RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: ASEC-W02

EXPLORING THE REAL-WORLD APPLICATION SECURITY TOP 10

Shannon Lietz

Director, DevSecOps
Intuit
@devsecops

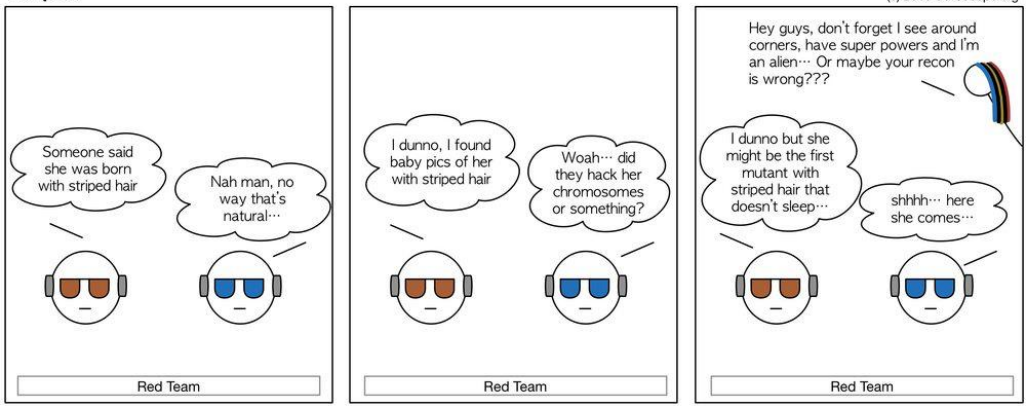
<me />

SOFTWARE
SAFER
SOONER

1984 1989 1996 2001 2011 PRESENT

DEVELOPER
SECURITY
OPERATIONS
"DEVSECOPS"
"RUGGED"

IANS



intuit

DEVSECOPS
-- FOUNDER --

HACKERGIRL
https://hackergirl.io

DEV SEC OPS
SOFTWARE SAFER SOONER

The Problem… Are we chasing the right issues?

1. How are the current issues the “right” issues?
2. Is what we are testing driving us towards the “right” issues?
3. Are we using the “right” tools?

How will we know?

Dimensions of the Proof

We will know when:

1) We **understand** our application and its adversaries.

2) We **measure** and track results.

3) We **correct continuously** to get ahead of adversaries.

a) Know our Application

Security Facts

Original Lines of Code	300
Open Source Components	25
Type: **Embedded** Version	1.0
Intended Version Lifetime/Expiration	02/2020
Organization Security Trend at Release	3.2
Security Degradation Rating	A
Required Monthly Customer Maintainence	2

	% Control Values
Adversary Interest	**97%**
Residual Risk	**8%**
Preventative Measures	**93%**
Access Control	100%
Encryption	95%
Tamper	91%
Detective Measures	**99%**
Remote	99%
Local	99%

NIST	99%	▪	OPNGBK	91%
PCI DSS	92%	▪		

* All values are based on modeled Abuse and FMEA cases for this class of device and applicable implementation patterns. Your results may fluctuate according to intended business risk profile and residual risk tolerances that allow for some controls to be less restrictive. Actual results may also vary with creative use or experimental implementation.

What do we know?

1) **Deployment Architecture** -> Attack Map or Threat Model

2) **Component Manifest** -> Required Patching Frequency/Upkeep

3) **Lines of Code** -> Defect Density

4) **Tests Applied** -> Quality

b) Know our Application's Adversaries

Security Facts

Original Lines of Code	300
Open Source Components	25
Type: **Embedded** Version	1.0
Intended Version Lifetime/Expiration	02/2020
Organization Security Trend at Release	3.2
Security Degradation Rating	A
Required Monthly Customer Maintainence	2

	% Control Values
Adversary Interest	97%
Residual Risk	8%
Preventative Measures	93%
Access Control	100%
Encryption	95%
Tamper	91%
Detective Measures	99%
Remote	99%
Local	99%

NIST	99%	▪	OPNGBK	91%
PCI DSS	92%	▪		

* All values are based on modeled Abuse and FMEA cases for this class of device and applicable implementation patterns. Your results may fluctuate according to intended business risk profile and residual risk tolerances that allow for some controls to be less restrictive. Actual results may also vary with creative use or experimental implementation.

