All Day DevOps

Connected Feedback Loops

Chetan Conikee
CTO/Founder
ShiftLeft Inc.

Goals

"An **enterprise** has to find all security holes in their applications and portals, an adversary only have to find one"

Adversaries are expanding their capabilities everyday. What are we doing?

Strategic Asymmetry

DEFENDER

- Perimeter Security
- Application Firewalls
- Static Analysis
- Dynamic Testing
- Runtime Protection
- Penetration Testing

Credits: Caerphilly Castle, Caerphilly South Wales

ATTACKER

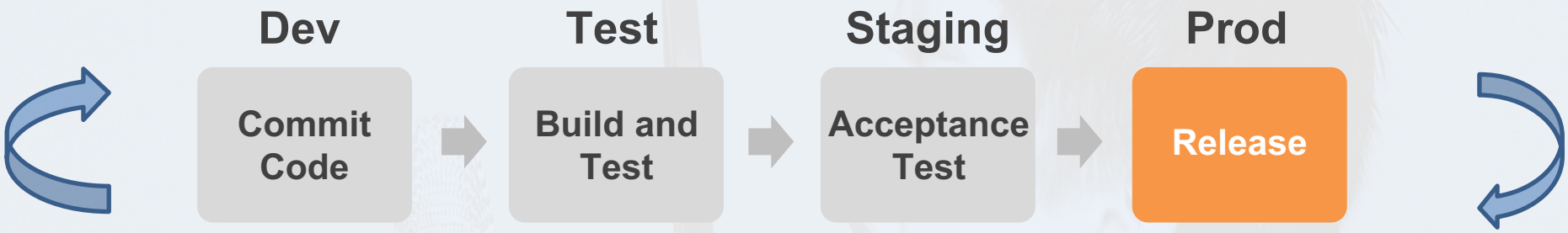
- Bypass opponent's defenses
- Undermine their strengths by exploiting their **weakest links**
- Using methods, non-traditional tactics, or technologies that differ significantly from the other side

Attacking applications is a classic case of manipulating a strategic asymmetry

Applications are often portals

- directly to sensitive data
- unknowingly, to soft underbelly of host and internal network

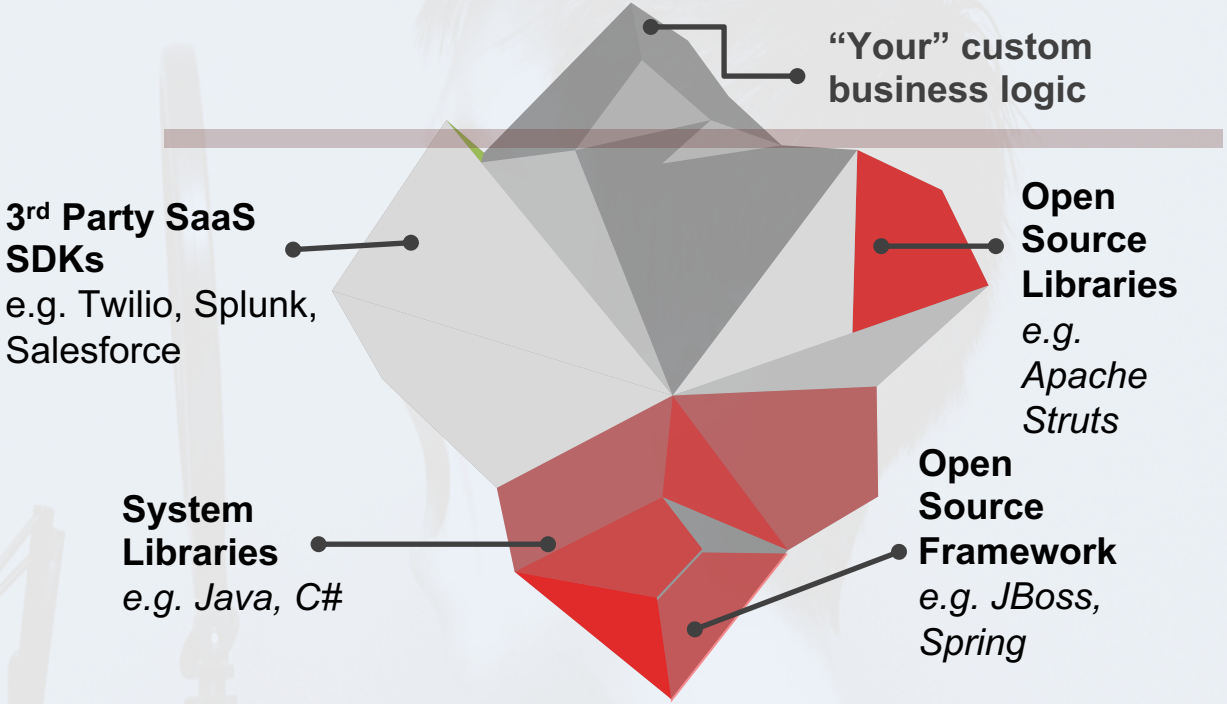
Why are applications the **targets** *du jour*?



