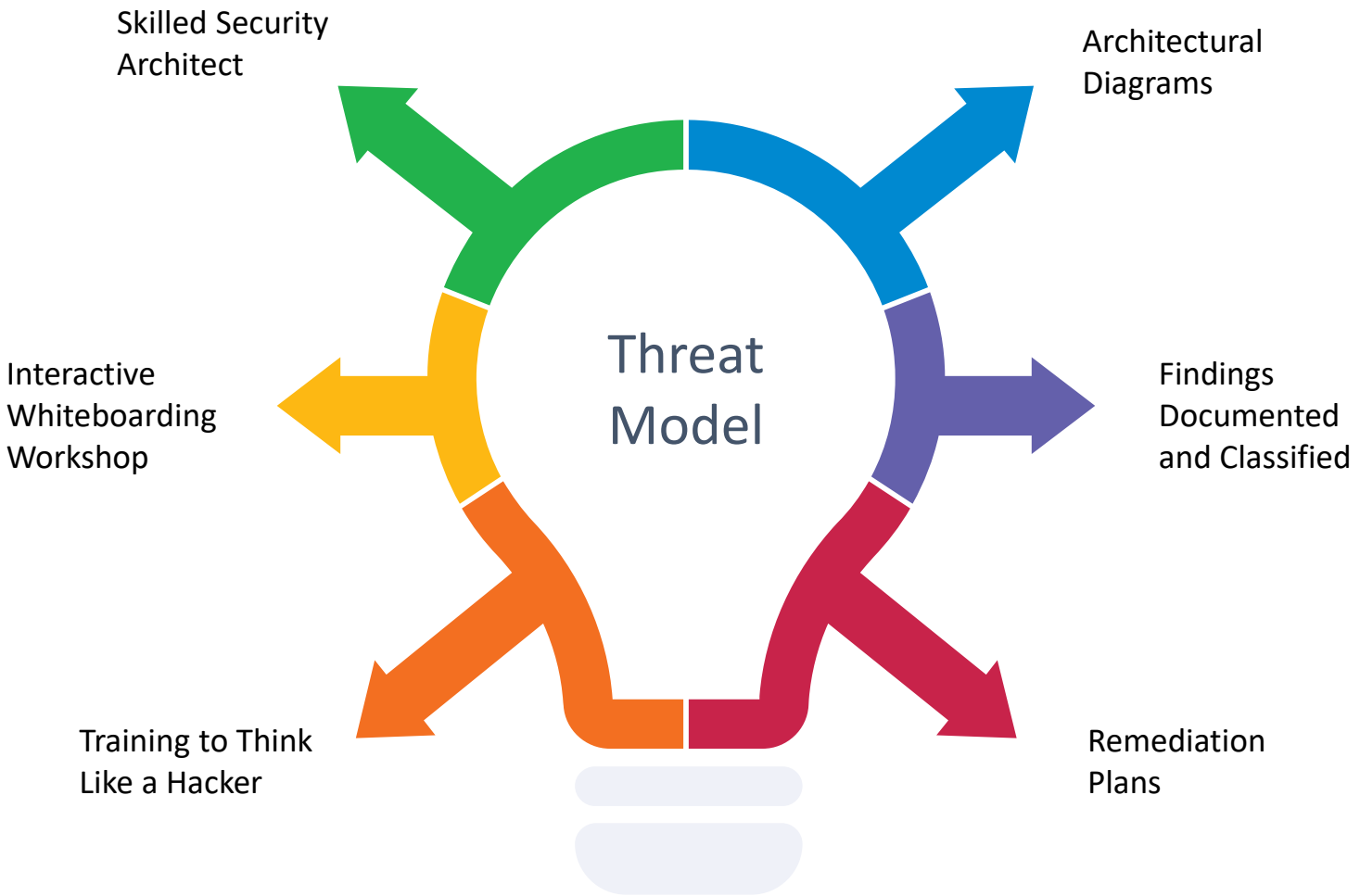
Assessment to determine the nature of services, data elements that the vendor stores, processes, and/or transmits, and risk rating

In depth assessment to further understand the nature of the relationship with Comcast and the type of information being handled

Security assessments required for highest-risk vendor applications examining the implementation and integrations between systems

COMCAST

Practice 5: Threat Modeling



COMCAST

Lesson #2

Innovate for change, enabling threat models to address privacy risk and scale for large organizations

