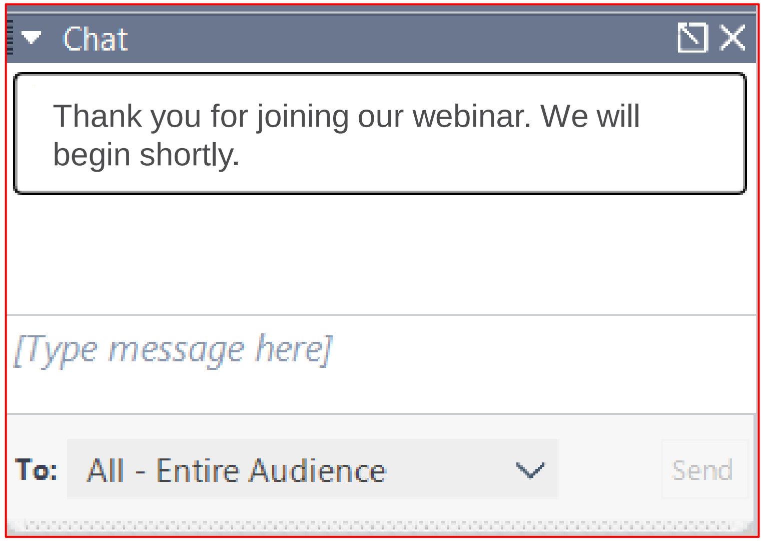
KROLL

Agile Penetration Testing: Scaling Application Assessments

September 20, 2023

Housekeeping

- Session is being recorded, You’ll receive access to the recording in a couple days
- Ask questions via chat >



Thank you for joining our webinar. We will begin shortly.

- We’ll try to answer as many questions as possible

Kroll Offensive Security Team

- 25+ Offensive Security Certified Professionals (**OSCP, OSWE**)
- 5+ CREST certified penetration testers (**CREST CRT**)
- 25+ penetration testers certified as **AWS Solutions Architects** or **Azure Security Engineers**
- 10+ CISSP, CISM, and CSSLP-certified penetration testers (**ISC2**)
- 5+ penetration testers certified in GPEN, GIAC, GXPN and GWEB (**SANS**)

Kroll's Offensive Security practice consists of **over 100 skilled penetration testers, application security engineers, and red teamers**, spanning over a dozen countries across Europe, North America, and Asia.

Kroll's Offensive Security practice performs:

100,000+ hrs.

of penetration testing per year for clients ranging from Fortune 100 companies to small-and-medium-sized businesses.

Speaker Profile

Rahul Raghavan

Senior Vice President, AppSec Advisory, Cyber Risk

LinkedIn – **torahulraghavan**
Twitter - **@rahul_raghav**

Over the next 35 mins…

- Context Setting / Verbiage Debunking
- The need for Agile Pentesting (as we know it)
- An example of an “How To” approach
- The Security Prioritization Matrix
- Key Takeaways

Background

Many organizations have adopted agile software development methodologies which enable development teams to release software quickly and efficiently in shorter cycles.

Yet when it comes to penetration testing, assessments are still primarily conducted annually, or at best bi-annually.

Challenge

- Large timespan between code changes and security testing; code is released to production with known and unknown risks
- Vulnerabilities do not get prioritized for remediation
- Lack of continuity from a product security and technical perspective
- Lack of metrics to measure the true state of application security
- Penetration testing is a standalone process

Solution

- Agile penetration testing program that integrates into your organization's software development lifecycle
- Build security culture into existing development processes
- Reduce risk of introducing vulnerabilities with new features
- Reduce time to remediation
- Help business and product teams make technical decisions with security in mind

Pentesting Program Comparison

Standard Pentesting

- **ICP** : Enterprise > SMB
- **Budget** : Security
- **Need** : Compliance, Regulation etc
- **Test Execution** : Partially Closed Box
- **Engineering Impact** : ++

