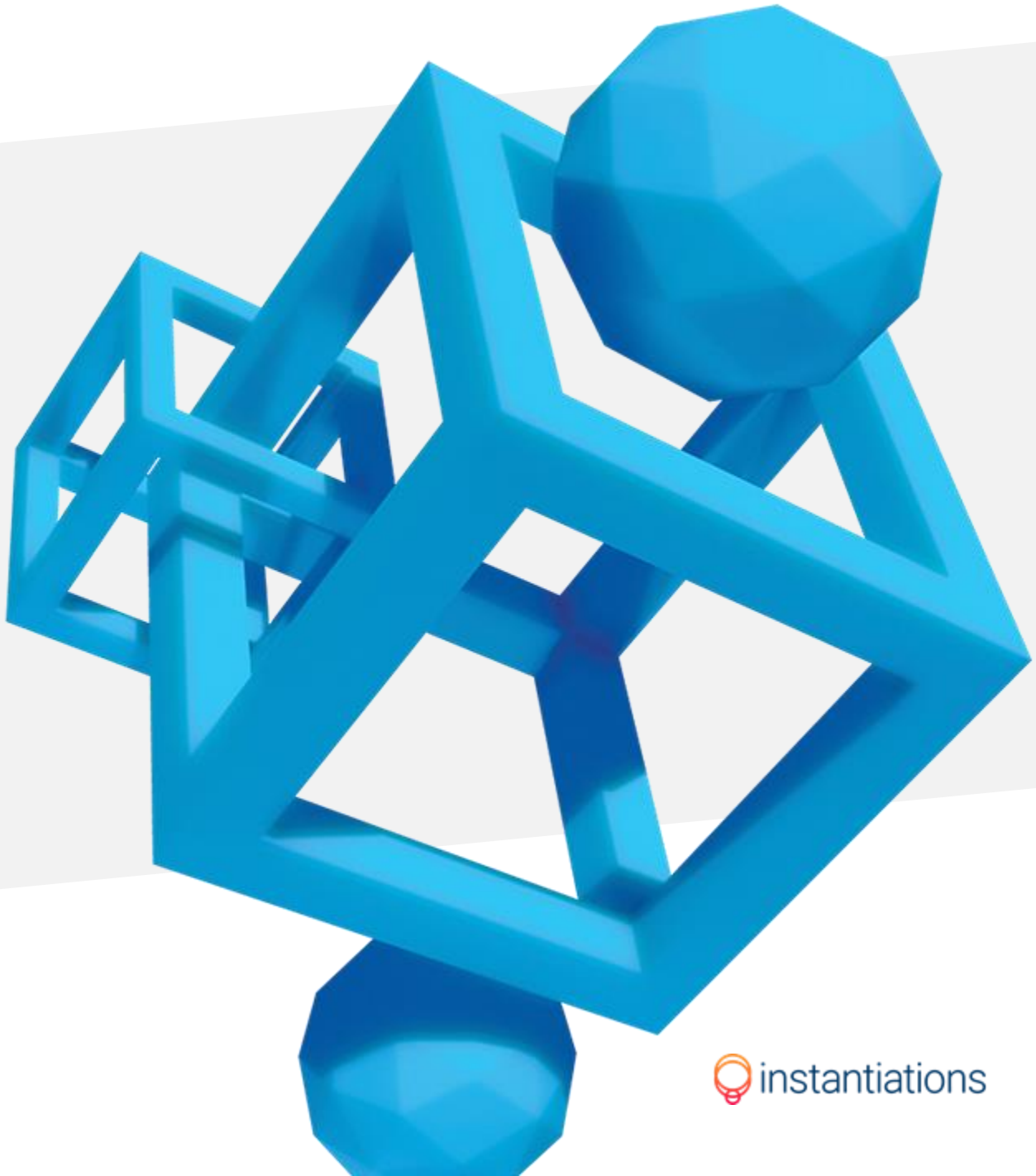

instantiations

instantiations

Enhancing Security in VAST

Towards Static Vulnerability Scanning



instantiations

Josh Wyatt

CISO / VP

Mariano Martinez Peck

Senior Software Engineer

instantiations

Thank you to the venue, the organizers, the sponsors, and the attendees.

instantiations

What is SAST?

