Extending DevSecOps Security Controls into the Cloud: A SANS Survey
Today’s Speaker

• Eric Johnson
  – Senior SANS instructor and co-author of SANS courses SEC540, 510, and 584
  – Principal Security Engineer, Puma Security
Attend the Panel Discussion

Extending DevSecOps Security Controls into the Cloud: A Panel Discussion of the 2020 SANS Survey

Wednesday, November 4, 2020
1 PM Eastern Time

https://www.sans.org/webcasts/114630
Today’s Agenda

1. Cloud & DevSecOps Landscape
2. Shift Left Analysis
3. Shift Right Analysis
4. Moving Forward
1. Cloud & DevOps Landscape
Increasing Velocity

Year-over-year comparison of how often changes are deployed to production systems:

- 74% of organizations are delivering changes to production more than once per month.
- 14% increase in velocity during the past 4 years

<table>
<thead>
<tr>
<th>Frequency of Delivery to Production</th>
<th>2017</th>
<th>2018</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuously (several times per day)</td>
<td>5.3%</td>
<td>10.0%</td>
<td>11.1%</td>
</tr>
<tr>
<td>Daily</td>
<td>12.0%</td>
<td>7.0%</td>
<td>12.1%</td>
</tr>
<tr>
<td>Weekly</td>
<td>25.4%</td>
<td>24.0%</td>
<td>31.4%</td>
</tr>
<tr>
<td>More than once per month</td>
<td>17.7%</td>
<td>25.0%</td>
<td>19.8%</td>
</tr>
<tr>
<td>Monthly</td>
<td>18.7%</td>
<td>15.0%</td>
<td>11.1%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>13.4%</td>
<td>11.0%</td>
<td>6.3%</td>
</tr>
<tr>
<td>More than once per year</td>
<td>3.8%</td>
<td>4.0%</td>
<td>3.9%</td>
</tr>
<tr>
<td>Annually</td>
<td>1.9%</td>
<td>1.0%</td>
<td>1.0%</td>
</tr>
<tr>
<td>Other (ad hoc/more than once per year)</td>
<td>1.9%</td>
<td>3.0%</td>
<td>3.9%</td>
</tr>
</tbody>
</table>
Increasing Cloud Adoption

Delivery increases as systems transition to the cloud provider's responsibility model.
Multiple Cloud Providers

Most organizations (92%) use at least one public cloud provider, with slightly more than 60% using three or more public cloud providers. Why?

• Corporate mergers & acquisitions
• Select the best platform/service available
• Avoid cloud vendor lock-in
Increasing Platform Risks

Development programming languages present risk to application security teams:

- JavaScript leaps into the top position as cloud & microservice adoption increases.
- Java, .NET, C++ continue to remain high-risk due to legacy usage.
27% of organizations do not perform security assessments at all.
Security vs. the Cloud

Are security teams shifting right and learning how to harden public cloud?

• Operations
• Monitoring
• Runtime security controls
2. Shift Left Analysis
Top 5 Shift Left Controls

- Risk Assessments & Threat Modeling
- Developer Security Training
- Manual Code Review
- Security Stories
- Dependency/Supply Chain Analysis
Continuous Integration Tools

Organizations are shifting to cloud native & cloud hosted Continuous Integration (CI) solutions:

<table>
<thead>
<tr>
<th>Continuous Integration Tools</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises open source (e.g., Jenkins)</td>
<td>56.3%</td>
</tr>
<tr>
<td>Cloud native (e.g., AWS CodePipeline, Microsoft Azure DevOps)</td>
<td>53.8%</td>
</tr>
<tr>
<td>Cloud hosted (e.g., GitHub Actions, GitLab CI)</td>
<td>49.2%</td>
</tr>
<tr>
<td>On-premises commercial</td>
<td>35.0%</td>
</tr>
<tr>
<td>Other</td>
<td>4.6%</td>
</tr>
</tbody>
</table>
Container Orchestration Tools

- Organizations are avoiding the complexity and overhead involved with installing, managing and hardening Docker and Kubernetes services.

Which container orchestration tools are managing your production workloads?
Select all that apply. Please skip if you are not using any.

