2017 Cyber Security R&D Showcase and Technical Workshop

July 11 - 13, 2017 | Washington, D.C.

Homeland Security

Science and Technology

Application Security Threat Attack Modeling

Chris Horn | Secure Decisions

July 12, 2017

Homeland Security

Science and Technology

Team Profile

Secure Decisions, prime

- Cyber R&D division of Applied Visions, Inc.
- Primarily serving DHS & DoD
- Specialties: application security, decision analysis, cyber visualization, cybersecurity education technology, technology transition

Team members

- AITEK
- Aspect Security
- Deloitte
- Denim Group
- Siege Technologies

SECURE DECISIONS
A DIVISION OF APPLIED VISIONS, INC.

AITEK ASPECT SECURITY Application Security Experts Deloitte.

DENIM GROUP SIEGE technologies

Customer Need

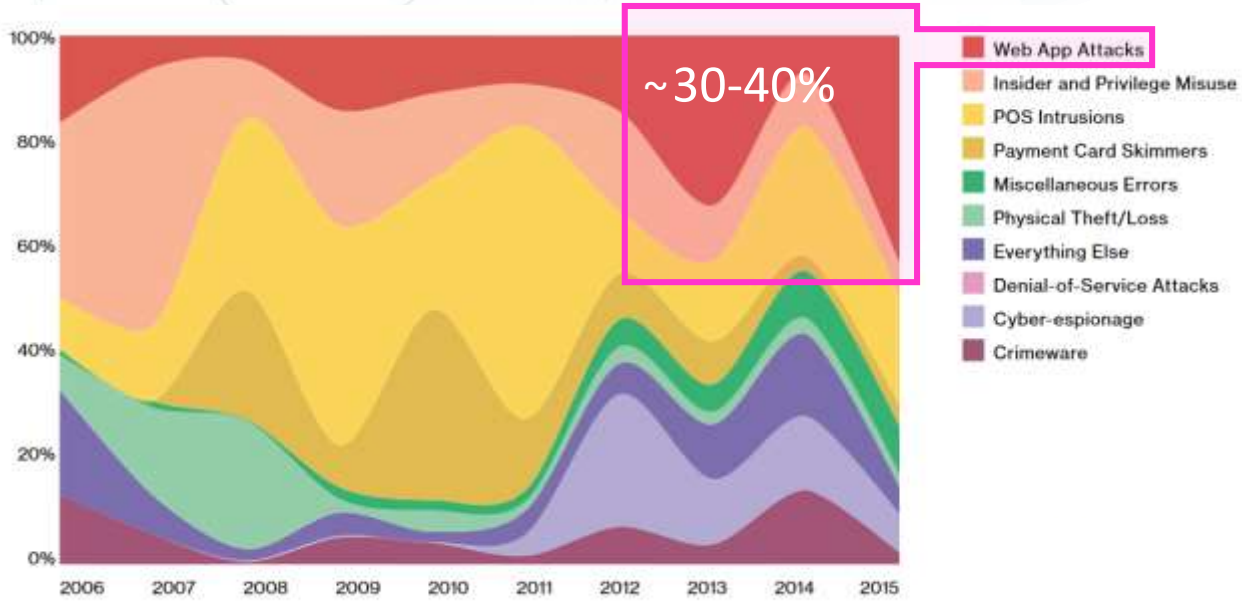
Organizations need to assure application security

- Web application exploits are behind 30-40% of breaches
- Regulatory compliance: finance, insurance, healthcare, defense

Application security is *hard*

- Resource intensive
  1. Identify & understand threats
  2. Identify vulnerabilities
  3. Implement security controls
  4. Verify & test security
- Handoffs are disjointed

