secureCENTRX

Precision Information Security

Securing Software

Threat Modeling
Secure SDLC
Ransomware Defense
Penetration Testing

Governance, Risk and Regulatory

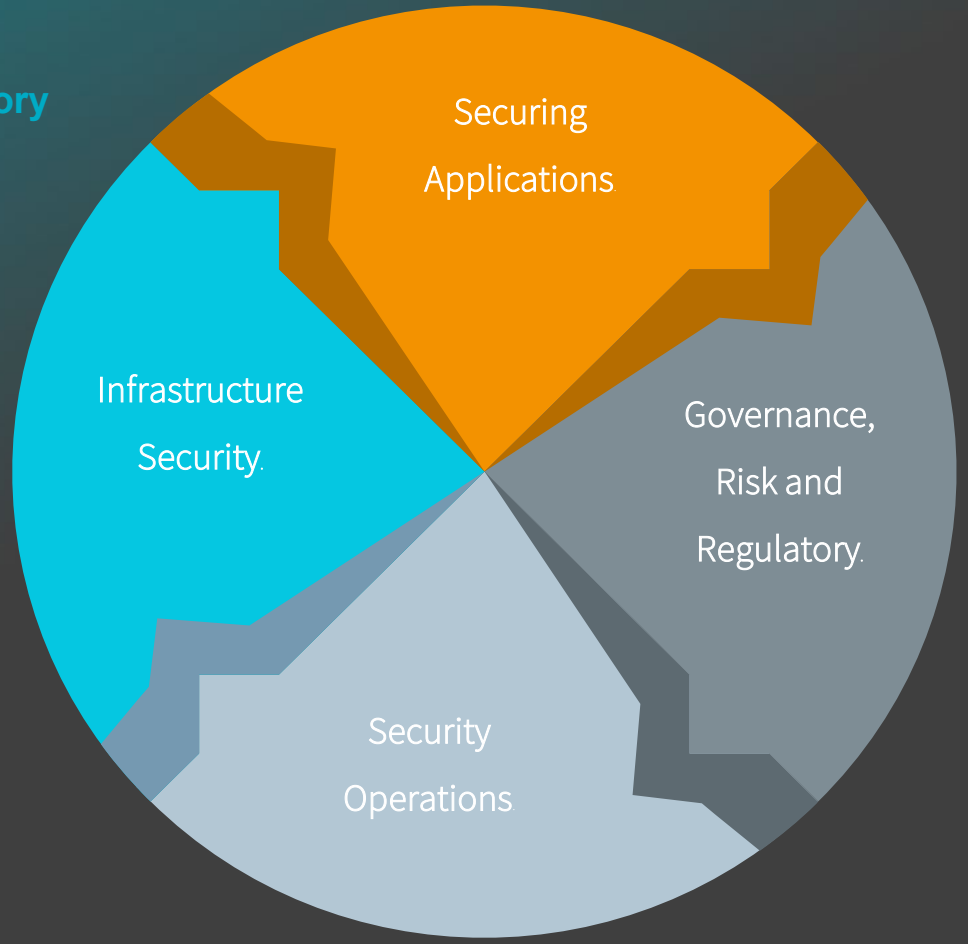
IT Control Framework
Policies as a Service
Audit Support
Risk Program
Assessment
InfoSec Management System

Testing and Response

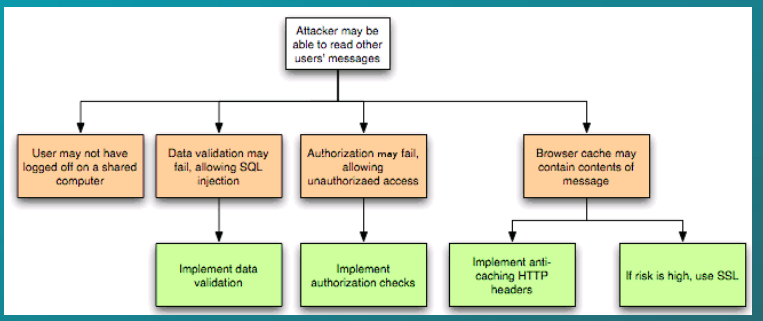
Red Teaming
Programs:
Ransomware Defense
Vulnerability Management
Penetration Testing
Major Incident Response