COMCAST

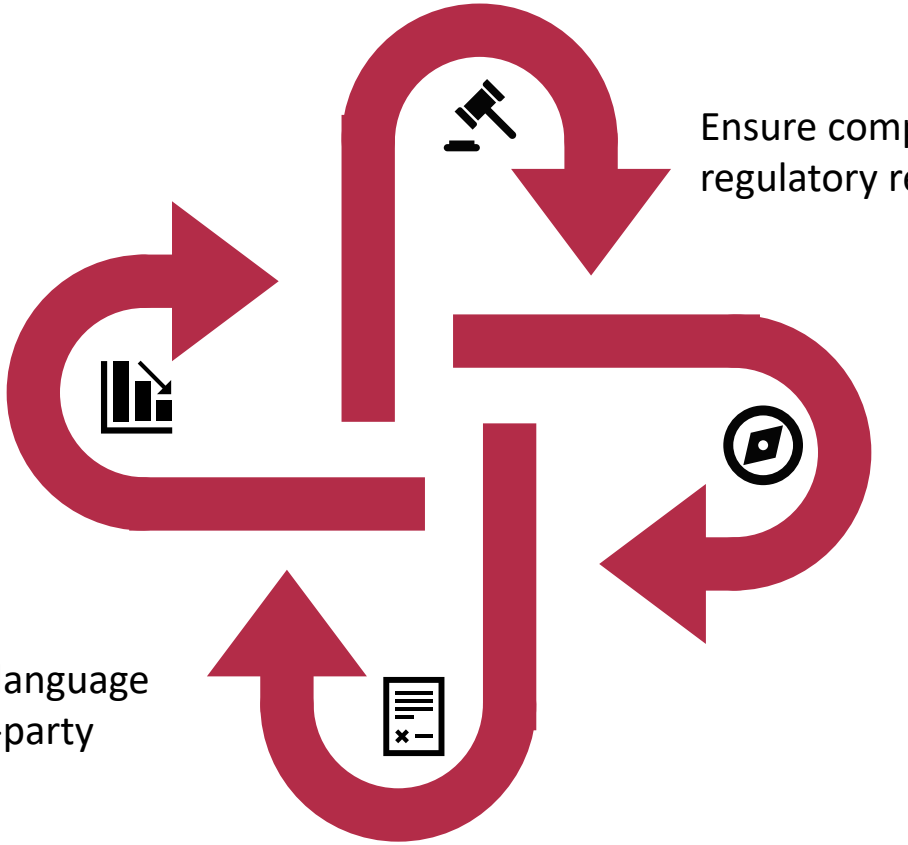
Practice 6: Privacy Impact Assessments

Ensure compliance with regulatory requirements

Ensure compliance with Comcast's internal policies

Inform contractual language for applicable third-party agreements

Identify opportunities to reduce privacy risk resulting from changes to design or implementation