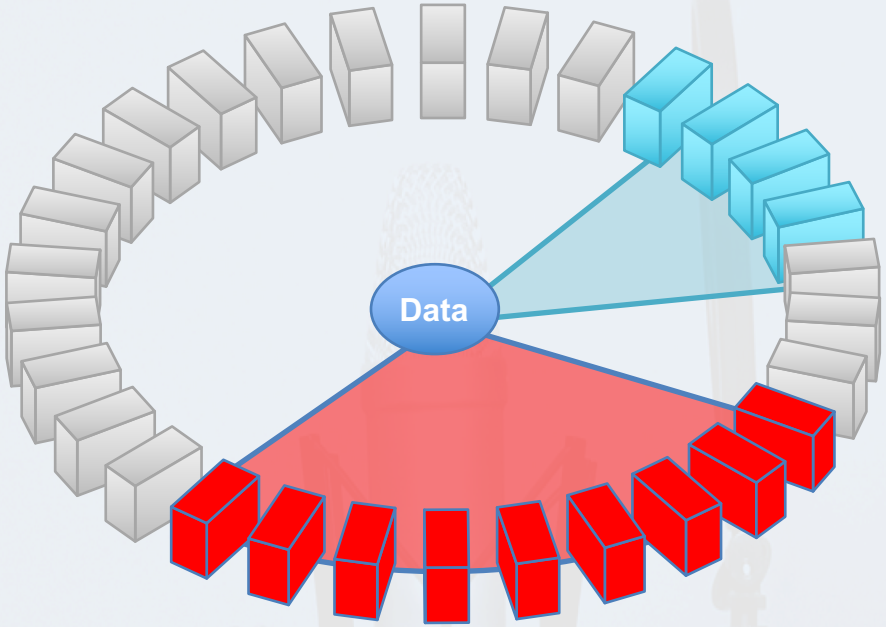
Automation has enabled faster release cycles, but security remains manual

Why are applications the targets *du jour*?

Efficiencies of leveraging 3rd party libraries and SDKs increase security complexity



Why are applications the targets *du jour*?



MicroService architectures make mapping data flows harder while regulations (GDPR & CA Consumer Privacy Act of 2018) expand the definition which data types are critical

The Security of a System

Vulnerabilities

defects or weaknesses in system that can be exercised and result in a security breach or violation of policy

Policies

Guarantees that a system can still give despite attacks. Expresses properties in dimensions of confidentiality, integrity and availability

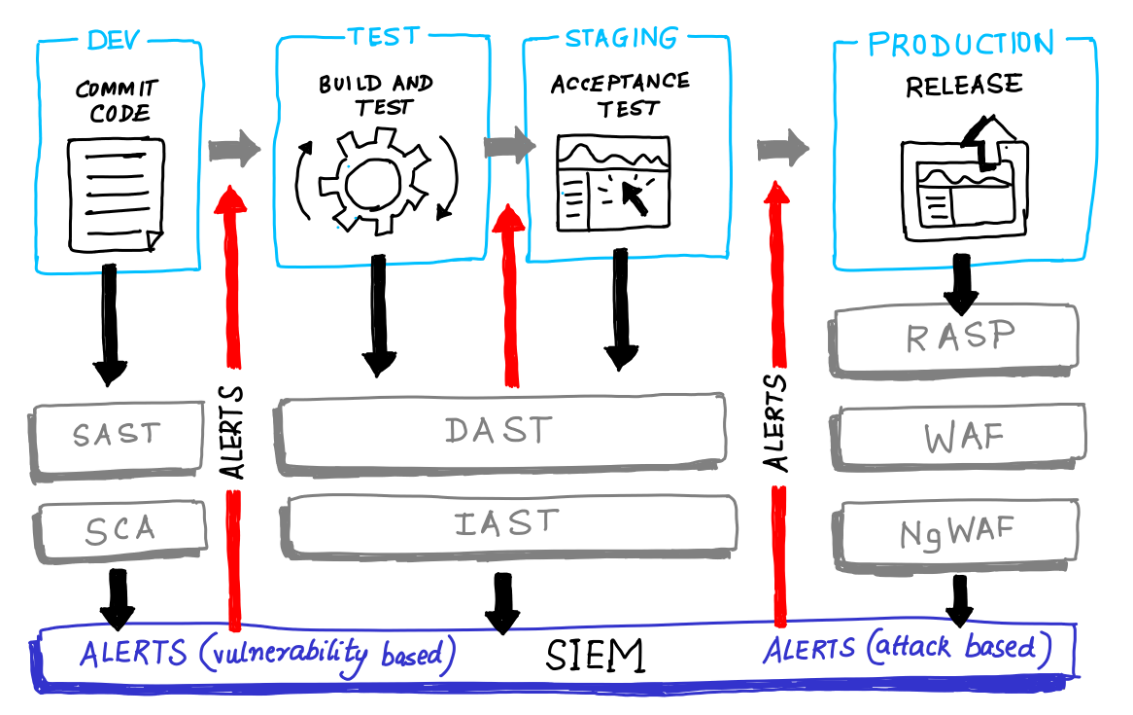
Attacks

Directed against system interface i.e. attack surface with goal of infringing at least one policy of a system