DEV SEC OPS — SOFTWARE SAFER SOONER

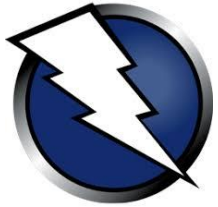
Approach

- Study for a year with layering approach
- Experiments should not overlap when possible
- Measurements are evaluated for skew
- Attackers should be unaware of the experiment
- We must understand motivations, methods, and interest

Tools used in this Research

HONEY

SCANNERS



DETECTION

Top 10 Comparison

	OWASP TOP 10 App Sec Risks	Real-World Top 10 Attacks
1	Injection	Direct Object Reference
2	Broken Authentication	Forceful Browsing
3	Sensitive Data Exposure	Null Byte Attack
4	XML External Exposures (XXE)	Command Injection
5	Broken Access Control	Feature Abuse
6	Security Misconfiguration	Evasion Techniques
7	Cross Site Scripting	Subdomain Takeover
8	Insecure Deserialization	Misconfiguration
9	Using Components with Known Vulnerabilities	Cross Site Scripting
10	Insufficient Logging/Monitoring	SQL Injection

Categories of Adversaries

Scanners

Researchers

Paid Noise

Advanced Adversaries

Motivations

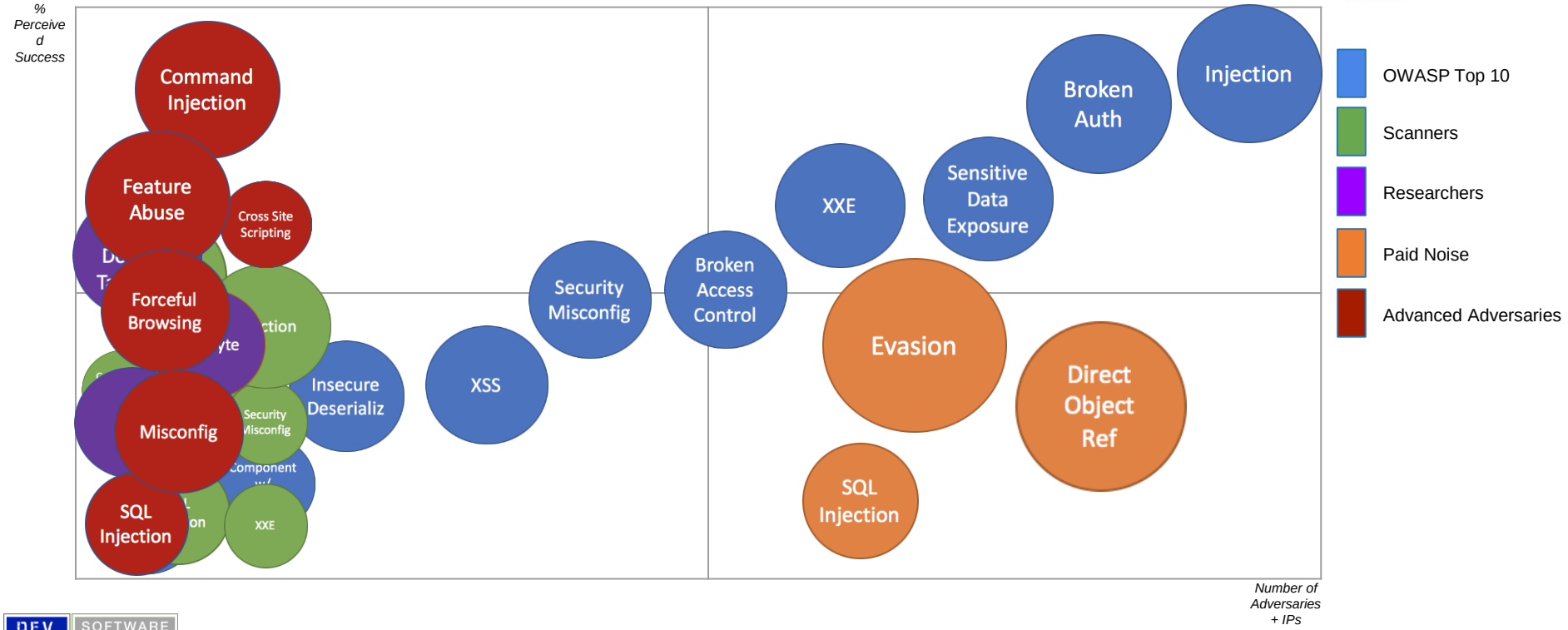
Information Brokerage

Fame / Payment

Continuous Payment

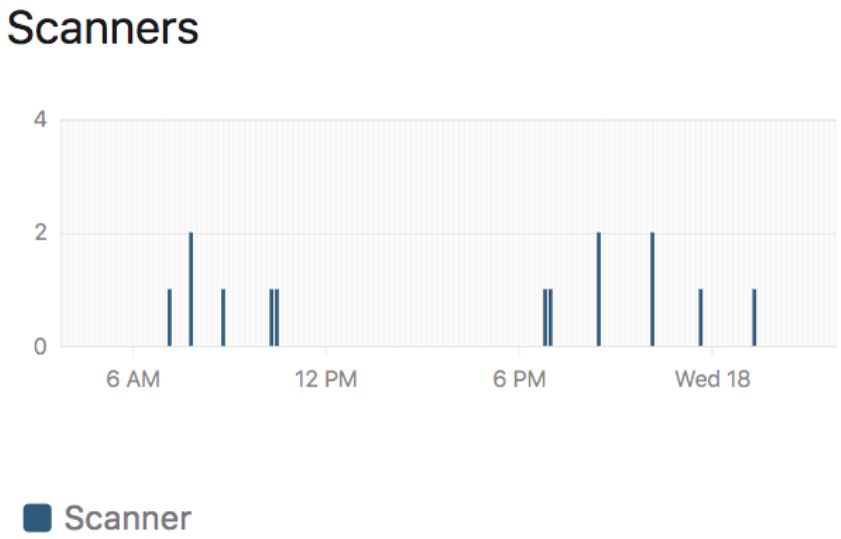
Control / Payment

OWASP vs. Real World



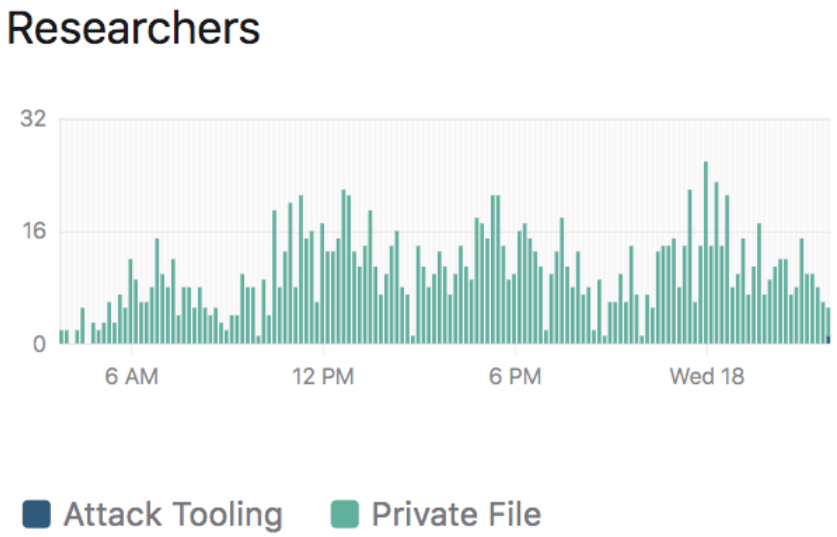
Scanners

- Continuously running on a schedule
- Scanners run for good and/or bad purpose
- Cost of running vs. Cost of information discovered