COMCAST

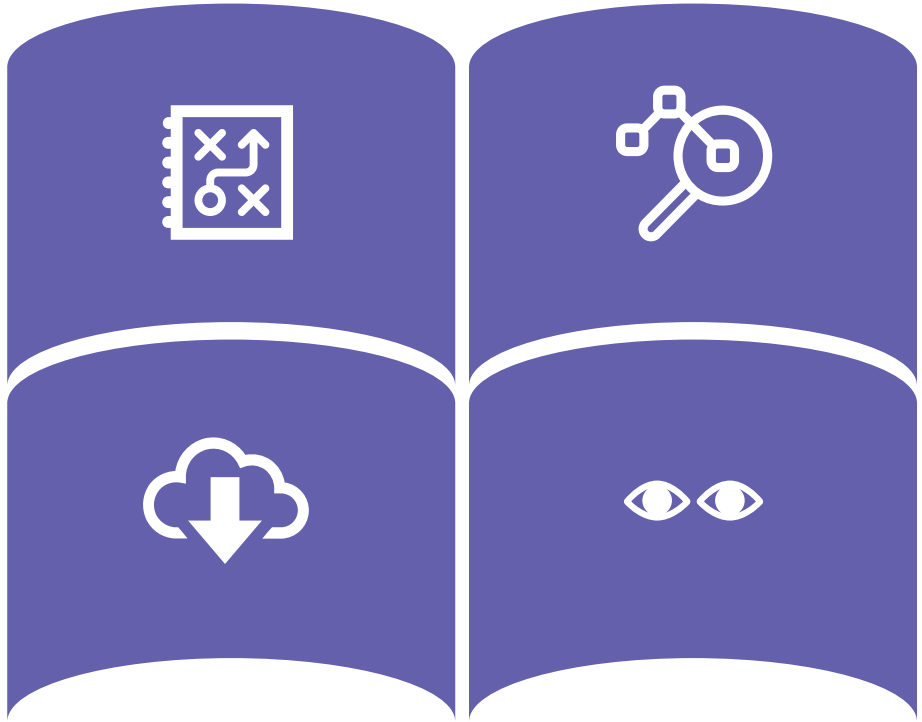
Practice 7: Secure Coding

Secure Design Patterns

- Use wherever possible to resolve recurring problems in an accepted, repeatable manner
- Contribute to the library

Software Composition Analysis (SCA)

- Analyzes 3rd party code
- Resolve high findings prior to each code merge



Primary Code Analysis (PCA)

- Can be Static Application Security Testing (SAST) or Interactive Application Security Testing (IAST)
- Resolve high findings prior to each code merge

Security Peer Review

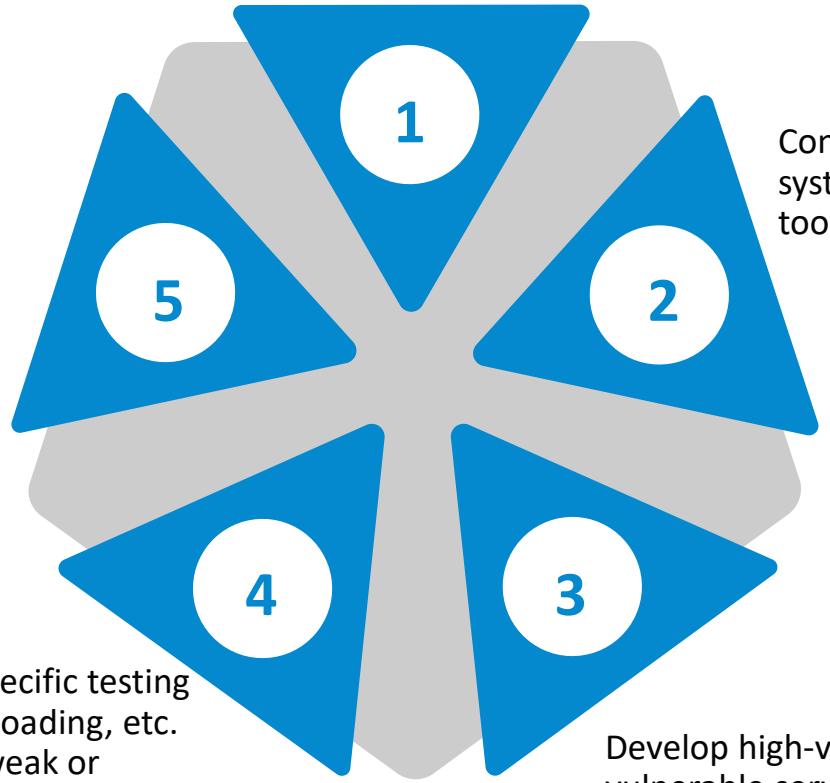
- Trained, second set of eyes
- Required status check added to branch protection configuration to assure reviews occur

COMCAST

Practice 8: Production-Ready Security Assessments

A Software PRSA typically involves the following process steps…

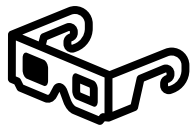
1. Review configuration files, source code, and other relevant documentation (attachments, wikis, etc.)
2. Conduct reconnaissance of systems using various scanning tools such as nmap.
3. Develop high-value target list of vulnerable services, etc. and conduct further investigation. This includes OS and packages system(s) are installed on
4. Conduct platform-specific testing such as fuzzing, sideloading, etc. Validate the use of weak or known passwords or exposed keys
5. Investigate the security of the data in transit and at rest and identify areas where malicious actors can exfiltrate data or interrupt the streams



This is an iterative process and each step in the process can trigger additional areas of concern and identified vulnerabilities

