Book Signing
2:05
Electric Cloud Booth

DevSecOps Handbook (2019)
Shannon Lietz
James Wicket
Ernest Mueller
John Willis
DevOps New Year's Eve 2018
Devops is a set of practices and patterns that turn human capital into high performance organizational capital.
You can’t Lean, Agile, SAFE or Devops your way around a bad organizational culture.
Organizational Discovery
Organizational Discovery at the Edge

Whenever we're talking about any kind of change or improvement you are counting on a bunch of human beings to change and make this happen. If they haven't been part of figuring out how to do it, the change efforts will be dead-on-arrival.
The Seven Disease’s

1. Invisible Work
2. Multiple Management Systems
3. Incomplete Inventory
4. Tribal Knowledge
5. Incongruent Organizational Design
6. Misunderstanding Complexity
7. Security and Compliance Theater
#1
Measuring and Managing Work
(Make Work Visible)
Where Does Work Start?
Dark Debt (Matter)

- Unforeseen interdependencies
- Invisible until revealed by anomalies
- Creeping complexity
- Cannot be seen by looking at pieces
- Specific countermeasures are too narrow

https://medium.com/@allspaw/dark-debt-a508adb848dc
Problems

• What Percentage of Work is Unknown?
• Can Work be Accurately Classified?
• Is There Complete Information?
• Lack of E2E Understanding
• Are there Workarounds and Hidden Work
• Can’t Analyze Bottlenecks (TOC)
• Hard to Create Repeatability (Automation)
The Phoenix Project

I conclude, “So... For the Phoenix task, assuming we have seven handoffs, and that each of those resources is busy ninety percent of the time, the tasks would spend in queue a total of nine hours times the seven steps...”

“What? Sixty-three hours, just in queue time?” Wes says, incredulously. “That’s impossible!”
#2
Multiple Work Management (Reduce Sprawl)
Areas

• **Ticketing Systems**
• Service Catalogs
• CI/CD Systems
• Monitoring
Problems (Ticketing Systems)

- How Many Ticketing Systems?
- Hard to Manage Work (Visibility)
- Inconsistent Messaging
- Non Existant Correlation
- Low Accurately
- Perpetuates Toil
- Motivates Workarounds
## Countermeasures

<table>
<thead>
<tr>
<th>Countermeasure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off-the-Shelf Replication</td>
<td>Replicate entities across tools using off-the-shelf products such as Tasktop.</td>
</tr>
<tr>
<td>Consolidation, Replication, and Strangulation</td>
<td>Choose a foundational system to replicate and consolidate work items to and strangle off non-strategic options.</td>
</tr>
<tr>
<td>Migrate</td>
<td>Wholesale migration of one or many work items to desired target, may include eventual depreciation of original source system.</td>
</tr>
</tbody>
</table>

Requires Development Based Methodology
#3
Inconsistent Inventory
(Services Alignment, Cadence, Coordination, and Relevance)
CMDB Relevance

- As a legacy modeling model
- Adhoc and post discovery models
- Accuracy and subjective models
- Does the organization even trust the model
- Not Cloud Native “aware”
Service Catalog

- Microservices
- Delivery Mesh
- Service Levels Objectives (SRE)
- Service Mesh “aware”
Service Mesh Integration

- ISTO and ENVOY
- Service Mesh Orchestration (Supermesh)
- SPIFFE (Secure Production Identity Framework For Everyone)
- Custom Resources (CRD’s)
Delivery Mesh Integration

- Configuration Management
- Deployment Orchestration
- Notary/TUF
- Open Policy Agent (OPA)
- API Documentation (Swagger)
- Event Driven Software
Institutional vs Tribal Knowledge (Theory of Constraints)
Five Focusing Steps (TOC)

• Identify the constraint
• Exploit the constraint
• Subordinate all other activities to the constraint
• Elevate the constraint to new levels
• Find the next constraint
#5
Incongruent Organizational Design
Problems

- Functional Oriented
- Silo’d Teams
- “I” vs “T” vs “E” Shaped
- Motivation/Apathy
Conway’s Law

