One of the 1st vulnerability researchers at the hacker think tank, L0pht in 90’s. Founding team at @stake 1st independent security consultancy. Founded Veracode in 2006.
Impacts from application security vulnerability

- Application Downtime: 49%
- Increased Operational Costs: 42%
- Application Performance Issues: 38%
- Customer Data Loss: 27%
- Negative Press/Damage to Brand: 25%
- Intellectual Property Loss: 22%

*How to Make Application Security a Competitive Advantage, IDG Market Survey, March 2018*
Customers are Concerned About Your Software Security

- **74%** Concerned about sharing data with businesses
  - IPOS-MORI Study

- **70%** Have taken steps to reduce exposure online
  - IPOS-MORI Study

- **50%** Have dropped a service after a publicized breach*
  - CA Digital Trust Survey

- **84%** Organizations include security requirements into contracts
  - IDG Survey Report on Security as a Competitive Advantage
INTERNALLY DEVELOPED VS. THIRD-PARTY (COMMERCIAL) APPLICATIONS

Applications Passing OWASP Top 10 Policy

<table>
<thead>
<tr>
<th>Year</th>
<th>Internally Developed</th>
<th>Passed</th>
<th>Did Not Pass</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>35%</td>
<td>65%</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>38.9%</td>
<td>61.1%</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>37%</td>
<td>63%</td>
<td></td>
</tr>
<tr>
<td>Third-Party</td>
<td>22.7%</td>
<td>77.3%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>25.4%</td>
<td>74.6%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>28%</td>
<td>72%</td>
<td></td>
</tr>
</tbody>
</table>

Pc of in-bu so de dc ap
Evaluating the Security of Software

1st Party Code
Secure Coding
Scan Frequency
Pre-/Post-Production

Open Sourced Code
How to Fix
Integrated Scanning

You change the world, we’ll secure it.

© 2019 VERACODE INC.
Validating a Secure Development Process

**Veracode Verified**
- **Code Security**
  - No Very High Flaws
- **Developer Training**
  - Security Champion
- **Assessment Target**
  - Assess 1st Party Code

**Verified Standard**
- Security Baseline
- No Very High Flaws

**Verified Team**
- Secure Coding Culture
- No Very High Flaws
  - No High Flaws

**Verified Continuous**
- Business-Driven Maturity
- No Very High Flaws
  - No High Flaws
  - No Medium Flaws

**Integrated Scanning**
- Assess 3rd Party Code
- Integrated Scanning

**Application Security Maturity**

---

You change the world, we’ll secure it.

© 2019 VERACODE INC.
DevSecOps is becoming the norm.
DevSecOps Indicator: Percentage of Scans by Account Type

SOURCE: Veracode, State of Software Security Volume 8, 2017-10-18
DevSecOps Indicator: Average Number of Scans Per Application

<table>
<thead>
<tr>
<th>Year</th>
<th>Scans Per Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>7.5</td>
</tr>
<tr>
<td>2016</td>
<td>10.9</td>
</tr>
<tr>
<td>2017</td>
<td>14.5</td>
</tr>
<tr>
<td>2018</td>
<td>21.9</td>
</tr>
</tbody>
</table>

SOURCE: Veracode, State of Software Security Volume 8, 2017-10-18
The DevSecOps Effect

Source: Veracode SOSS Volume 9

You change the world, we’ll secure it.
A Roadmap to Compliance

You change the world, we'll secure it.

© 2019 VERACODE INC.
Roadmap to Self-Regulation

- Incentive-based
- Outcomes
- Prescriptive & Directive

not

- Punishment-based
- Point-in-time
- Technology

You change the world, we’ll secure it.
But what about?

- Threat modeling
- Code review
- Manual penetration tests

Use information from multiple trusted sources to feed into one score. Like a credit rating!
A Software FICO?

1. Payment History: 35%
2. Amounts Owed: 30%
3. Length of Credit History: 15%
4. New Credit: 10%
5. Types of Credit in Use: 10%

1. Code Security
2. Developer Training
3. Assessment Target
4. Threat Modelling
5. Manual Penetration Testing
VERACODE
You change the world, we’ll secure it.

Chris Wysopal
cwysopal@veracode.com
@weldpond

https://www.veracode.com/verified/directory