COMCAST

Lesson #3

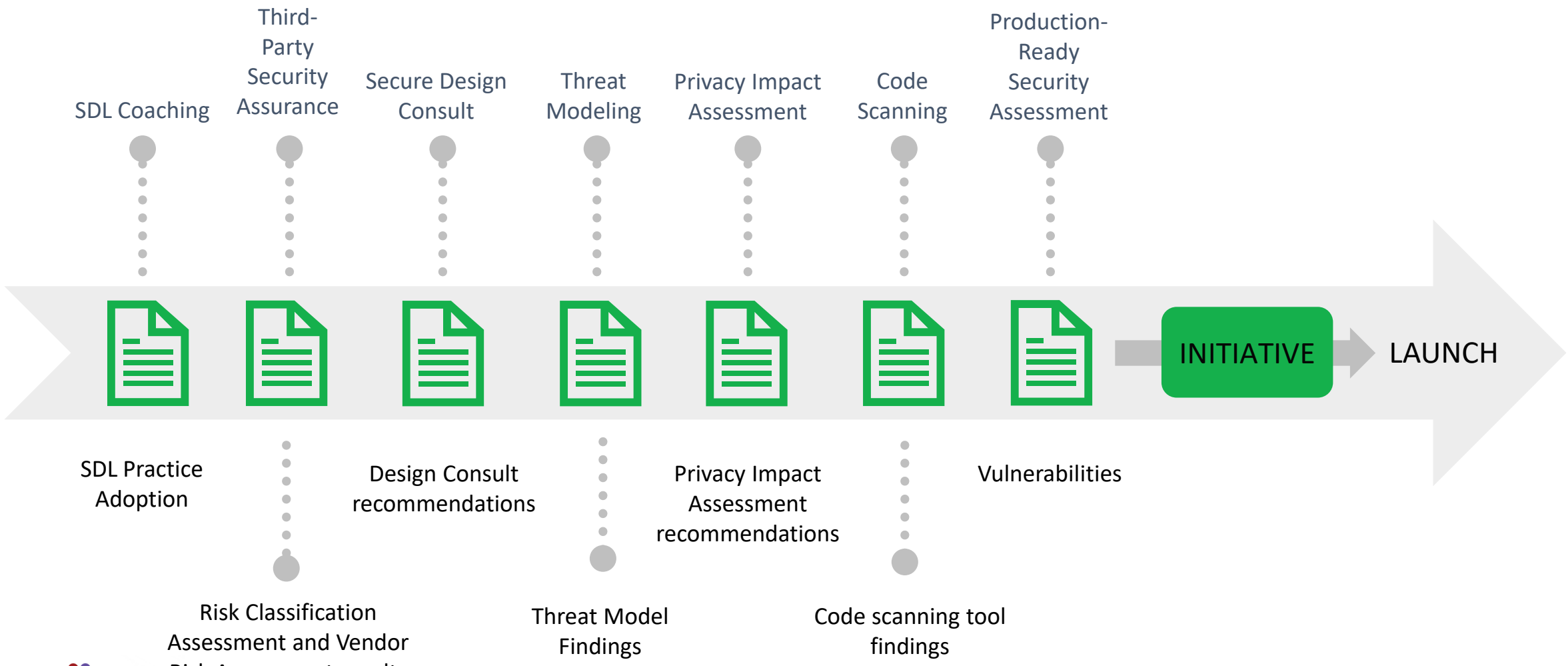


Change Your Lens: Pen testing teams should evolve to address emerging threats and scale their service to protect large enterprises