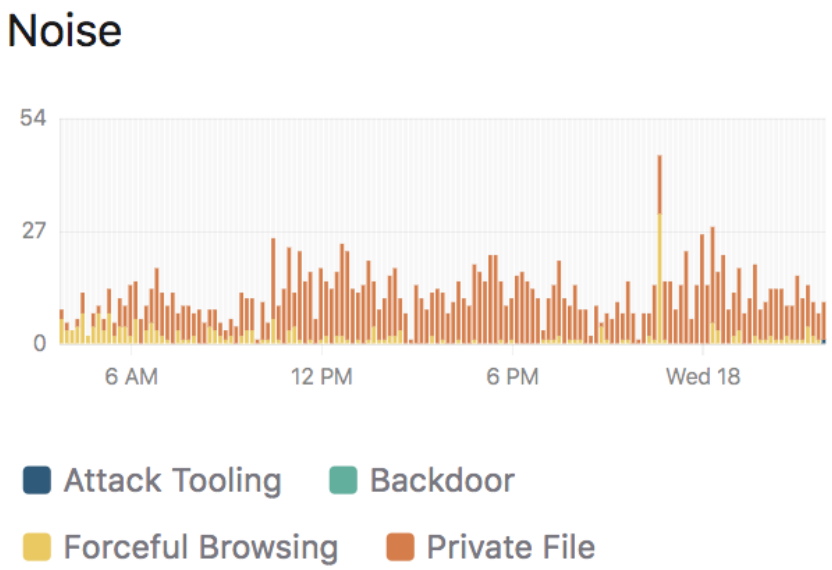
Researchers

- Commonly apply their efforts to get paid through bug bounties
- More likely to use common tools and standards
- Time spent must be worth effort



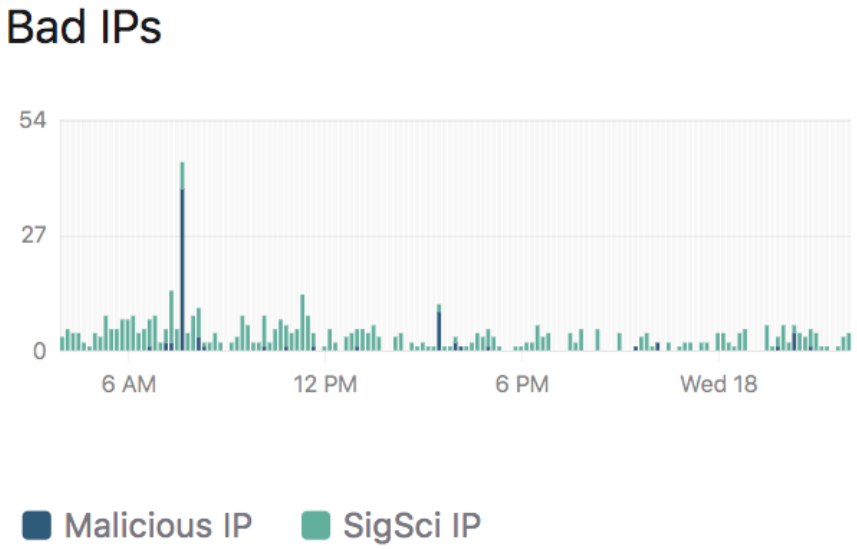
Paid Noise

- Running when other attacks occur
- Used to outrun automated detection and AI/ML
- Cost of running must be low enough to allow for profit



Advanced Adversaries

- Commonly low and slow
- Leverages more human assisted automation schemes
- Investment must not be easy to disrupt



Some interesting insights...