An adage named after computer programmer Melvin Conway, who introduced the idea in 1967. It states that, "organizations which design systems ... are constrained to produce designs which are copies of the communication structures of these organizations."
The Equifax Data Breach
Majority Staff Report
115th Congress
December 2018

Richard Smith
Chief Executive Officer

David Webb
Chief Information Officer

John Kelley
Chief Legal Officer

Graeme Payne
SVP & CIO for Global Corporate Platforms

Susan Mauldin
Chief Security Officer
Webb asked Mauldin whether she would support moving the CSO back under the CIO.\textsuperscript{362} Webb testified:

A. I actually did have a conversation one time with Susan Mauldin about whether she thought it was a better option.

Q. And what was her response?

A. I think she was comfortable with where it was.\textsuperscript{363}

Mauldin testified about her knowledge of the origin of the particular organizational structure. She stated:

[T]hat structure was in place . . . at the time I arrived at Equifax. It was the structure that was there with the person that was my predecessor. And I knew that it was that structure going in. I didn’t question it. I was okay with it. And so it was just what was there, and so it continued with what it had been.\textsuperscript{364}
Based on information confirmed on July 31 by the lead forensic analyst, Mauldin stated “I felt like I knew at that point that PII had been involved in this incident.” She reported this to John Kelley on July 31, but did not inform David Webb. Mauldin testified:

Q. Is there any particular reason why you did not report to the CIO your belief that PII may have been exfiltrated in connection with the security incident we have been discussing?

A. I don’t remember a particular reason about that . . . . I just don’t remember thinking about that.
ORGANIZATIONAL ARCHETYPES

• Functional-Oriented
  • Optimize for expertise, division of labor, or reducing cost

• Matrix-Oriented
  • Combine functional and market orientation

• Market-Oriented
  • Optimize for responding quickly to customer needs

Dr. Roberto Fernandez
The Service Owner is the single Transformational Leader accountable for the: end to end construction, operation, SLAs, customer experience and stewardship of business value for a product or set of services.
#6
Managing Complexity
(Understanding Complex Systems)
Problems

• Blame Culture
• Root Cause Thinking
• Physiological Un-Safety
• Pluralistic Ignorance
• Normalization of Deviance
• Dark Debt
• Goldratt
• Deming
• Lean
• Safety Culture
• Learning Organizations
HOW ORGANISATIONS PROCESS INFORMATION

Pathological
- Power-oriented
- Cooperation low
- Messengers shot
- Responsibilities avoided
- Bridging discouraged
- Failure → scapegoating
- Novelty crushed

Bureaucratic
- Rule-oriented
- Cooperation modest
- Messengers neglected
- Responsibilities narrow
- Bridging tolerated
- Failure → justice
- Novelty → problems

Generative
- Performance-oriented
- Cooperation high
- Messengers trained
- Shared risks
- Bridging encouraged
- Failure → inquiry
- Novelty enacted

Diagram adapted from A Typology of Organisational Cultures (Westrum, R.) (2004)
#7
Security & Compliance
DevSecOps
(Shift Left Auditors)
Problems (Shift Left Auditors)

- Review Boards (ARB, PRB, CAB)
- Check Box Compliance
- Workarounds and Hidden Work
- Auditor Workarounds
- Vulnerability Theater
- Negative RIO
- Policy Theater
DevSecOps

Requirements & Design
- Application Risk Classification
- Security Requirement Definition
- Threat modeling

Development
- Static Analysis/IDE
- Secure Libraries
- Secure Coding Standards

CI
- Static Analysis (CI)
- Open Source Governance (CI)
- Container Security Compliance (CI)

Interval Trigger Assessment
- Dynamic Assessments
- Threat-Based Pen Test

Production
- Perimeter Assessment
- Web Application Firewalls
- Automated Attack/Bot Defense
- Container Security Management

Security Mavens (Security-Trained Developers and Operations)

Role Based Software Security Training

Continuous Monitoring, Analytics and KPI Gathering
Automated Governance

- Move From Subjective Compliance to Objective
- Automated Attestation in CI/CD
- Grafeas (Google)
DevSecOps Operational Tips