- Continuous Penetration Testing / Hackfests
- Tooling

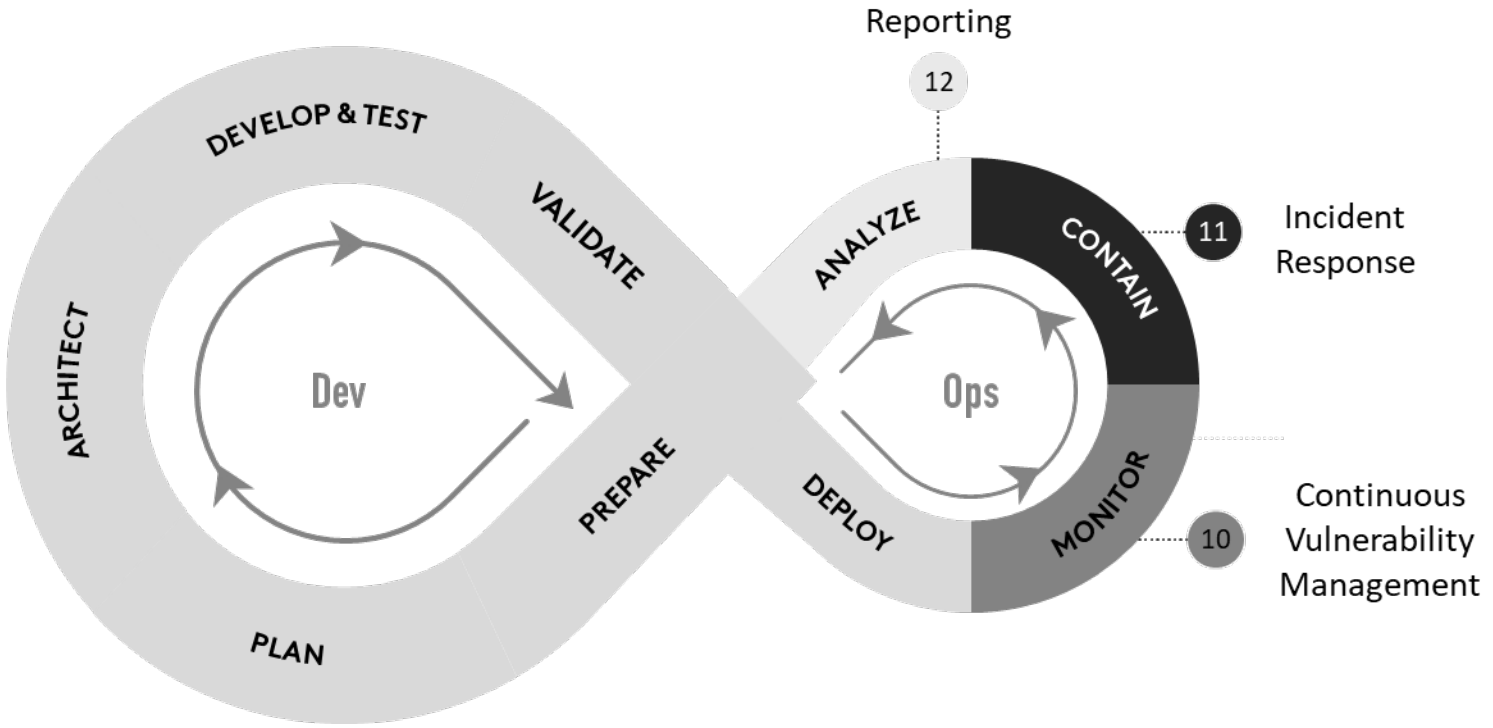
COMCAST

Practice 9: Security Reviews



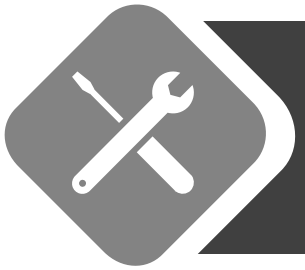
COMCAST

Operating Securely (Practices 10-12)



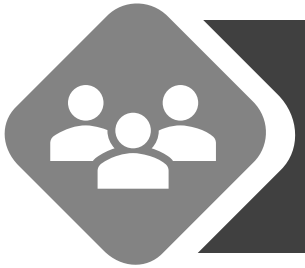
COMCAST

Practice 10: Continuous Vulnerability Management



Technical Controls

- Utilizing certified secure images and configurations
- Deploying anti-virus/malware protection, configuration compliance monitoring, data loss prevention tools, forensic tools, and local encryption
- Removing unnecessary software, services, and users
- Closing unnecessary ports



Process Controls

- Utilizing a robust patching and update strategy
- Managing software and hardware lifecycles so that patches and updates can be applied
- Managing privileged account access

COMCAST

Practice 11: Incident Response

PSIRT

Some customer-facing applications are selected as part of Comcast's bug bounty program (PSIRT), which offers incentives to qualified external researchers for responsibly disclosing vulnerabilities