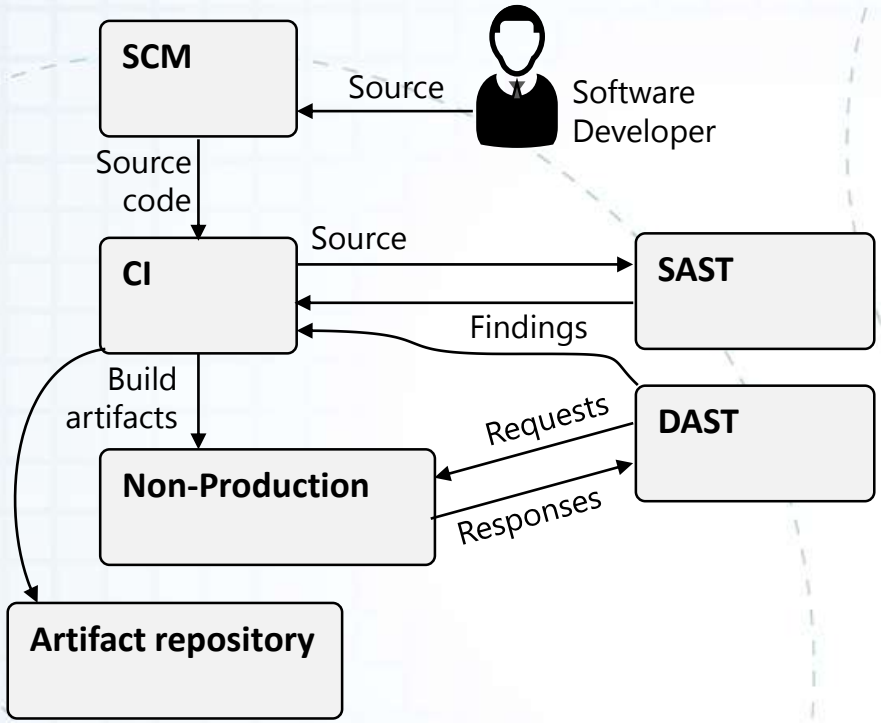
Frequency of incident classification patterns over time across confirmed data breaches