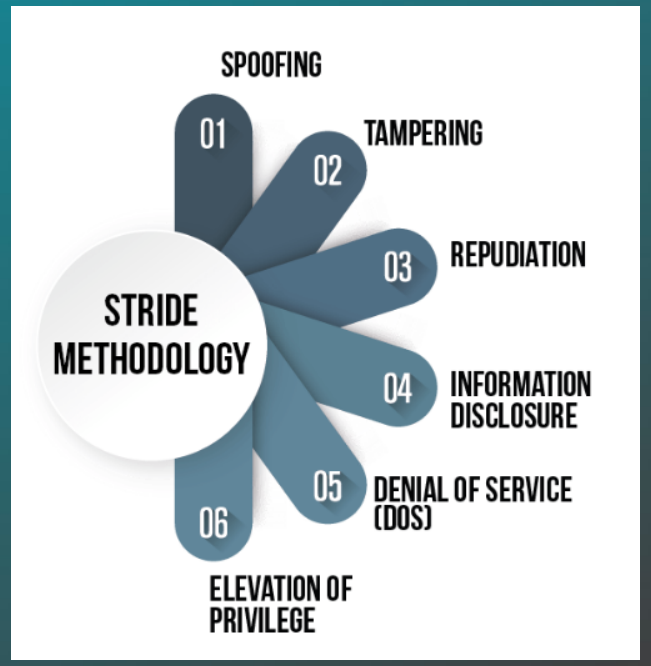
Security Operations Center

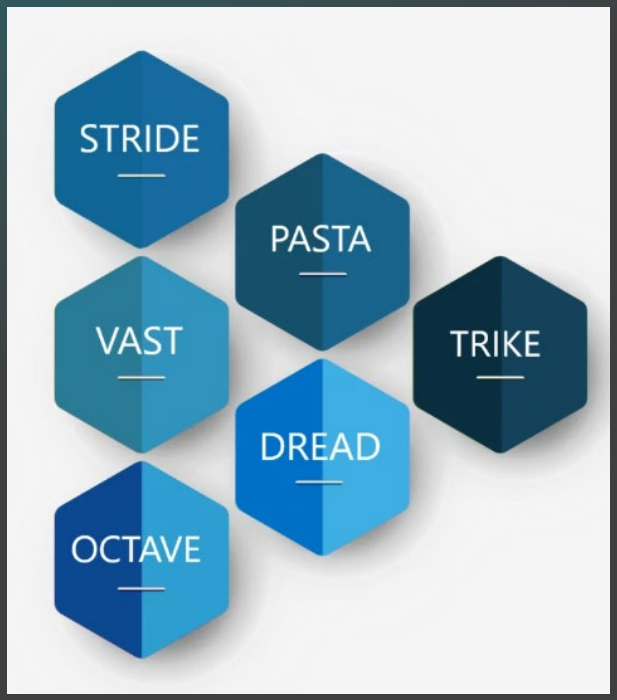
7x24x365
Detection and Response
Security Incident Response
Patch Management

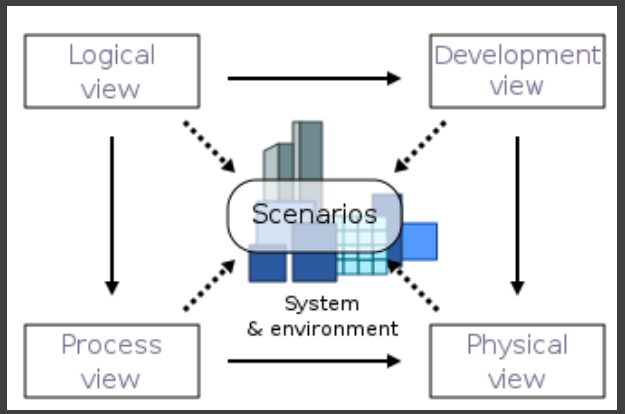


Threat Modeling is an expensive, dark art.