Playbooks

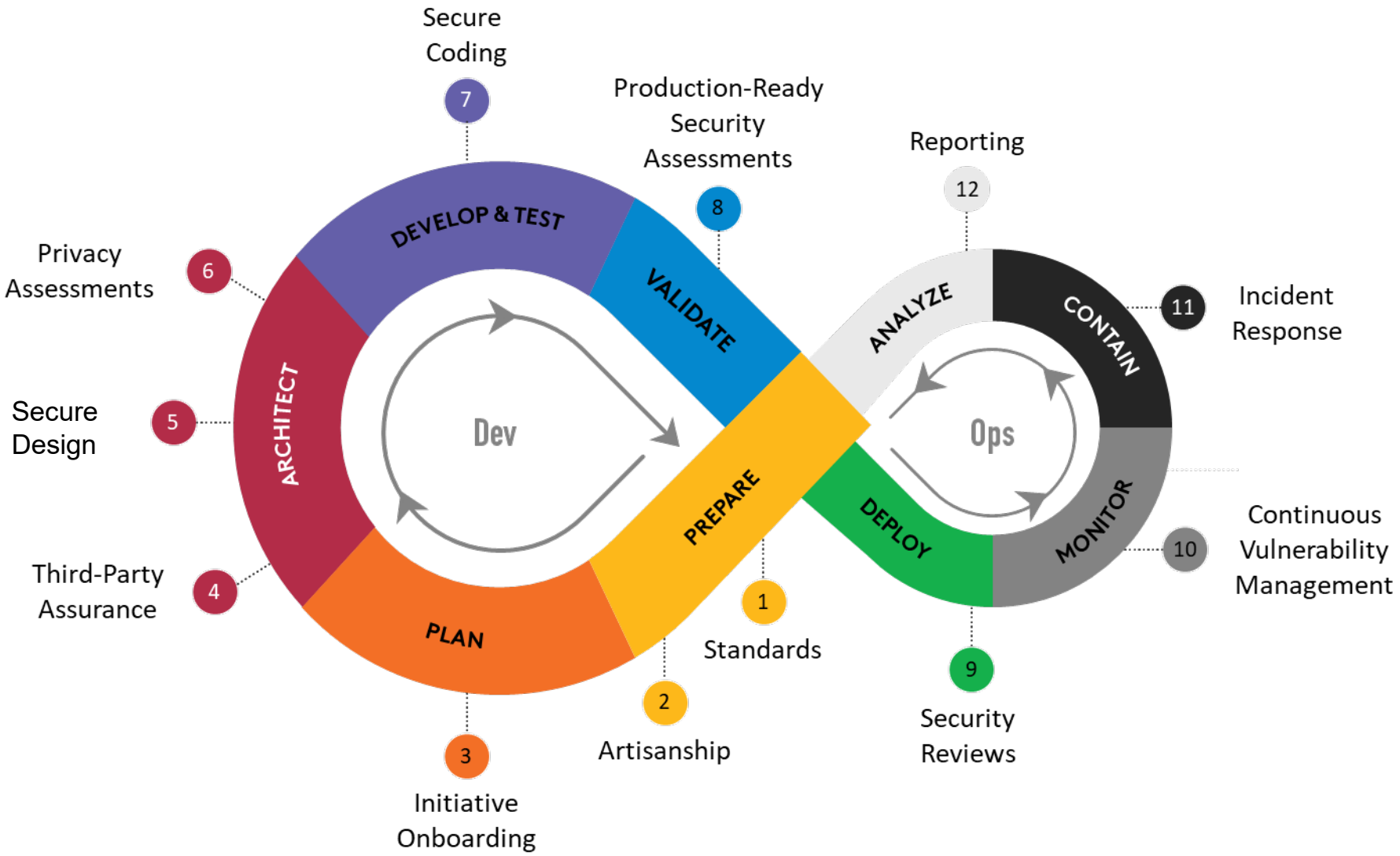
Cybersecurity Incident Response Playbooks include up-to-date roles with 24x7x365 contacts, workflows, prioritization / scoring / ranking, tracking repositories and working agreements

Tabletops

Tabletop exercises test the efficacy of Incident Response playbooks and ensure all players know their role and how to respond to an incident

COMCAST

Practice 12: Reporting with Comcast xCyberScore



COMCAST

Lesson #4

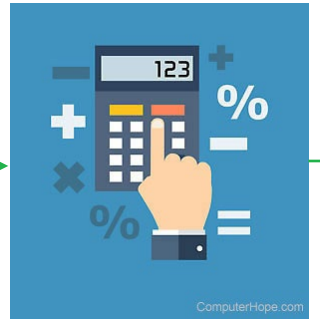
Gamify: Provide a single pane of glass for security work and a weighted score with fairness to drive friendly competition