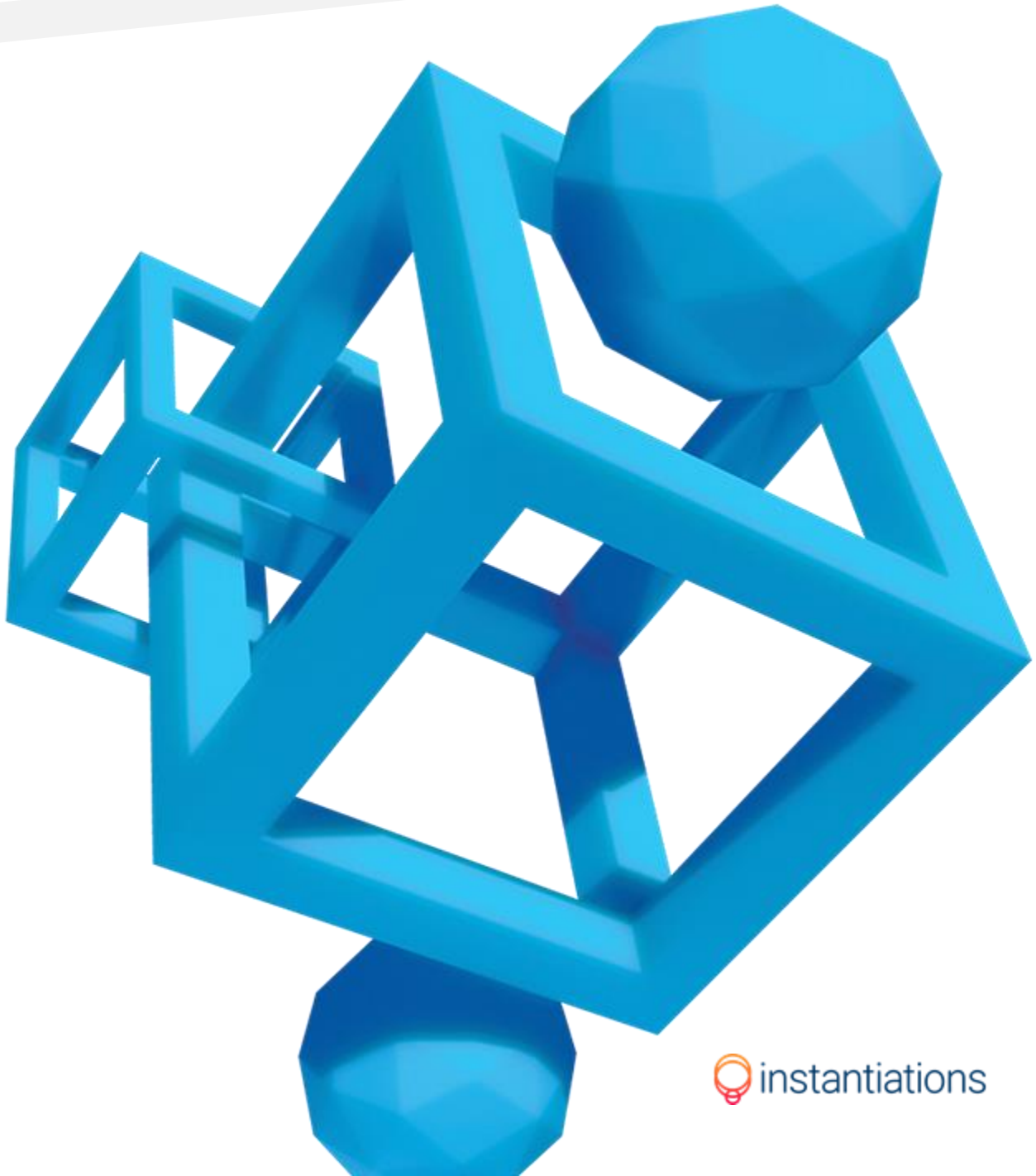
instantiations

SAST is Static Analysis - for Security

S Static
A Analysis for
S Security
T Testing

What is Static Analysis?