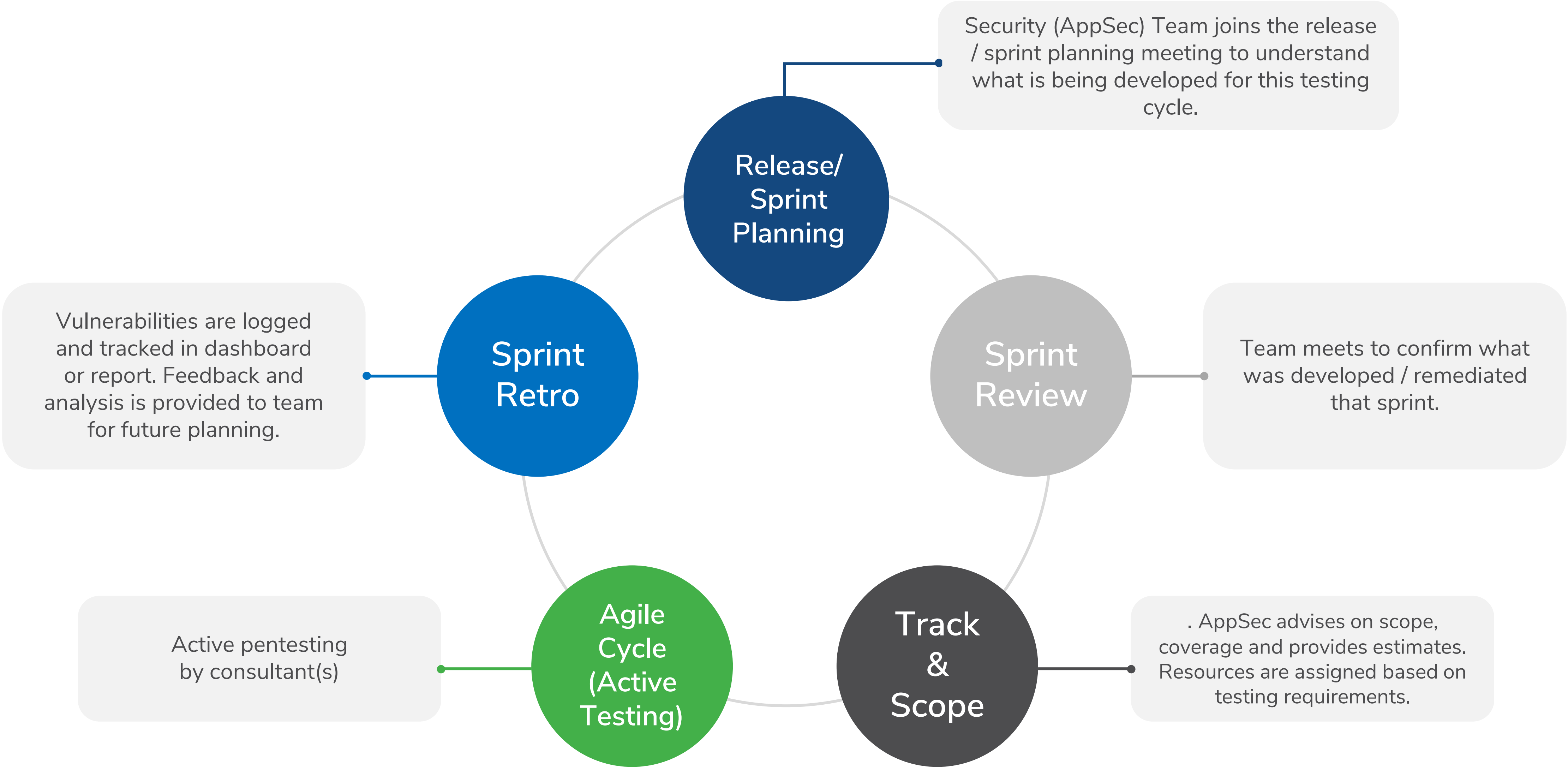
Agile Pentesting

- **ICP** : SMB > Enterprise
- **Budget** : Engineering / Security
- **Need** : Process Maturity, Differentiator etc
- **Test Execution** : Open Box
- **Engineering Impact** : +++

My position on Agile Pentesting

- A programmatic model to introduce the **right testing**, to the **right scope** at the **right time**
- A means to increase the frequency of security assessments to a particular scope within a set time period
- Provide visibility on test coverage both within and across the application real estate
- Provide (over time) metrics to engineering teams to estimate and plan security testing budgets
- Segue to step up software security initiatives within SDLC (security tooling, automation etc.)
- **Not** designed or intended to reduce or replace annual pen-testing programs

Agile Assessment Lifecycle



Security (AppSec) Team joins the release / sprint planning meeting to understand what is being developed for this testing cycle.