COMCAST

Comcast xCyberScore at a Glance

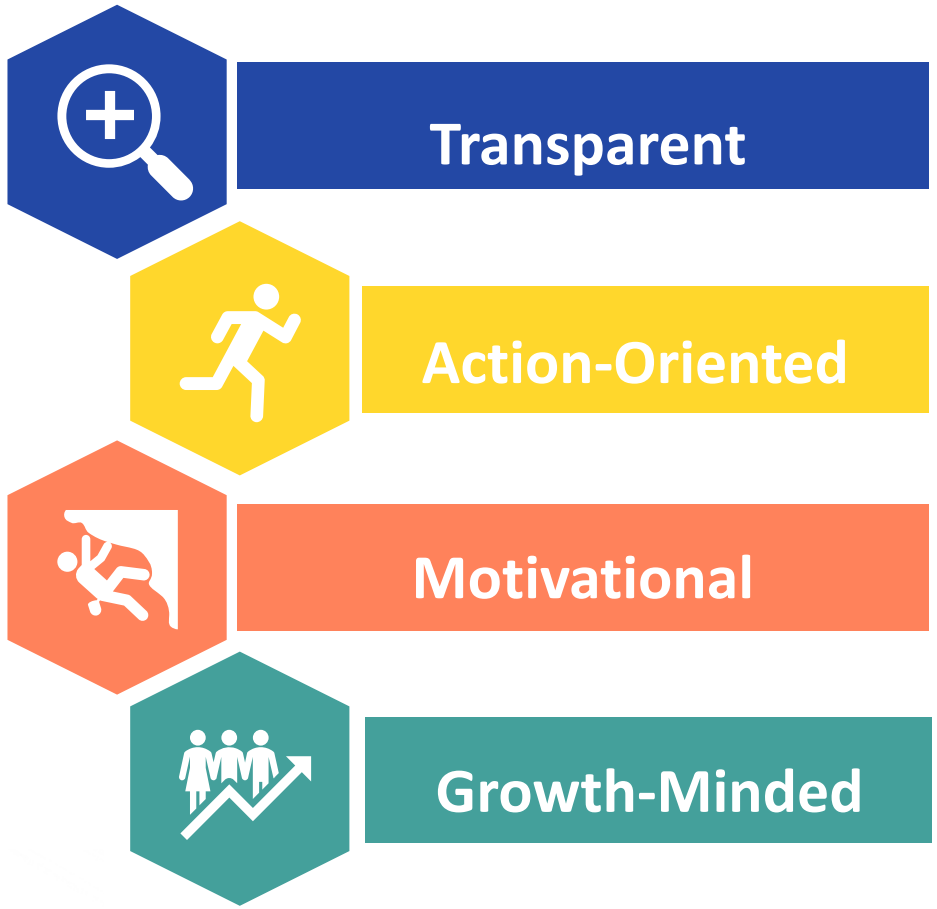
AGGREGATE | WEIGHT | CALCULATE | REPORT | PRIORITIZE

- Standards x%
- Artisanship x%
- Initiative Onboarding x%
- Third-Party Security x%
- Secure Design x%
- Privacy Assessments x%
- Secure Coding x%
- Production-Ready Security Assessments x%
- Security Reviews x%
- Continuous Vulnerability Management x%
- Incident Response x%
- Reporting x%



Comcast xCyberScore Core Attributes

xCyberScore product decisions align to a few key attributes based on SDL mission and intended audience



Clear line of sight from scores to the underlying findings in order to **build trust** and inform teams as to the **impact** of security work

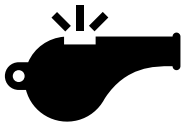
Calculations and UI elements are based on **open** findings rather than showing a full history of what was **closed**

Scores improve with **any reduction** in time to resolve vulnerabilities, rather than cutting off at **SLA date**

Findings are classified according to mapped **SDL practice** to draw a correlation to **practice adoption** and **growth**