2016 Verizon Data Breach Investigation Report

Approach

System of 4 severable capabilities



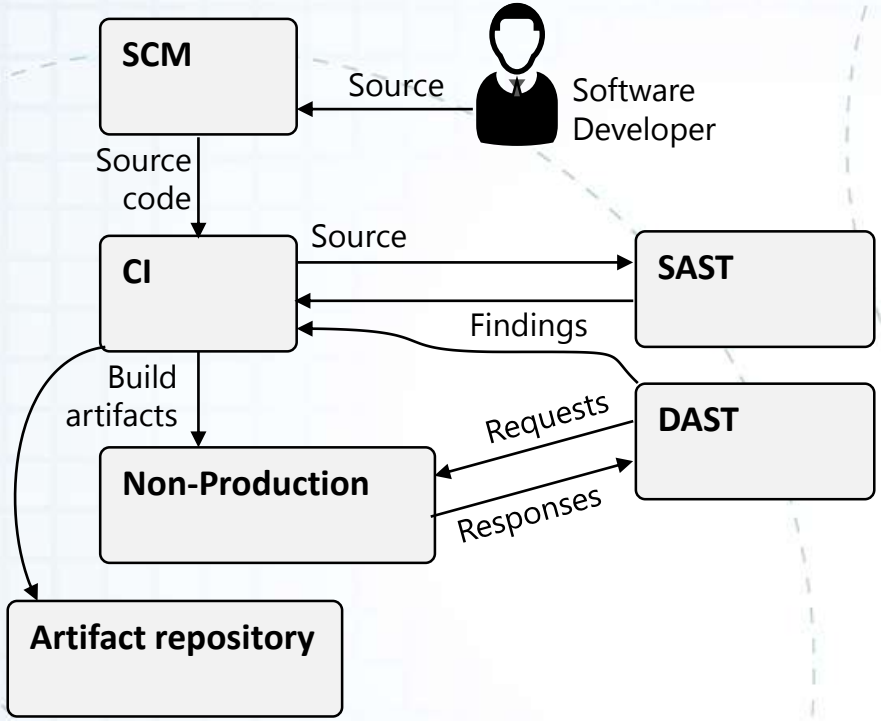
LEGEND

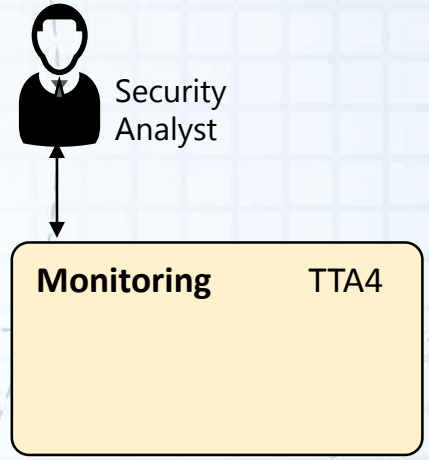
Customer infrastructure

ASTAM component

Approach

System of 4 severable capabilities





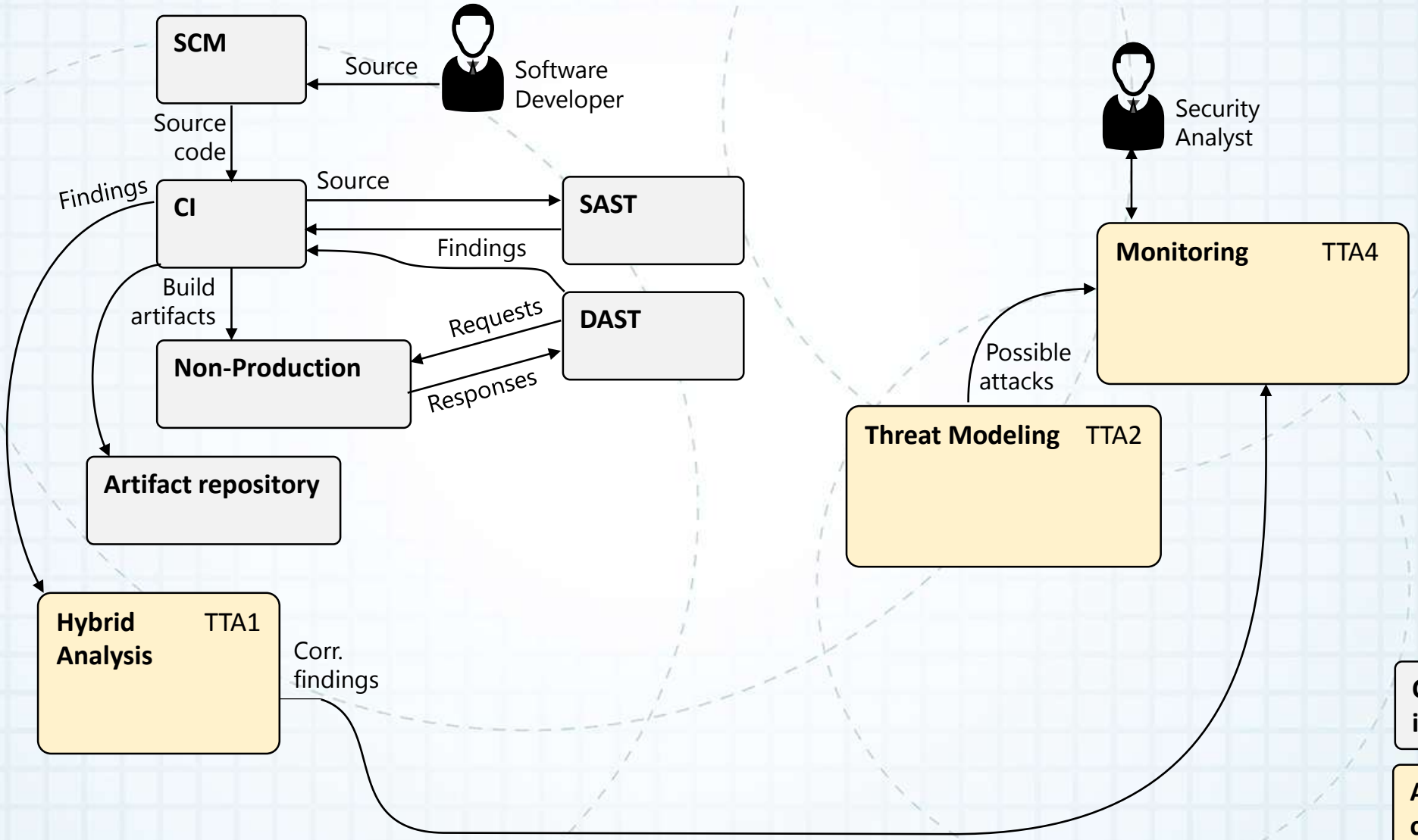
LEGEND

Customer infrastructure

ASTAM component

Approach

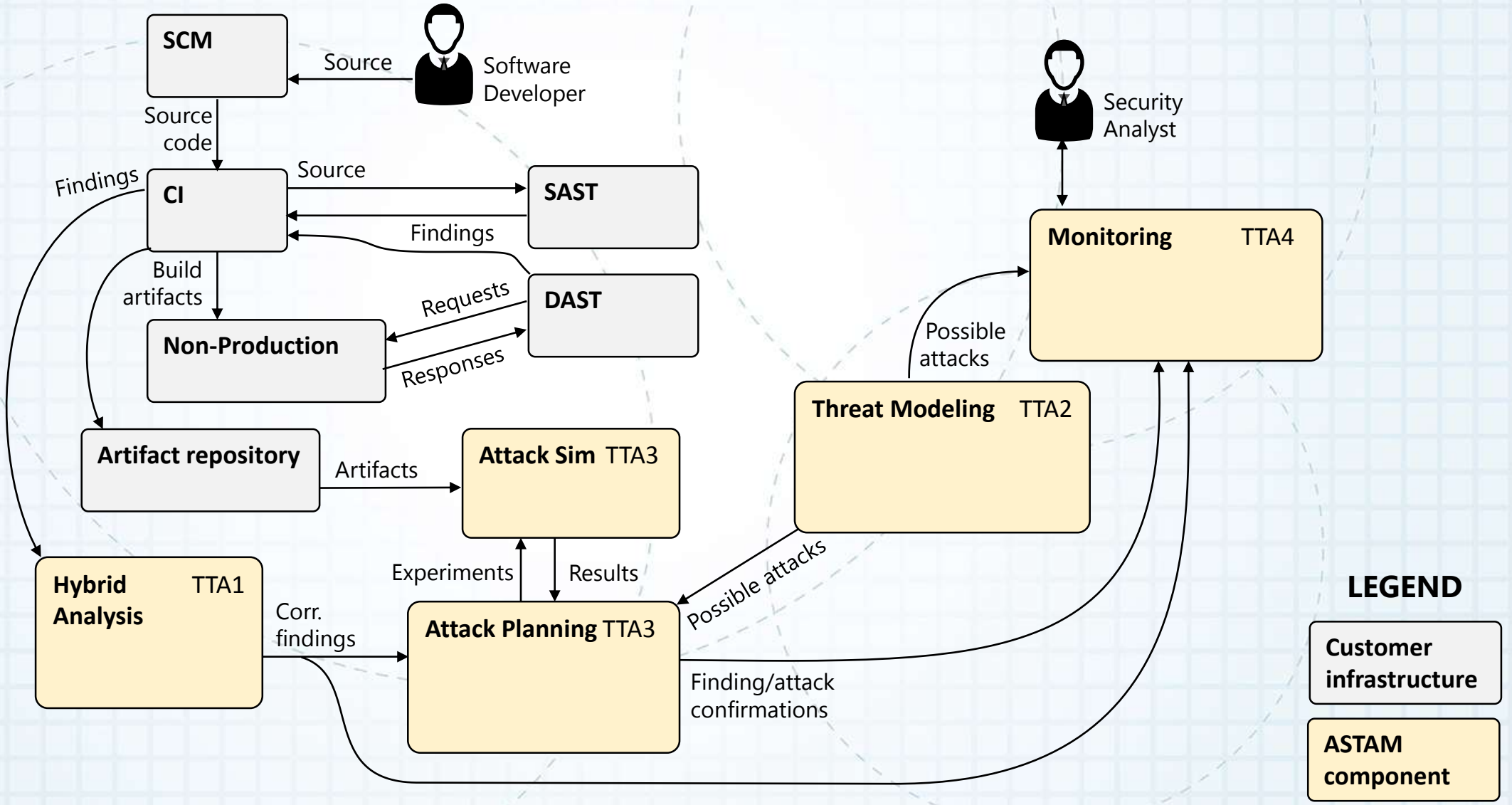
System of 4 severable capabilities



Approach

System of 4 severable capabilities

Integrated into a Unified Threat Management system



Approach

Four distinct & severable capabilities:

1. **Hybrid analysis mapping**
   De-duplicate SAST & DAST findings
2. **Application threat modeling**
   Identify potential attacks & which source code they would likely target
3. **Attack & countermeasure simulation**
   Confirm & discover application vulnerabilities
4. **Continuous monitoring & assessment**
   Support security capability implementation decisions

Benefits

Reduce analysis time and resources

