The Flaws in Hordes,
The Security in Crowds

MIKE SHEMA
MIKE@COBALT.IO
“You see, in this world there’s two kinds of people, my friend: Those with loaded guns and those who dig. You dig.”

– Clint Eastwood, *The Good, the Bad, and the Ugly.*
“There are two kinds of spurs, my friend. Those that come in by the door; those that come in by the window.”

Uneasy Alliances

“What’s the price for this vuln?”
— Bounties

“What’s the cost to fix this vuln?”
— DevOps

“What’s the value of finding vulns?”
— CSOs
Disclosure Happens
Some Observations of Swarms of Strange Insects, and the Mischiefs done by them.
Bounties are an imperfect proxy for risk, where price implies impact.

- $0
- $15K
- $10,000
- $50
- XSS self, no auth
- XSS any auth’d user, access sensitive info

~$800 avg.
Bounties are an imperfect proxy for work, where earnings often diverge from effort.
Acceptance State of Vulns (2016)

Duplicate | Invalid | Out of Scope | Valid

Bug Bounty | Pen Test
Noise increases cost of discovery and reduces efficiency.
Volume—
Reports/day
Percent valid

Triage—
Time/report
People/report

The Cost of Noise

Overhead

Signal + [Baseline]
<table>
<thead>
<tr>
<th>Category</th>
<th>Pen Test</th>
<th>Bug Bounty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and Sessions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Components with Known Vulnerabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross-Site Request Forgery (CSRF)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross-Site Scripting (XSS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insecure Object References</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misconfiguration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Missing Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redirects and Forwards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Code Execution (RCE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensitive Data Exposure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL injection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Scanners

Overlaps, gaps, and ceilings in capabilities. Fixed-cost, typically efficient, but still require triage and maintenance.
Exhausting the Pace of Vulns...or Attention?

Days Since Valid (Any) Report

Days Since Previous Valid Report

Valid Vulns per Program

<table>
<thead>
<tr>
<th></th>
<th>2016</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days Since Valid (Any) Report</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50%</td>
<td>7 (4)</td>
<td>4 (1)</td>
</tr>
<tr>
<td>80%</td>
<td>16 (8)</td>
<td>10 (5)</td>
</tr>
<tr>
<td>95%</td>
<td>33 (14)</td>
<td>23 (11)</td>
</tr>
</tbody>
</table>

50% | 80% | 95%

Days since any report: 2, 5, 11
The Crowd's Hoard

Public, Private Bounties
The Crowd's Hoard

Reports

Researchers

12%
36%
67%

Pen Tests
“We’ll always have bugs. Eyes are shallow.”

– Mike’s Axiom of AppSec
BugOps vs. DevOps
Chasing bugs isn’t a strategy.
As we move to security as code, code moves to inevitable legacy.
Threat Modeling

DevOps exercise guided by security.
Influences design.
Informs implementation.
Increases security awareness.
Risk Reduction
“You’re not using HTTPS.”
“Use HTTPS.”
“Seriously. Please use HTTPS.”
Let’s Encrypt.
Bounty ranges as a proxy for SDL, where price implies maturity.

<table>
<thead>
<tr>
<th>Price</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1</td>
<td>Experimenting</td>
</tr>
<tr>
<td>$1,000</td>
<td>Enumerating</td>
</tr>
<tr>
<td>$10,000</td>
<td>Exterminating</td>
</tr>
<tr>
<td>$100,000</td>
<td>Extinct-ifying</td>
</tr>
</tbody>
</table>
Security from Inventory

Enumerate your apps.
Generate their dependency graphs.
Identify ownership.
Security from Crowds

Provide reasonable threat models.
Report via issue trackers.
Automate reproduction steps.
Security from DevSecOps

Measure vuln discovery effort
Monitor risk for trends
Illuminate brittle design
Thank You!
Questions?

@CodexWebSecurum
Advertisement.

The Reader is hereby advertised, that by reason of the present Contagion in London, which may unhappily cause an interrup-
tion as well of Correspondencies, as of Publick Meetings, the
printing of these Philosophical Transactions may possibly for a
while be intermitted; though endeavors shall be used to continue
them, if it may be.
R —
www.r-project.org
RStudio —
www.rstudio.com
data.table
ggplot
A cacophony of hordes.

A scrutiny of crowds.