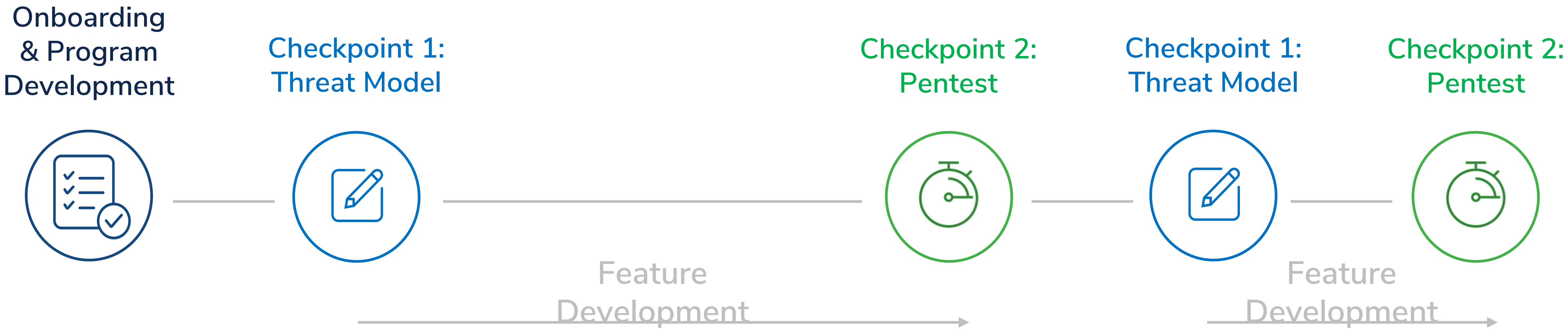
Team meets to confirm what was developed / remediated that sprint.

. AppSec advises on scope, coverage and provides estimates. Resources are assigned based on testing requirements.

Active pentesting by consultant(s)

Vulnerabilities are logged and tracked in dashboard or report. Feedback and analysis is provided to team for future planning.

‘In-Sprint’ Execution Model



Onboarding & Program Development

Checkpoint 1: Threat Model

Checkpoint 2: Pentest

Checkpoint 1: Threat Model

Checkpoint 2: Pentest

Feature Development

Feature Development

Onboarding

- Contextual Knowledge of scope
- Security Requirements Strategy
- Agile Framework & Methodology
- Release Cadence / Cycles
- Roadmap Planning

Threat Model

- Abuse case and business logic-based Threat Modelling of features
- Output contains threats, weaknesses and potential vulnerabilities based on the planned design and architecture
- Informs the test cases for the pen test

Pentest / Assessment

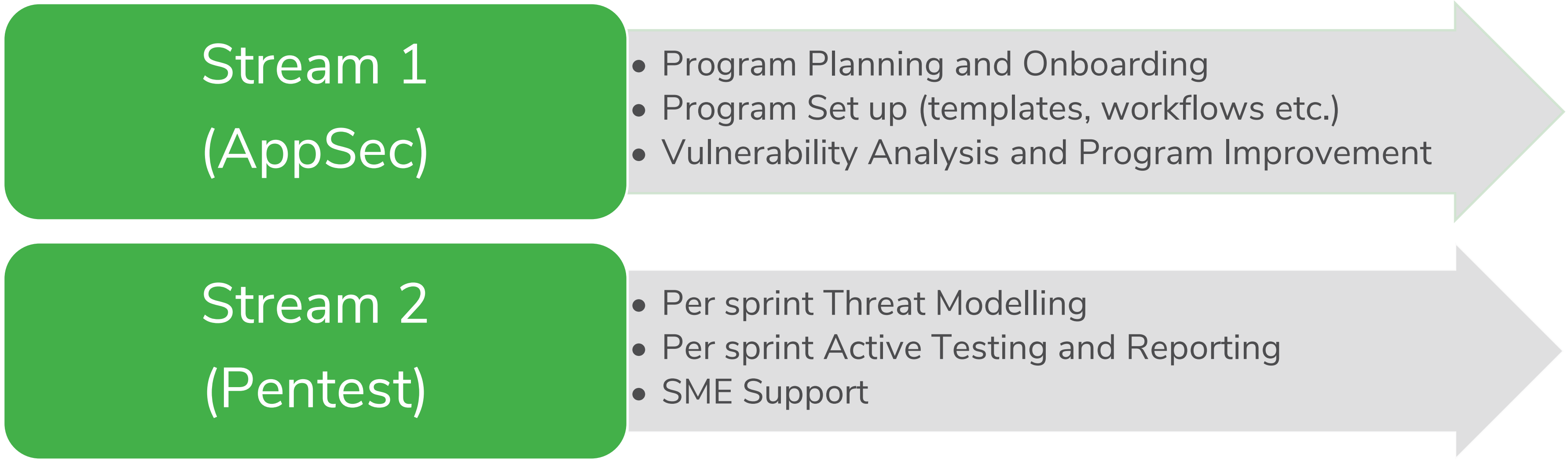
- Testing and validation of Threat Models for each completed and ready to release feature
- Additional exploratory test scenarios