Defenses

Enforce policies when violation is detected using monitoring, isolation and obfuscation

Defense in Depth has failed us



- Lack of Context
- False Positives
- Questionable Relevance
- No clear prioritization
- SIEM architecture limitations

Outcome

ars TECHNICA

Muni system hacker hit others by scanning for year-old Java vulnerability

GIZMODO

Wag Left User Data Exposed

Bloomberg Technology

Uber Hack Shows Vulnerability of Software Code-Sharing Services

- **159,700 Cyber Incidents**
- **7B records exposed**
- **$5B financial impact**
- **93% of breaches could have been prevented**

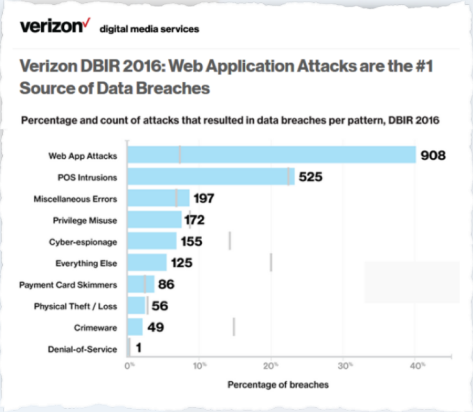
*One Trust Alliance report 2018

"A vast majority of the attacks will be on the custom code in an application"