Increase coverage of vulnerabilities

Scan more with higher repeatability

Increase confidence in findings & remediation decisions

- Automated threat modeling to identify architecturally-relevant weaknesses
- Automated correlation of SAST & DAST scan findings to remove duplicates
- Automated attack simulation to verify findings as exploitable
- Prioritized findings
- Continuous monitoring to measure & track progress with actionable metrics

Competition

Hybrid analysis mapping

- Code Dx

Correlation based on robust code tracing

Does not seed DAST with application endpoint attack surface

Requires an agent

Competition

Hybrid analysis mapping

- Code Dx

Threat modeling

- Consulting firms
- In-house teams

Fully manual
(time consuming & expensive, requires expertise)

- Microsoft Threat Modeling Tool
- OWASP Threat Dragon

Highly manual, requires expertise
(mostly just a graphical drawing tool)

- IriusRisk
- MyAppSecurity ThreatModeler
- Amenaza SecurITree

Looks up common threats based on questionnaire
Do not consider source code

Competition

Hybrid analysis mapping

- Code Dx

Threat modeling

- Consulting firms
- In-house teams
- Microsoft Threat Modeling Tool
- OWASP Threat Dragon
- IriusRisk
- MyAppSecurity ThreatModeler
- Amenaza SecurITree

Attack & countermeasure simulation

- Consulting firms
- In-house penetration testers
- Application security testing (HP, Veracode, IBM)
- Metasploit

Fully manual
(time consuming & expensive, requires expertise)

DAST difficult to set up & run
Can't execute multi-step attacks

Infrastructure & network-focused

Competition

Hybrid analysis mapping

- Code Dx

Threat modeling

- Consulting firms
- In-house teams
- Microsoft Threat Modeling Tool
- OWASP Threat Dragon
- IriusRisk
- MyAppSecurity ThreatModeler
- Amenaza SecurITree

Attack & countermeasure simulation

- Consulting firms
- In-house penetration testers
- Application security testing (HP, Veracode, IBM)
- Metasploit

Continuous monitoring

- Custom in-house
- GRC (IBM, RSA Archer, Qualys, Veracode)