Bad guys:

- like to use scanning signatures to **whitelist themselves**
- **don't use commercial scanners** except for noise or whitelisting
- have a few **"goto" TTPs** because they just work
- don't underestimate the value of **cryptocurrency** mining
- are not afraid of **AI/ML**
- **hide** in lots of noise

Measurements

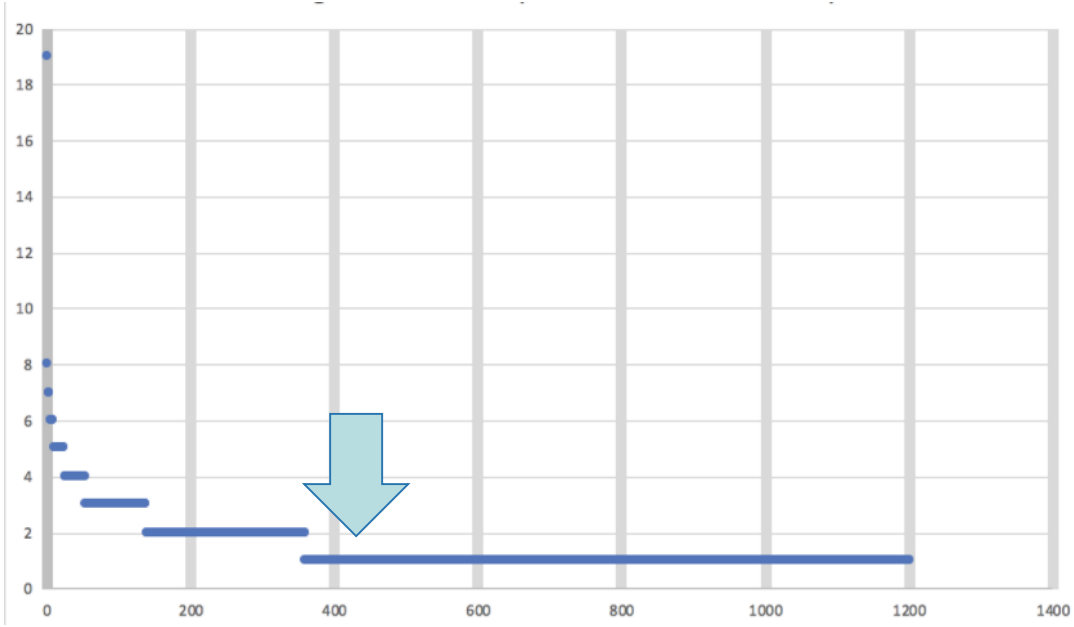
1) How often do adversaries return? ***Return Rate***

2) How often do adversaries change their tactics? ***Rate of Change***

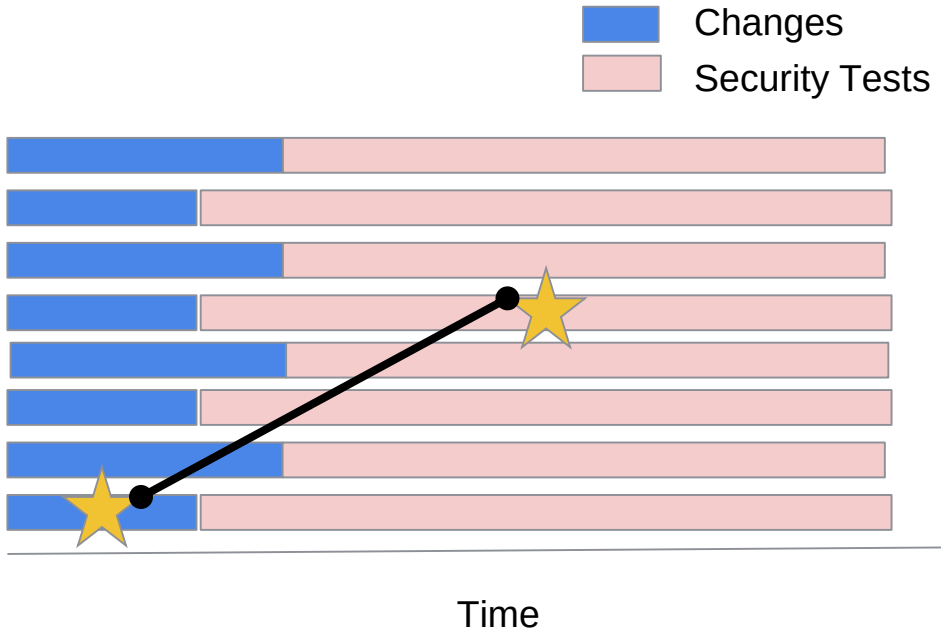
3) How confident is the adversary? ***Cost of fix***