COMCAST

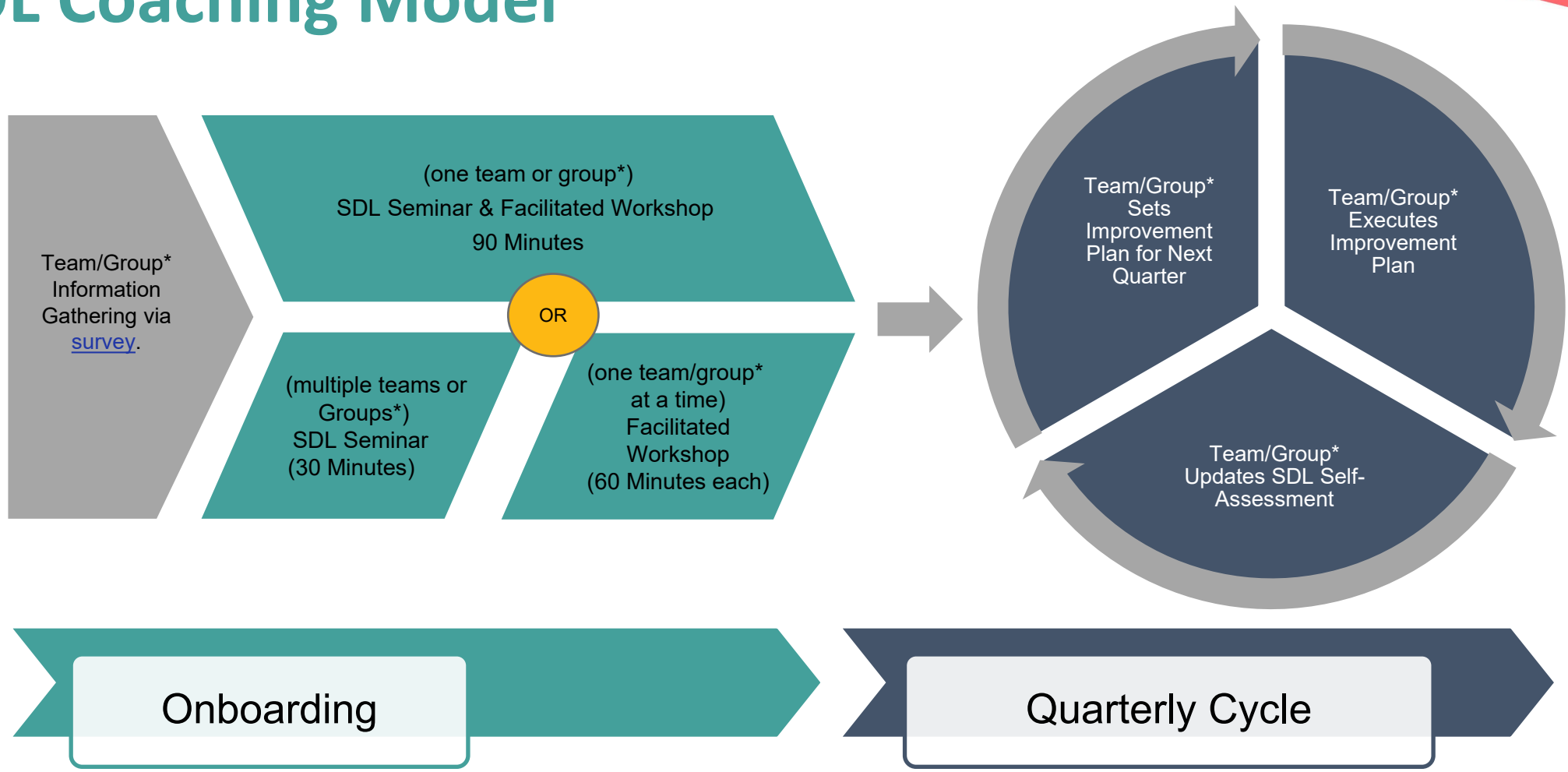
Lesson #5



SDL coaching is key to helping teams continually mature in making security part of their **culture**.

COMCAST

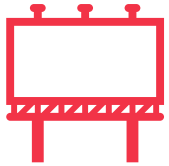
SDL Coaching Model



* A “group” is 1-N teams that:
    1. Work on related code (usually a product or product line)
    2. Share essentially the same development process (Scrum, Kanban, etc.)
    3. Share essentially the same toolchain (languages, build, etc.)

When it’s a single team, we’re looking for every team member to attend, but when it’s more than one team, we’re looking for representatives from each team to attend.

Apply Comcast's Lessons Learned



Brand a company-wide SDL program and present consistent **taxonomy** to drive alignment and measured progress.

Innovate for change, enabling threat models to address **privacy** risk and **scale** for large organizations

Change Your **Lens**: Evolve pen testing teams to address emerging threats and **scale** their service to protect large enterprises

Gamify: Provide a single pane of glass for security work and a weighted score with **fairness** to drive friendly **competition**

Invest in **SDL coaching,** which is key to helping teams continually mature in making security part of their **culture**.

COMCAST