The State of Application Security

Sandy Carielli, Principal Analyst, December 10, 2019
21 Days Until The End Of The Decade
I FEEL THE NEED

THE NEED, FOR SPEED!
Development Teams Are Moving Faster

In 2018, 27% of developers indicated that they released monthly or faster. In 2019, the number jumped to 38%.

Base: 3,294 Developers
Source: Forrester Business Technographics Global Developer Survey, 2019

Base: 3,228 Developers
Source: Forrester Business Technographics Global Developer Survey, 2018
Yes, Open Source Is Prevalent In IoT

Synopsys: 2019 Open Source Security And Risk Analysis
In 2019, 54% of Containers Live For Five Minutes or Less

33% of firms suffered a breach as a result of an external attack. This is how.

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software vulnerability (software exploit)</td>
<td>40%</td>
</tr>
<tr>
<td>Web application (SQL injection, cross-site scripting, remote file inclusion)</td>
<td>37%</td>
</tr>
<tr>
<td>Use of stolen credentials (logins, encryption keys)</td>
<td>28%</td>
</tr>
<tr>
<td>DDoS</td>
<td>25%</td>
</tr>
<tr>
<td>Strategic web compromise (watering hole attack)</td>
<td>25%</td>
</tr>
<tr>
<td>Mobile malware</td>
<td>25%</td>
</tr>
<tr>
<td>Exploitation of lost/stolen asset</td>
<td>25%</td>
</tr>
<tr>
<td>DNS</td>
<td>20%</td>
</tr>
<tr>
<td>Phishing</td>
<td>19%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>14%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>

Base: 283 Enterprise global network path security decision makers who experienced an external attack when their company was breached

Sources: Forrester Analytics Global Business Technographics® Security Survey, 2019

Software vulnerabilities and web applications are the top two ways external attacks are carried out.
**CVE-2000-0388 Detail**

**Current Description**
Buffer overflow in FreeBSD libmytinfo library allows local users to execute commands via a long TERMCAP environmental variable.

https://nvd.nist.gov/vuln/detail/CVE-2000-0388

Synopsys: 2019 Open Source Security And Risk Analysis
Containers And Images Are Not Immune

Source: Snyk: Shifting Docker Security Left: https://snyk.io/blog/shifting-docker-security-left/
KEEP CALM AND SHIFT LEFT
SAST adoption

Phase of the SDLC in which SAST is implemented

- Planning to implement within the next 12 months
- Implementing/implemented + Expanding/upgrading implementation

<table>
<thead>
<tr>
<th>Phase of the SDLC</th>
<th>Planning within 12 months</th>
<th>Implementing/implemented + Expanding/upgrading implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>18%</td>
<td>17%</td>
</tr>
<tr>
<td>Development</td>
<td>35%</td>
<td>34%</td>
</tr>
<tr>
<td>Testing</td>
<td>42%</td>
<td>37%</td>
</tr>
<tr>
<td>Production</td>
<td>25%</td>
<td>40%</td>
</tr>
</tbody>
</table>

Base: 1,014 global network path security decision makers who are adopting SAST
Source: Forrester Analytics Global Business Technographics Security Survey, 2019
SCA adoption

Base: 1,035 global network path security decision makers who are adopting SCA
Source: Forrester Analytics Global Business Technographics Security Survey, 2019
Container Security adoption

Phase of the SDLC in which Container Security is implemented

- Planning to implement within the next 12 months
- Implementing/implemented + Expanding/ upgrading implementation

Base: 1,033 global network path security decision makers who are adopting Container Security
Source: Forrester Analytics Global Business Technographics Security Survey, 2019
10 Steps To Secure Containers In Software Delivery Life Cycle

Source: “Ten Basic Steps To Secure Software Containers” Forrester report
Recommendations For Trustworthy IoT

- Embrace open source and modern deployment methodologies
- Shift left and scan often
- Engage development in the security process
Thank You.

Sandy Carielli

Principal Analyst

+1 617.613.6324
scarielli@forrester.com