4) How long do they have to find an issue? ***Mean Time to Identification***

Adversary Return Rate



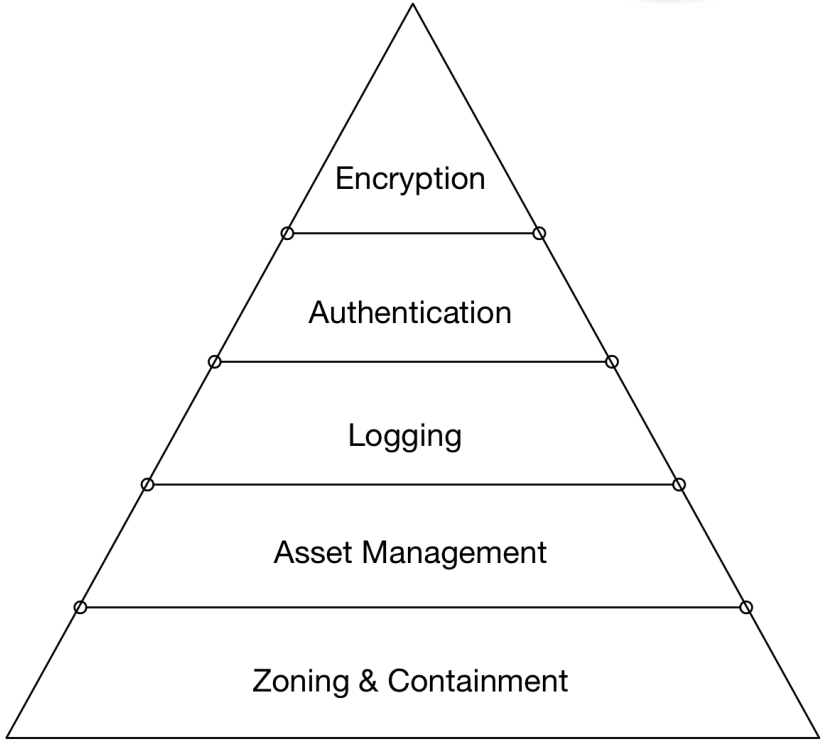
Mean Time to Identification



How do we correct continuously?