- Analysis of code without running it
- Mostly a semantic strategy (similar to “linting”)
- Perfect companion for IDE
- Can be automated
- Different types focused on structure



instantiations

What is Static Analysis?

Focus on structure like:

- call tree, nodes, functions
- flow
- invocation
- pattern matching

What is Static Analysis?

- Mostly a semantic strategy (similar to “linting”)
- Pattern matching
- Rules definition and testing
- Structure, again

What is Static Analysis?

Perfect companion for IDE

- Intimate relationship with:
  - keyword matching (like ‘Password123’)
  - method invocations
  - some data and object instantiations
- Leverages existing power of VAST components

What is Static Analysis?

Different types focused on structure

- Pattern-based analysis
- Flow-based analysis
- Metric-based analysis
- Semantic analysis

Example: SQL Injection

Static Analysis can…

- Catch poor practices like unsafe query manipulation
- Identify good practices like FFI

Static Analysis cannot…

- pre-suppose injectable content

What Static Analysis is NOT?

- **Dynamic analysis**

- **Cannot identify ephemeral items such as:**
  - dynamic memory allocation
  - external system invocations
  - external variations on input

- **Cannot identify external influence like:**
  - system environment
  - fuzzing
  - performance issues (like race conditions)

Why build a SAST?

instantiations

Why build a SAST for VAST?

- Customer needs for improved compliance and security
- Improvement of Operational Maturity
- Instantiations' ever-growing commitment to R&D