• Work with and educate your auditors
• Move Subjective Attestation to Objective Attestation
• Ruthlessly eliminate false positives to Developers
• Explain the vulnerabilities in business impact terms
• Devops the vulnerability (JIRA, backlog, Kanban)
• Open the code base to everyone in the organization
• Educate on how to fix
Summary

1. Invisible Work - **Capture All Work “Visible”**
2. Management System Toil - **Consolidate Work Management Systems**
3. Incomplete Inventory - **Coordinate Legacy With Cloud Native**
4. Tribal Knowledge - **Remove Bottlenecks and Institutionalize Knowledge**
5. Incongruent Organizational Design - **Inverse Conway Maneuver**
6. Managing Complexity - **Blameless Culture with Engineering Mindsets**
7. Security and Compliance Theater - **Automate Your Governance**
Bonus
Container Notes

- CIS Docker Benchmark
- Minimize bind mounts
- Set USER in Dockerfile
- Avoid --privileged
- SECOMP
- AppArmor
- SeLinux
- CNCF Projects
  - TUF
  - notary
- Restrict syscalls and file access
- Default Docker profiles are good
- But aren’t automatically applied in Kubernetes
Kubernetes Notes

CIS Kubernetes Benchmark

- TLS
- Audit Logs
- Network Policies
- Pod Security Policies
- Secrets

**TLS Checklist:**
1. Nodes and Master
2. User and Master
3. Everything etcd
4. Kubelet to API Server

SECOMP
AppArmor
SeLinux

clair
kube-bench
Moving Target Defense
Knowing Adversities and Motivations

- Scanners
- Researchers
- Paid Noise
- Advanced Adversaries
- Information Brokerage
- Fame / Payment
- Continuous Payment
- Control / Payment

Shannon Lietz
Director, DevSecOps
Intuit
@devsecops
Knowing Adversities and Motivations

Adversary Return Rate
Kill Chain Workshop
• nmap - Used to scan ports
• skipfish - Webscan tool to crawl links
• metasploit - Uses well known exploits to execute vulnerabilities
10 Years of Exponential Growth in OSS Demand

Download Requests for Java Components 2008-2017 are a proxy for the popularity of automated software development.

Source: Sonatype
The Cost

• Heartland Payment Systems 2008 - $145 million
• The Target Breach in 2013 - $162 Million
• The Home Depot Breach in 2014 - $19.5 million
• OPM Breach 2015 - $133 million
• The Anthem Breach in 2016 - $100 million
• The Equifax Breach in 2017 - $4 Billion

IBM report 2018 has the average cost of a breach in the US at 7.9 million
“On average, each record costs $148 and a breach of 1 million records costs $40 million
while a breach of 50 million costs $350 million”
Actual Exploitation 2015 VZ DBIR

NOT ALL CVES ARE CREATED EQUAL.

If we look at the frequency of exploitation in Figure 11, we see a much different picture than what’s shown by the raw vulnerability count of Figure 12. Ten CVEs account for almost 97% of the exploits observed in 2014. While that’s a pretty amazing statistic, don’t be lulled into thinking you’ve found an easy way out of the vulnerability remediation rodeo. Prioritization will definitely help from a risk-cutting perspective, but beyond the top 10 are 7 million other exploited vulnerabilities that may need to be ridden down. And therein, of course, lies the challenge; once the “mega-vulns” are roped in (assuming you could identify them ahead of time), how do you approach addressing the rest of the horde in an orderly, comprehensive, and continuous manner over time?

About half of the CVEs exploited in 2014 went from publish to pwn in less than a month.

Figure 11.
Cumulative percentage of exploited vulnerabilities by top 10 CVEs
DevSecOps as Supply Chain?

Source: Wikipedia - Continuous Delivery
Solutions

- System-wide coach for:
  - follow-up
  - graphical story teller
- Lean coffees
- Slack (chatbot)
- Internal Devopsdays
- Hackathons
- Dojo