AGENDA

1. DevOps & User Experience

2. Deployment for DevOps

3. Securing New Attack Vectors

4. Deployment with Common Tools

5. Q & A

SAM CORONADO

Security Engineer

From infrastructure to policy, I support security system and service health. Before coming to Armor, I gained experience with web development and DevOps engineering.

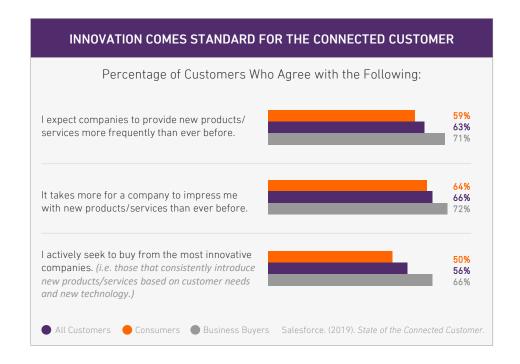Contact me at:
sam.coronado@armor.com

DEVOPS & USER EXPERIENCE

DEVOPS & UX

- Users expect rapid feature delivery

- Users expect maximum uptime

- Speed of software delivery is a competitive advantage

EXCEL OR DIE.

— DORA. (2019). *Accelerate State of DevOps 2019.*

INNOVATION COMES STANDARD FOR THE CONNECTED CUSTOMER

Percentage of Customers Who Agree with the Following:

I expect companies to provide new products/services more frequently than ever before.
- 59%
- 63%
- 71%

It takes more for a company to impress me with new products/services than ever before.
- 64%
- 66%
- 72%

I actively seek to buy from the most innovative companies. *(i.e. those that consistently introduce new products/services based on customer needs and new technology.)*
- 50%
- 56%
- 66%

● All Customers ● Consumers ● Business Buyers   Salesforce. (2019). *State of the Connected Customer.*

DEPLOYMENT FOR DEVOPS

DEPLOYMENT FOR DEVOPS

- Deployment Automation is a critical function of elite DevOps teams

- Infrastructure–as–Code is key to repeatable infrastructure

- Software that requires minimal effort to securely install and configure can help your deployment velocity

AUTOMATION & INTEGRATION BY PERFORMANCE PROFILE				
	LOW	MEDIUM	HIGH	ELITE
Automated Build	64%	81%	91%	92%
Automated Unit Tests	57%	66%	84%	87%
Automated Acceptance Tests	28%	38%	48%	58%
Automated Performance Tests	18%	23%	18%	28%
Automated Security Tests	15%	28%	25%	31%
Automated Provisioning and Deployment to Testing Environments	39%	54%	68%	72%
Automated Deployment to Production	17%	38%	60%	69%
Integration with Chatbots / Slack	29%	33%	24%	69%
Integration with Production Monitoring and Observability Tools	13%	23%	41%	57%
None of the above	9%	14%	5%	4%

DORA. (2019). *Accelerate State of DevOps 2019.*

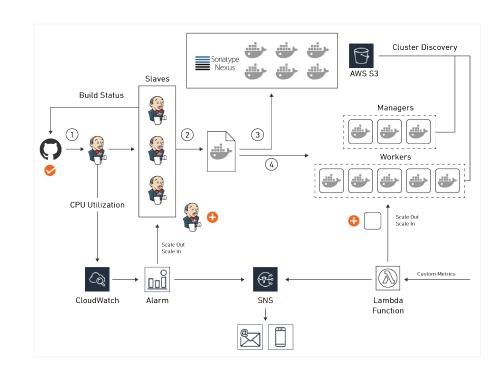SECURING NEW ATTACK VECTORS

ARMOR | SECURECON 2019 | DALLAS, TEXAS

SECURING NEW ATTACK VECTORS

- With explosion of automation and CI/CD tools, attack vector area increases

- DevOps software and system operators are vulnerabilities too

- Attacks targeting common DevOps tools on the rise
  - XMRig/Monero JenkinsMiner attacks – $3 million mined*
  - CoinMiner campaigns creating malicious DockerHub images**

- DevOps infrastructure can be the least protected but most connected in a given environment

ARMOR RECOMMENDATIONS

- **Use Armor Anywhere to protect and monitor infrastructure running your tooling**
  - Protect servers and containers from malware
  - Defense-in-depth for images that host malware
  - Vulnerability scanning, file integrity monitoring, log management, and intrusion detection on servers

- **Automate deployment of Armor Anywhere with common tools**

- **Use Armor Automated Security & Compliance – Prisma to automate monitoring cloud configurations**
  - Misconfigurations are one of the most common ways data gets leaked or attackers gain access in the cloud – enforce visibility and protection by default

DEPLOYMENT WITH COMMON TOOLS

DEPLOYMENT WITH COMMON TOOLS DEMO

TERRAFORM

AWS CLOUD FORMATION

TAKEAWAYS

1 Devops capabilities are a competitive advantange.

2 Automate deployments as much as possible.

3 Use Armor Anywhere and Armor Automated Security & Compliance – Prisma to automate securing some of your most valuable assets.

Q & A

SAM CORONADO

Security Engineer