Security Prioritization Matrix

Project	Release	Assets Impacted	Asset Criticality	Asset Change	Business Impact	Prioritization	IR / FR
Project 1	R 2.5	Auth API	High	Minor	High	S1	Yes
		CRM	High	Major			
		Website	Medium	Minor			
Project 2	R 3.4	S3	Medium	Major	Medium	S2	Yes
		Report API	Medium	Minor			
		Website	Medium	Major			
Project 3	R 3.4	Public File Repo	Low	Major	Low	S3	No

Prioritization	Threat Model	SCA	SAST	DAST	Internal Pentest	External Pentest
S1	✓	✓	✓	✗	✓	✓
S2	✓	✓	✓	✗	✓	✗
S3	✗	✓	✓	✓	✗	✗

Representative Team Structure



Stream 1 (AppSec)

- Program Planning and Onboarding
- Program Set up (templates, workflows etc.)
- Vulnerability Analysis and Program Improvement

Stream 2 (Pentest)

- Per sprint Threat Modelling
- Per sprint Active Testing and Reporting
- SME Support

The Kroll Engagement Team

Engagement Owner:

- Oversees the entire program
- Point of Escalation & Resolution

Technical Program Manager:

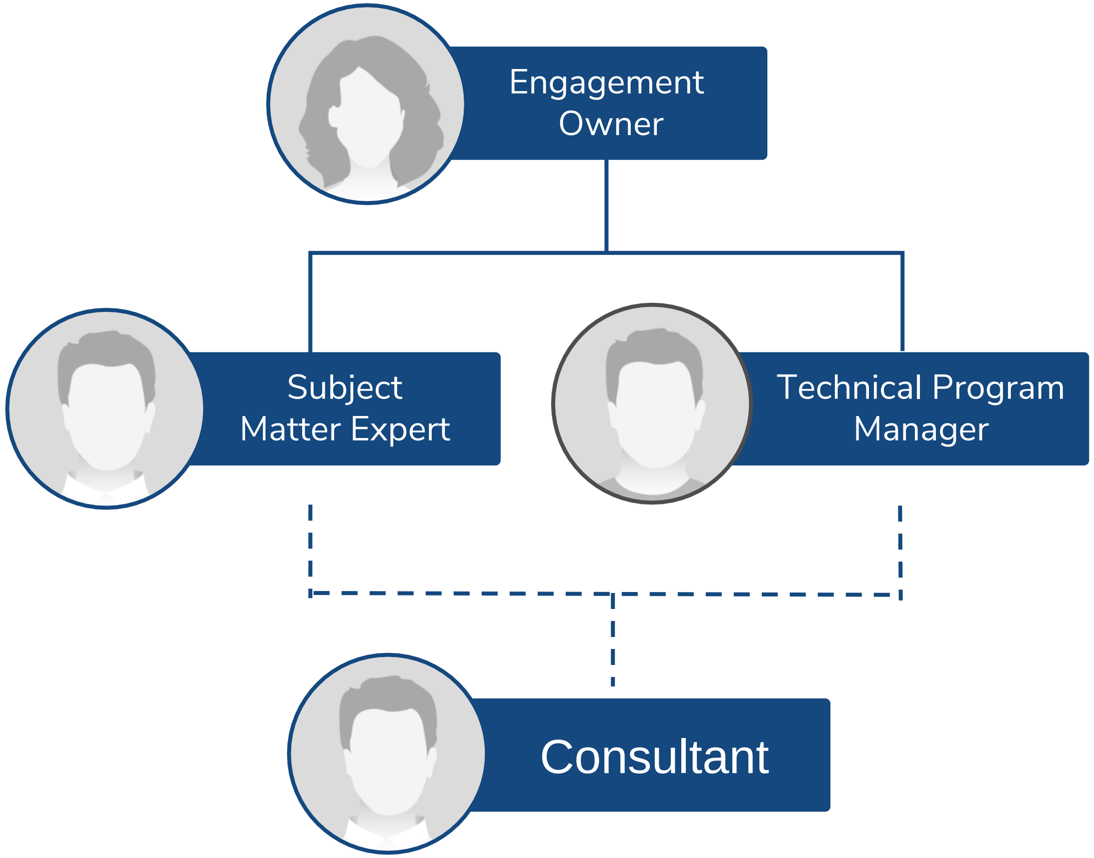
- Main Point of Contact
- Manage Scope, Budget and Scheduling
- Metrics & Reporting
- Trends and Analysis
- Resources to match evolving needs