Gartner

TC

Mixpanel analytics accidentally slurped up passwords



WIRED

LILY HAY NEWMAN SECURITY 09.14.17 01:27 PM

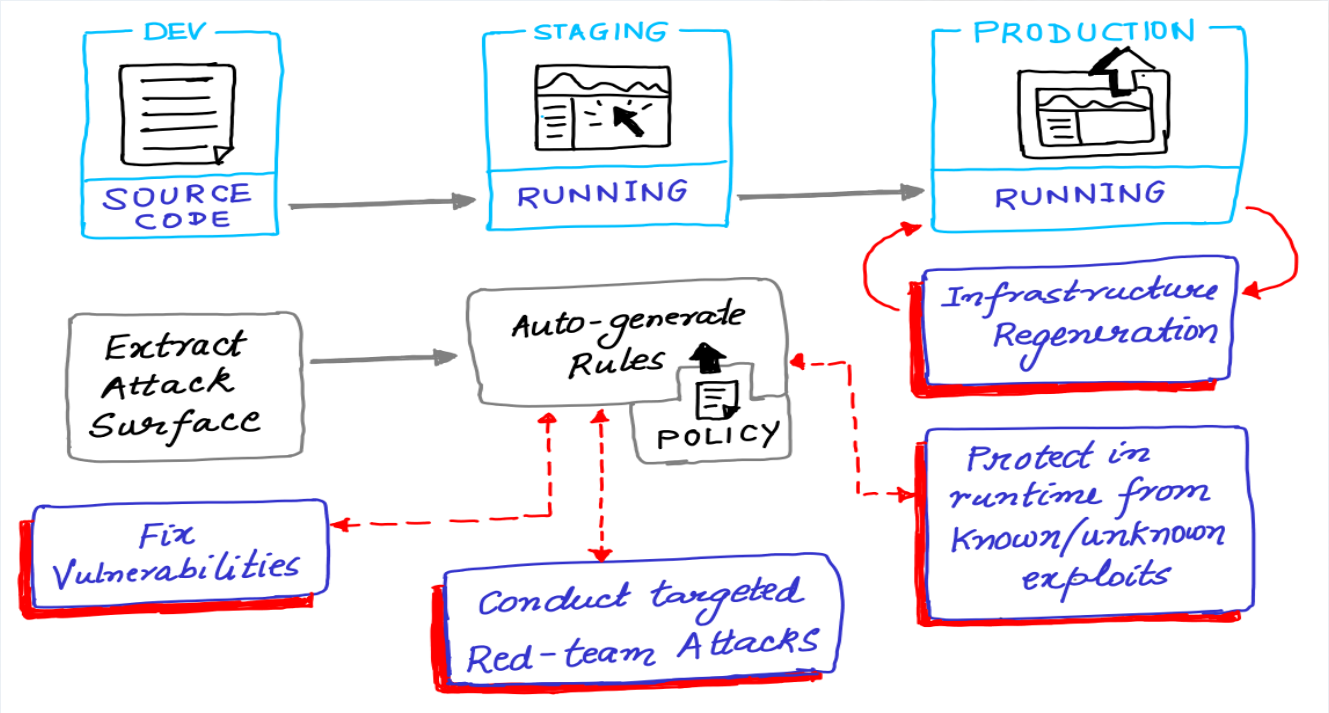
EQUIFAX OFFICIALLY HAS NO EXCUSE

InfoWorld FROM IDG

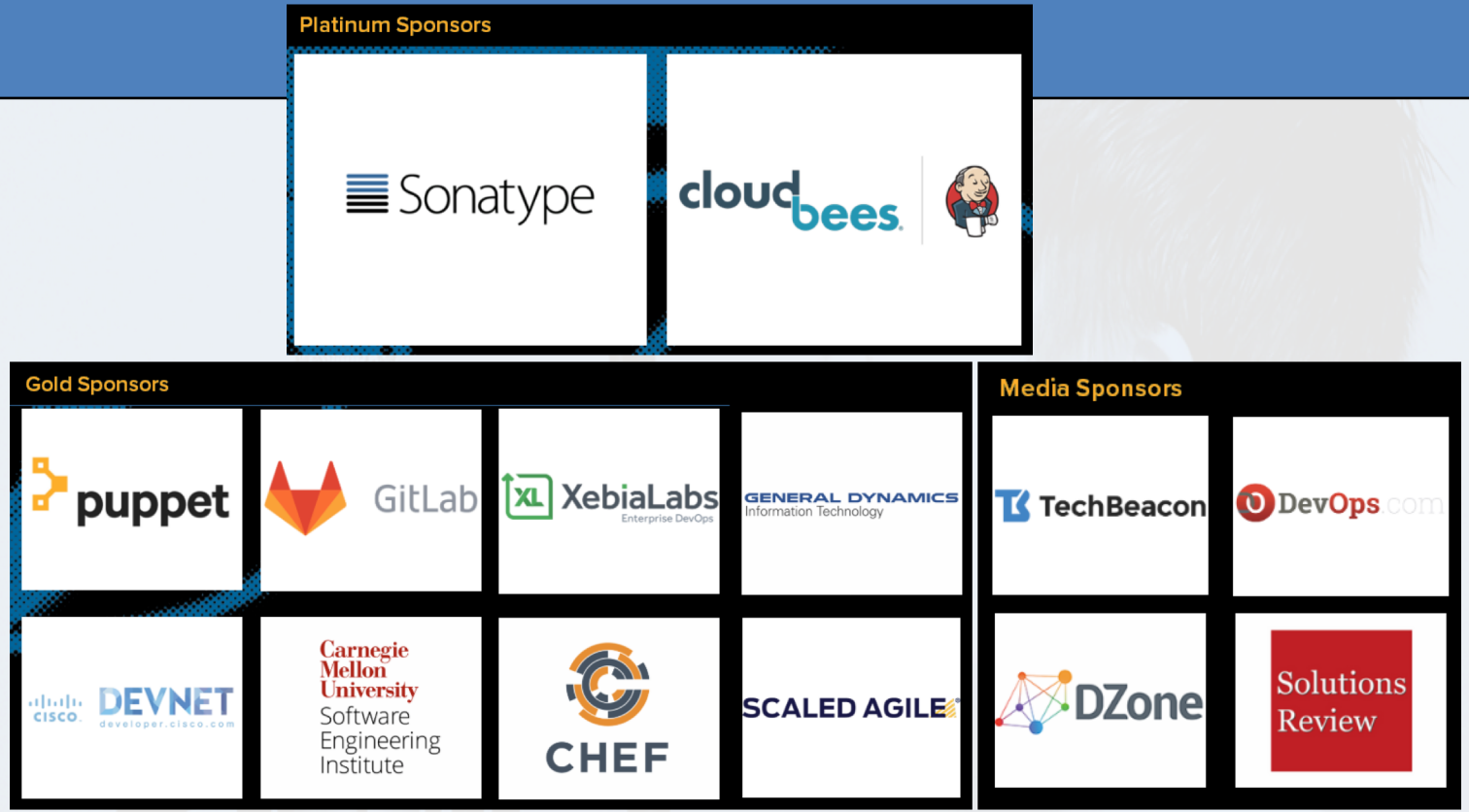
How you could be leaking your secrets onto GitHub

Connected Feedback Loops

Understand offense to inform defense



Thank You All Day DevOps Sponsors



Thank You All Day DevOps Supporters

Meet Me in the Slack Channel for Q&A

bit.ly/addo-slack