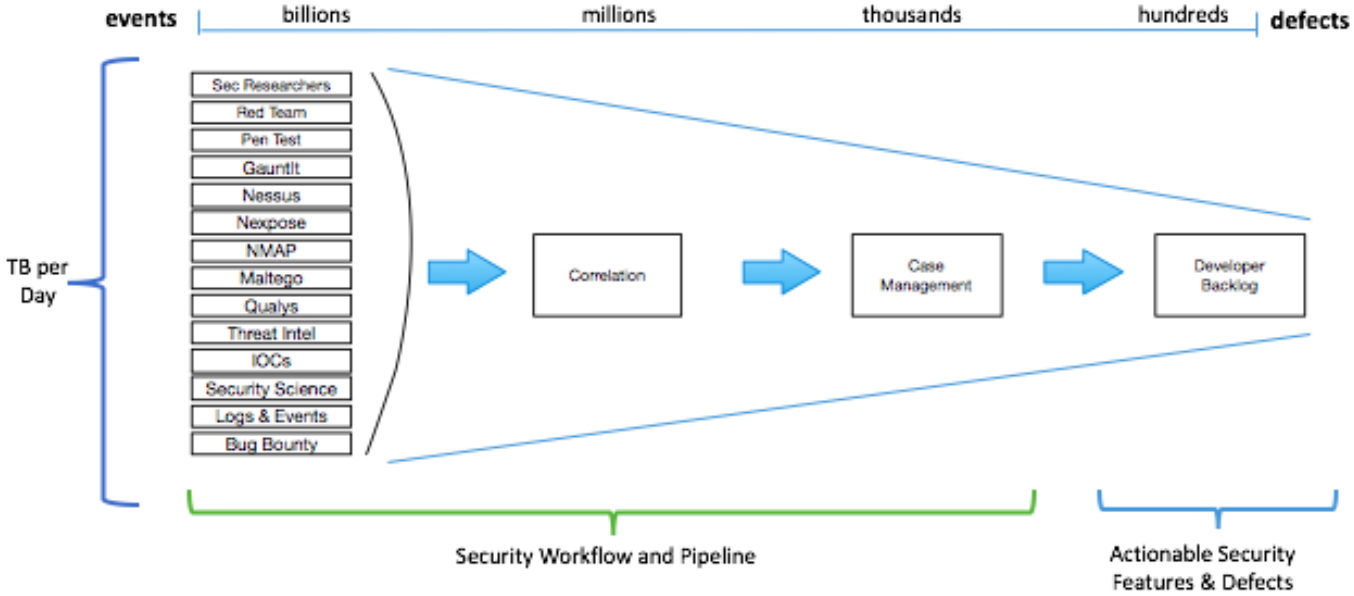
- Everyone knows Maslow…
- If you can remember 5 things, remember these ->

"Apps & data are as safe as where you put it, what's in it, how you inspect it, who talks to it, and how its protected…"

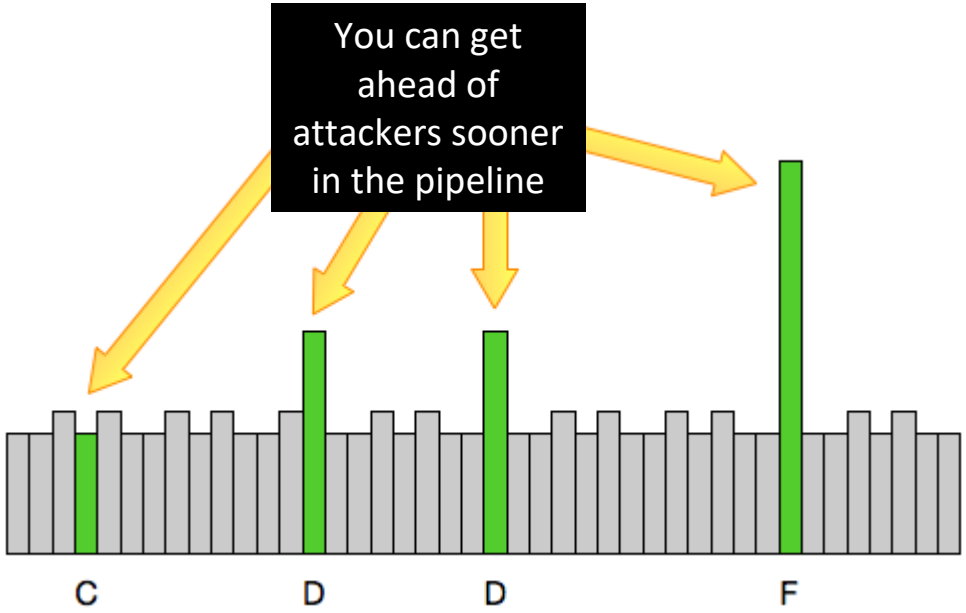


DEV SEC OPS SOFTWARE SAFER SOONER

How do we keep pace?



How do we get ahead?



Apply What You Have Learned Today

- **Next week you should:**
  - Assess your attack surface and collect telemetry
- **In the first three months following this presentation you should:**
  - Examine telemetry data and determine the characteristics for your application's adversaries
  - Can you say who your top adversary or attack is?
- **Within six months you should:**
  - Understand how to forecast the most important issues to fix
  - Be able to measure and report on defects fixed ahead of adversaries