- Cloud-hosted Docker (e.g., EC2, Azure VM, GCE) - 43.4%
- Cloud-hosted Kubernetes (e.g., EC2, Azure VM, GCE) - 42.2%
- Cloud-managed container service (e.g., AWS ECS, AWS Fargate, Azure Container) - 41.6%
- On-premises Docker Engine - 35.3%
- On-premises Kubernetes - 32.4%
- Cloud-managed Kubernetes service (e.g., AWS EKS/Fargate, Azure AKS, Google GKE) - 29.5%
- Open Shift - 13.9%
- Docker Swarm - 10.4%
- Other - 6.9%
Security Testing Phases

• Less than 40% of organizations shift security reviews into upfront requirements & design.
3. Shift Right Analysis
Top 5 Shift Right Controls

- Configuration Security Monitoring
- Vulnerability Scanning
- Container Image Scanning
- Web Application Firewalls (WAF)/Next Gen WAF
- Network Detection & Response/Network Traffic Analysis
Security Testing Responsibility

- Security teams (internal & external) still conduct most testing.
- Security testing cannot scale at the velocity of DevOps.
- Development and cross-functional teams must contribute more.

<table>
<thead>
<tr>
<th>Role</th>
<th>Managing</th>
<th>Conducting</th>
<th>Accepting</th>
<th>Corrective Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business unit owner</td>
<td>39.3%</td>
<td>12.6%</td>
<td>52.6%</td>
<td>26.8%</td>
</tr>
<tr>
<td>Commercial application vendors</td>
<td>17.4%</td>
<td>23.4%</td>
<td>19.4%</td>
<td>33.3%</td>
</tr>
<tr>
<td>Cross-functional teams in DevOps or DevSecOps</td>
<td>28.8%</td>
<td>38.1%</td>
<td>29.4%</td>
<td>39.2%</td>
</tr>
<tr>
<td>Development team</td>
<td>28.8%</td>
<td>38.1%</td>
<td>36.8%</td>
<td>63.3%</td>
</tr>
<tr>
<td>External security consultants</td>
<td>8.5%</td>
<td>42.8%</td>
<td>13.2%</td>
<td>9.2%</td>
</tr>
<tr>
<td>Internal security team</td>
<td>50.1%</td>
<td>65.4%</td>
<td>34.1%</td>
<td>22.6%</td>
</tr>
<tr>
<td>Quality assurance</td>
<td>17.9%</td>
<td>33.4%</td>
<td>28.8%</td>
<td>18.1%</td>
</tr>
<tr>
<td>Security architect</td>
<td>42.1%</td>
<td>38.8%</td>
<td>28.8%</td>
<td>24.1%</td>
</tr>
</tbody>
</table>
Top DevSecOps Key Performance Indicators:

- Time-to-fix
- Security issues found after deployment
- Time-to-detect

What are the major KPIs you use to measure the success of your DevSecOps activities? Select all that apply.

- Time-to-fix security issues: 64.2%
- Number of security issues discovered after deployment: 51.5%
- Time-to-detect security issues: 47.0%
- Human hours spent resolving security issues: 35.8%
- Post-audit remediation steps required: 35.1%
- Builds delayed due to security issues: 29.1%
- Builds failed due to security issues: 24.6%
- Other: 3.7%
Mean Time To Recover (MTTR)

- Less than half of organizations are repairing critical vulnerabilities satisfactorily and in a timely manner.
4. Moving Forward
Organizational Challenges

Major challenges are fundamentally organizational:

- Insufficient budget
- Shortage of security skills and security training
- Organizational silos
- Lack of buy-in from management and development teams
Top Success Factors

- Securing buy-in from managers and developers
- Improving communications across disciplines
- Moving into the cloud can help organizations become more agile and secure.
Conclusions

Shift right in order to improve success shifting left:

Automation & Tooling
Create a control plane for enforcing security and compliance.

Help security and compliance move at the speed of DevOps.

Test Coverage
Collect attack data to identify real risks that need to be defended.

Understand gaps in testing and controls, and shift left to improve process design and tooling.

Cloud Platforms

Production Weaknesses
Q&A

Please use GoToWebinar’s Questions tool to submit questions to our panel.

Send to “Organizers” and tell us if it’s for a specific panelist.
Acknowledgments

Thanks to our sponsors:

And to our attendees, thank you for joining us today!