Subject Matter Expert:

- Provides technical expertise and maintains institutional knowledge on the application real estate and the overall program
- Conducts per sprint threat modeling and test case identification
- Consistent support throughout

Consultant (on Rotation) :

- Refers to program design and workflow
- Conducts per sprint / release testing
- Reporting



Summary

- Right Testing of the Right Scope at the Right Time!
- Validate assessment needs with a Security Prioritization Matrix
- Not every scope requires a Penetration Test
- Enable Product and Project Managers for successful delivery models

Questions?

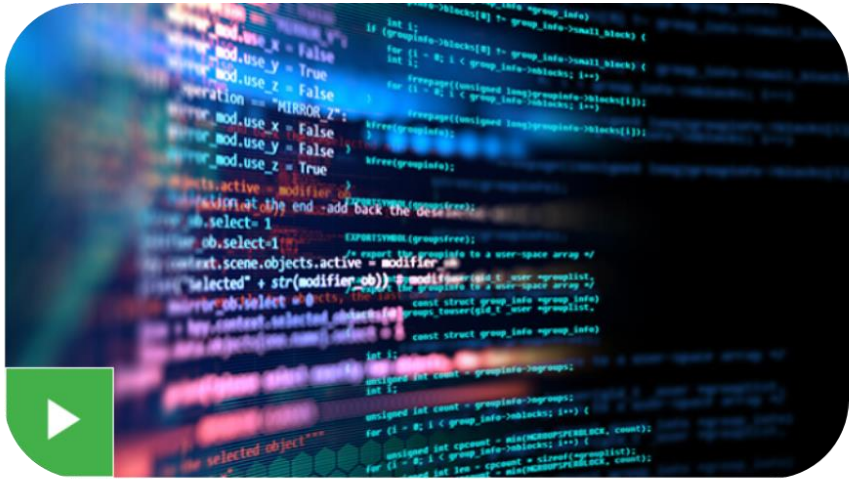
Additional Resources

KROLL

An Introduction to Agile Penetration Testing

Get Started on Your Agile Pen Testing Program with the eBook.

Download now



Explore why *'Threat Modeling'* is often misunderstood—or worse, neglected—in agile product engineering.

Watch the webcast replay now

KROLL

For more information, please contact: your local Kroll office or today's presenters:

KROLL HOTLINES

EMEA region and United Kingdom

- +44 (0) 808 101 2168 (toll free)
- +44 20 3885 0882 (toll)

United States and Canada

+1 877 300 6816

PRESENTER: Rahul Raghavan

Rahul.Raghavan@kroll.com

LinkedIn – torahulraghavan

Twitter – @rahul_raghav

EMAIL
CyberResponse@kroll.com

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With 5,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.