Roadmap and Release Strategy

instantiations

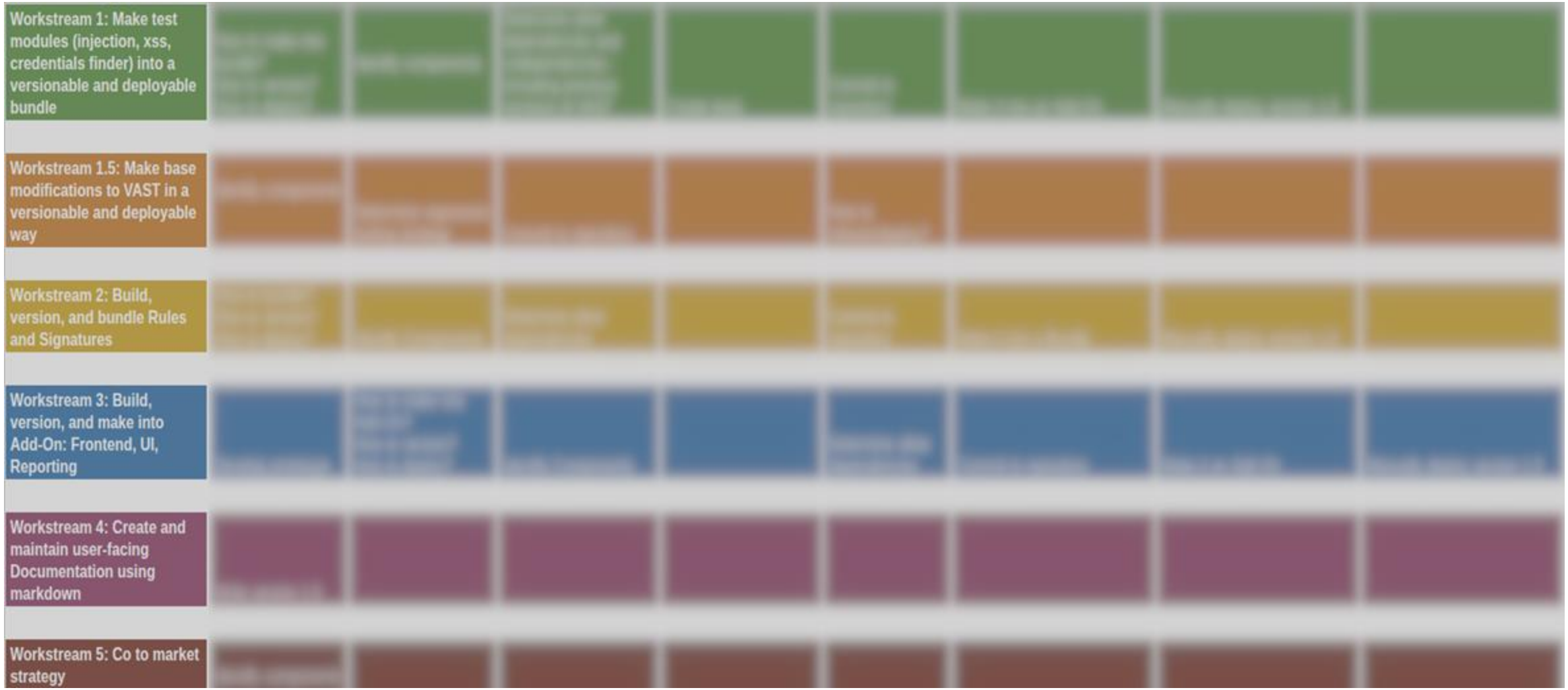
SAST Security Scanner Product Vision

To build a Security Scanning Suite in VAST to include:

- An initial set of scanning tools that use rules and signatures to detect Injection, XSS, and embedded Credentials, with whitelisting, hinting, and annotation capability
- An initial set of customizable rules and signatures to be consumed by the scanning tool modules, separately packaged, versioned, and maintained
- A frontend configuration and reporting tool to empower the user to best use the scanning tools and generate actionable reports

Roadmap Workstreams

- Develop Testing Engine and Strategy
- Considering Modifications to VAST
- Separately Develop Rules and Signatures
- Front-end, User Interface, and Reporting
- Create and Maintain Documentation
- Execute *Go to Market* Strategy


Workstream 1: Make test modules (injection, xss, credentials finder) into a versionable and deployable bundle
Workstream 1.5: Make base modifications to VAST in a versionable and deployable way
Workstream 2: Build, version, and bundle Rules and Signatures
Workstream 3: Build, version, and make into Add-On: Frontend, UI, Reporting
Workstream 4: Create and maintain user-facing Documentation using markdown
Workstream 5: Co to market strategy

Strategy and Implementation

- Evaluate Industry needs and Customer requests
- Leverage Instantiations' expert knowledge of Smalltalk and VAST platform strengths
- Engage Security Industry Experts to help build
- Discovery and prototype phase for feasibility and lessons learned
- Apply lessons learned to build and polish something we can release

Alpha and Beta testing

instantiations

Demonstration and Q&A

instantiations

instantiations

Thank you!

Questions?

Josh Wyatt
CISO / VP

jwyatt@instantiations.com

/in/dragonwyatt/

Mariano Martinez Peck
Senior Software Engineer

mpeck@instantiations.com

@MartinezPeck

/in/mariano-martinez-peck/

Contact

General Inquiry
info@instantiations.com

Sales
sales@instantiations.com

VAST Support Portal
vast-support.instantiations.com

North America, Toll Free
855 476 2558

International
+1 503 263 0058

© Instantiations, Inc. All rights reserved. 'Instantiations' and the 'intersecting circle design' are registered trademarks of Instantiations, Inc. in the United States. All product names, trademarks, and registered trademarks are property of their respective owners. Company, product, and service names not owned by Instantiations are used for identification purposes only. Use of these names, trademarks, and brands does not imply endorsement.