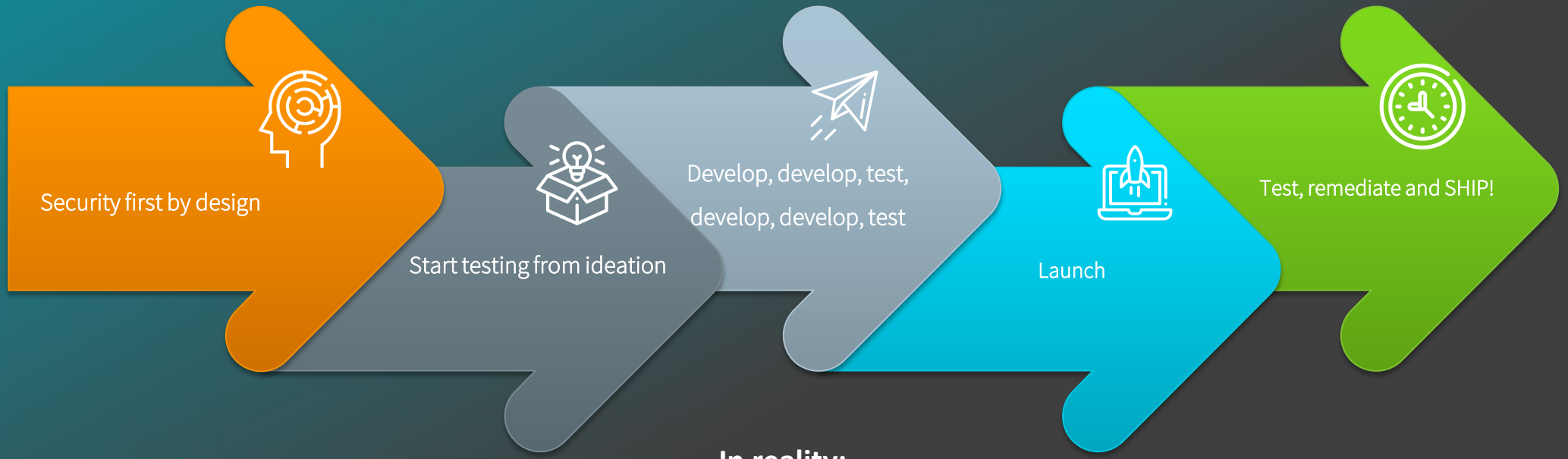




Attack Trees, STRIDE, Movie Plotting, 4+1 and so on…

Threat Modeling has not been a linear process

Frameworks look good in theory
The process is painstaking



In reality:

Shipping is a feature

Threat Modeling does not move at the speed of business

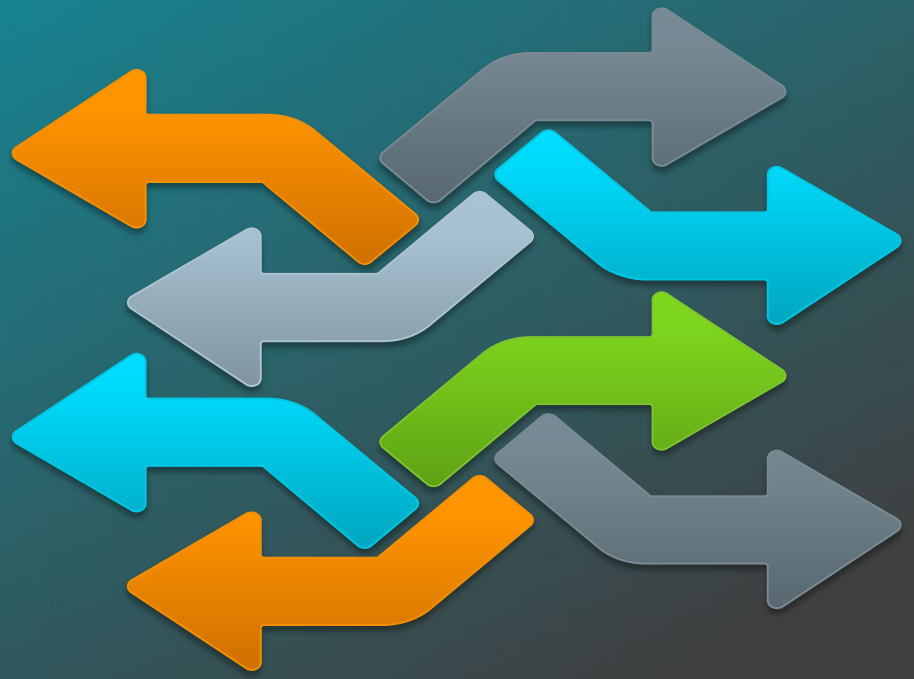
Shortcuts are expensive on many levels

Proving Threat Modeling is tough: usually after a milestone or when threats are found by outsiders

The need for Threat Modeling is clear; the reality is less so…

- **In theory**
  - Threat Model early in the development cycle for Security First
  - Identify security bugs early to mitigate risks
  - Design and build more robust products
  - Think: OWASP Cheat Sheet, Threat Modeling Manifesto, and the Secure Developer‘s Checklist
- **In reality**
  - Manual, inconsistent, invasive, disruptive
  - Based on experience, and experience is expensive
  - Time-consuming for Executive, Business, Developers & IT resources
  - Which threats are credible and relevant?
  - What about future zero-day exploits?
  - How to consistently prove errors of omission?

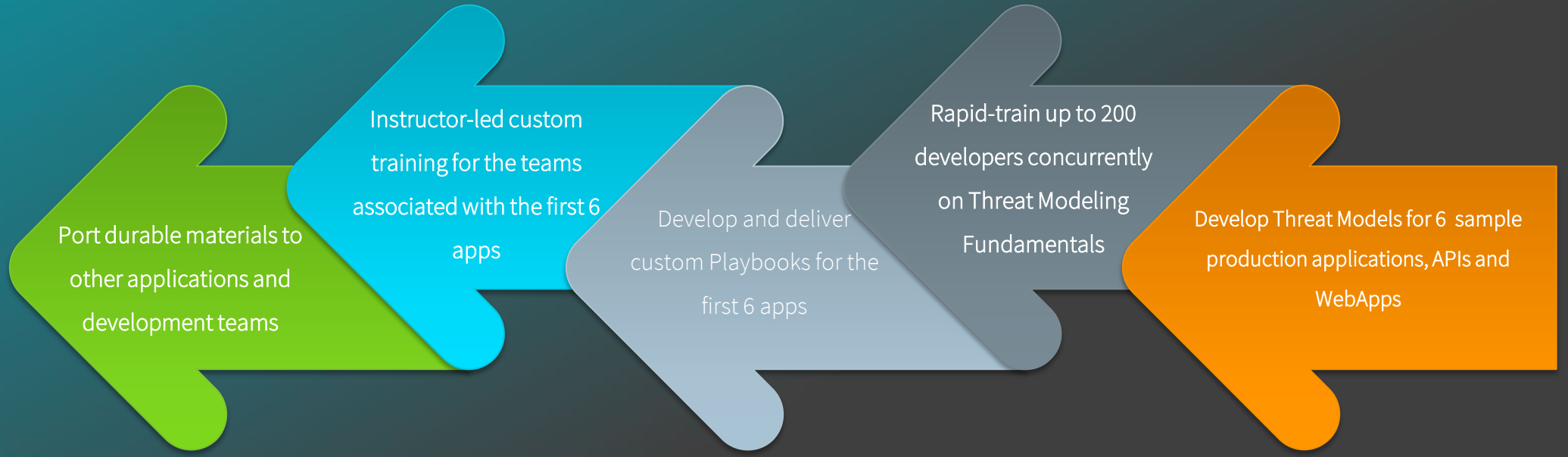
Business velocity is also slowed by the volume of projects



- What accelerates threat modeling at scale?
- What makes threat modeling perpetual?