Expensive
Metrics often insufficient

Current Status

TRL = Technology Readiness Level

Hybrid analysis mapping	TRL 8 – Java Spring TRL 7 – .NET MVC TRL 4 – Python	Enhancing Java & .NET capabilities Adding Python support Conducting performance testing & analysis
Threat modeling	TRL 3	Changed approach to machine learning analysis of source code & lookup of common threats
Attack planning	TRL 3	Automating SQLi & HTTP attribute-based XSS attacks using existing attack tools
Attack execution	TRL 4	Extending existing TRL 7 technology with APIs & simplifying “templates”
Continuous monitoring	TRL 2	Investigating methods of modeling risk Developing actionable metrics

Next Steps

Continue software development process

Identify integration points with commercial products

Evaluate internally

Engage our Board of Advisors for feedback

Continue outreach & publicity

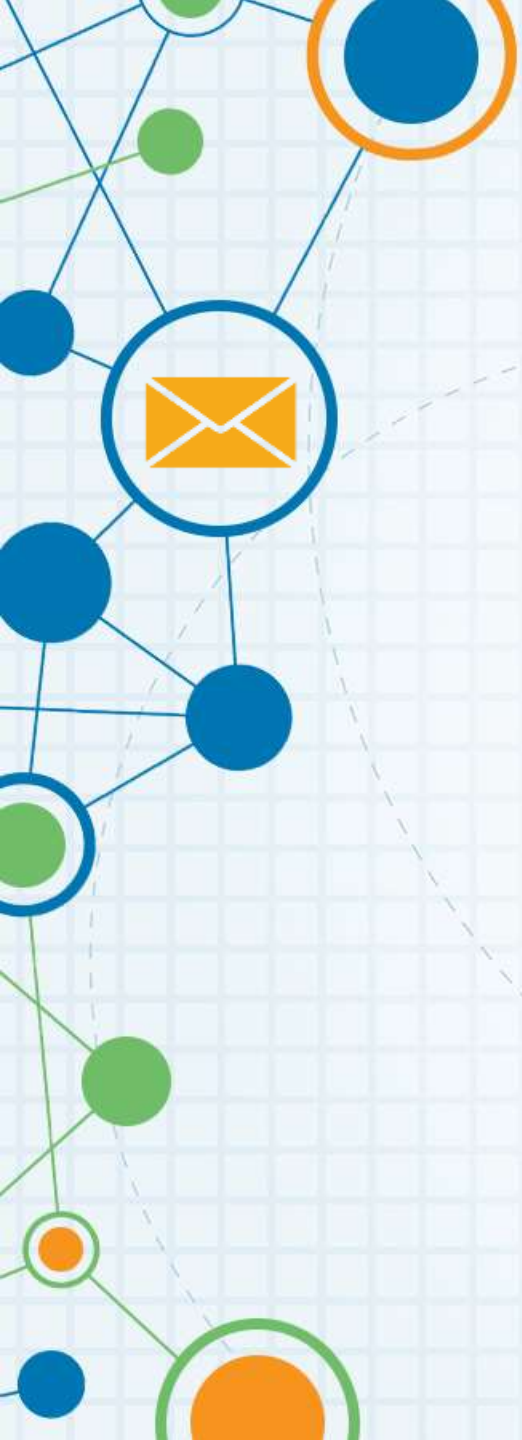
- Presenting at AppSec USA 2017 in September
- Meetings with interested parties

Potential Transition Activities

Open source releases planned for July & September

Targeting larger organizations in finance, insurance, healthcare, and defense

- Currently early-stage interest-building
- Anticipate interest solidifying late 2017 w/ working prototype



Contact Info

All feedback welcome

We should talk

Chris Horn
Secure Decisions
chris.horn@securedecisions.com
(518) 207-3111
@chornsec

2017 Cyber Security R&D Showcase and Technical Workshop

July 11 - 13, 2017 | Washington, D.C.

Homeland Security

Science and Technology