Accelerated Threat Modeling

Start with shipping products
Develop institutional knowledge
Build skills through tiered-training
Work from relevant, custom playbooks



Automated and curated:

Expert Team of practitioners

Advanced tooling for mapping and training

Changing the tradecraft into procedures :

- **Measurable**
- **Scalable**
- **Repeatable**
- **Effective**
- **Durable**

RESULTS:
Perpetual Threat Modeling
A Culture of Excellence

Benefits to Accelerated Threat Modeling:

Automation :

- Less impact on stakeholders
- Accurate
- Repeatable

Curation:

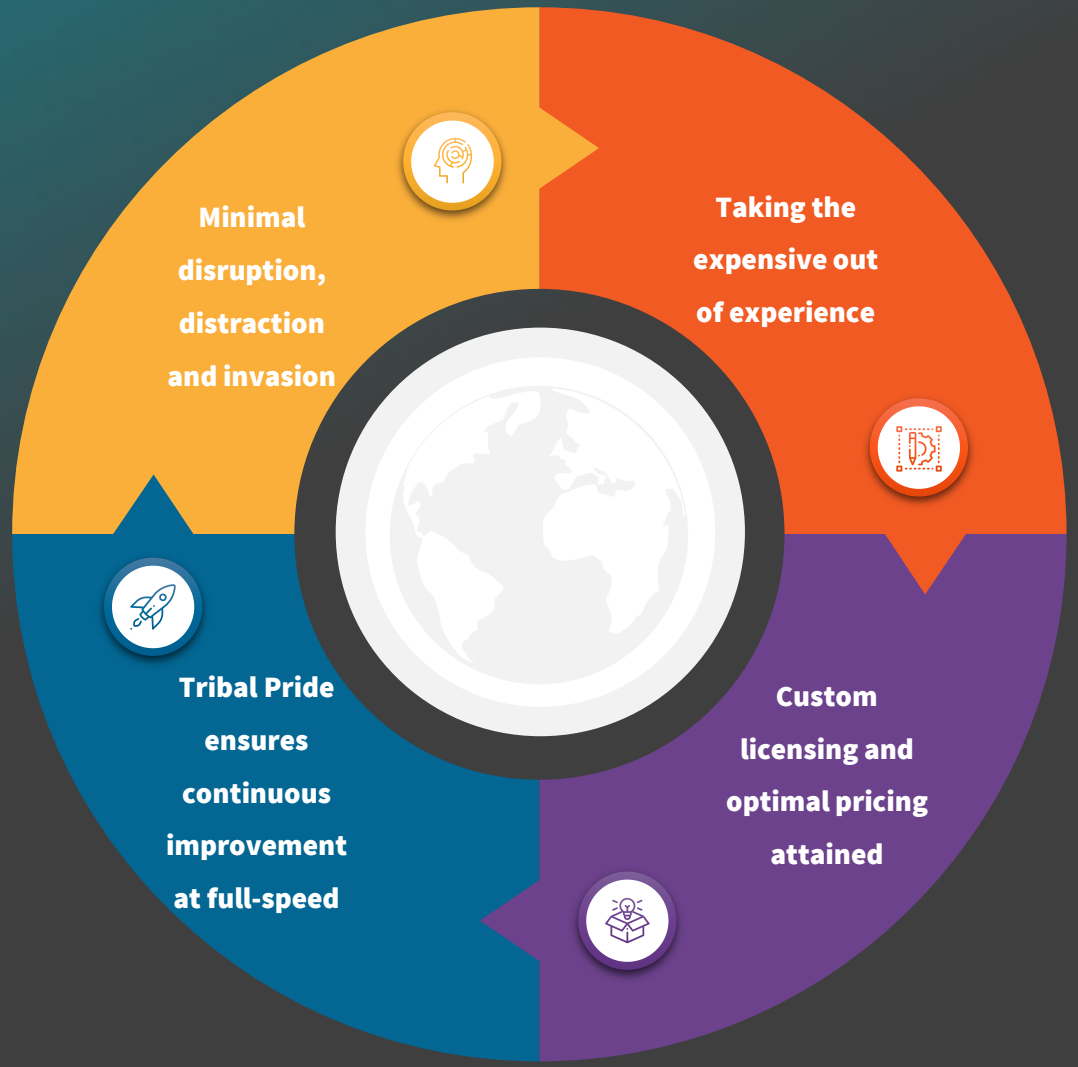
- Expert practitioners
- Expert Educators
- Expert Program Managers

The operative word is Accelerated:

- Everyone is empowered to improve
- Concurrent processed at every phase

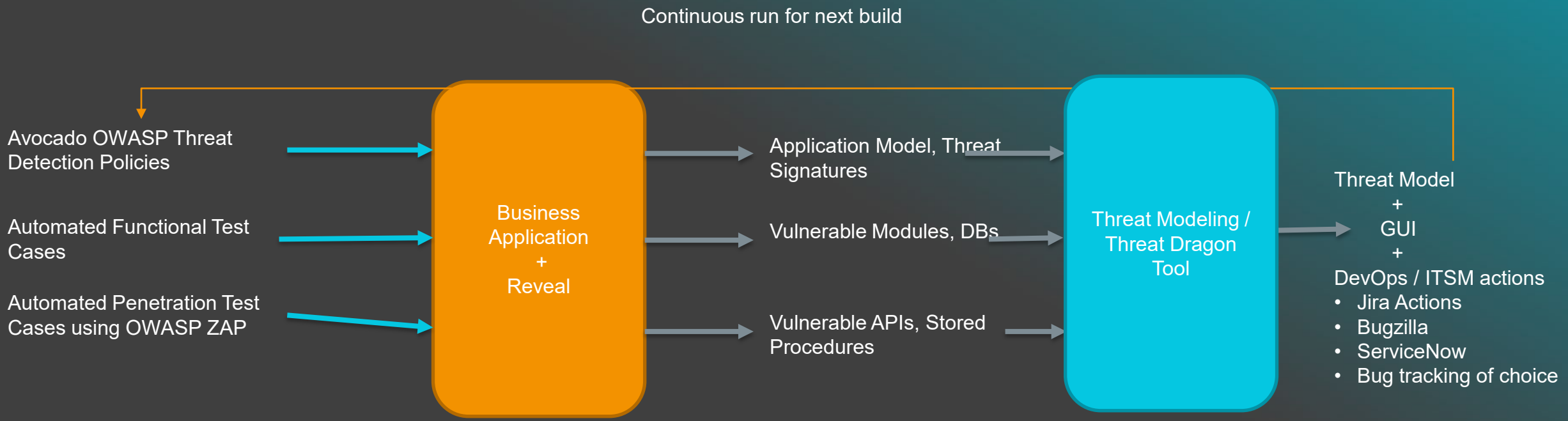
Tooling and Expertise:

- Application Security Observability
- Multiple tools concurrently
- Custom Learning Management System



Automation: Accelerated Threat Modeling

(example of one aspect)



secureCENTRX

Other Professional Services

- **True Red Teaming** – Adversary Emulation: incident preparedness and response programming
- **Software and Systems Testing** – including advanced Threat Modeling
- **Ransomware Prevention Programming** – A curated, comprehensive institutional shift in action
- **vCISO consulting –** references available upon request
- **Secure Software Development Lifecycle** – uniquely qualified practitioners with advanced tools
- **Process Management –** risk-based approach to ISMS aligned to business objectives
- **Managed Security Operations-** high-caliber TTP for firms who do not fund a complete InfoSec team