BUILDING SYSTEMS ON SHAKY GROUNDS
10 TACTICS TO MANAGE THE MODERN SUPPLY CHAIN
DevOps Lifecycle

Supply chain

Why value?

Alignment to mission

Product is live
DevOps Lifecycle

https://robert-wood.com
@HolyCyberBatman

Supply chain

Why value?

Alignment to mission
DevOps Lifecycle

- Supply chain
- Why value?
- Alignment to mission

Product is live
DevOps Lifecycle

Gather requirements → Product is live

Supply chain

Why value?

Alignment to mission
DevOps Lifecycle

- Gather requirements
- Design
- Product is live

Supply chain
Why value?
Alignment to mission
DevOps Lifecycle

- Gather requirements
- Code
- Design
- Test
- Product is live

Supply chain

Why value?

Alignment to mission
DevOps Lifecycle

- Gather requirements
- Design
- Code
- Test
- Accept
- Push to production
- Product is live

Supply chain
Why value?
Alignment to mission
DevOps Lifecycle

- Gather requirements
- Code
- Accept
- Design
- Test
- Push to production
- Product is live

Supply chain
Why value?
Alignment to mission
Supply chain

"The supply chain is a system of organizations, people, activities, information, and resources involved in providing value to stakeholders."
Why value?

Value is what the customer ultimately wants.
Why value?

Value is what the customer ultimately wants.

They don't care about your product. They care about "me."
Mission

“To give everyone the power to create and share ideas and information instantly, without barriers.”
Mission

Focus beyond the product.

Focus on the way the customer receives value.

Align security with the organization's mission leads to a greater sense of partnership.
BUILDING SYSTEMS ON SHAKY GROUNDS
10 TACTICS TO MANAGE THE MODERN SUPPLY CHAIN
Supply chain risk management
Inside the DevOps lifecycle
Software composition analysis

Different flavors

GitLab

node.js

Python

php
Software composition analysis
Dependency graph for **dschadow/ApplicationIntrusionDetection**.
Colored areas are **ognl ognl 3.0.8** or transitive dependencies to **ognl ognl 3.0.8**.
Different flavors

Checking immediate dependencies for CVEs
Different flavors

Checking direct + transitive dependencies for CVEs and non-CVEs
Checking immediate dependencies for CVEs
Different flavors

- Checking whether or not your code actually calls the vulnerable code
- Checking direct + transitive dependencies for CVEs and non-CVEs
- Checking immediate dependencies for CVEs
Different flavors

- Checking whether or not your code actually calls the vulnerable code
- Checking direct + transitive dependencies for CVEs and non-CVEs
- Checking immediate dependencies for CVEs
Different flavors

- Checking whether or not your code actually calls the vulnerable code
- Checking direct + transitive dependencies for CVEs and non-CVEs
- Checking immediate dependencies for CVEs
Code analysis

Linting | Lightweight, heavily customized, CI friendly

Considerations
Code analysis

<table>
<thead>
<tr>
<th>Linting</th>
<th>Lightweight, heavily customized, CI friendly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static analysis</td>
<td>Control flow and taint flow analysis, slower, requires heavy tuning</td>
</tr>
</tbody>
</table>
# Code analysis

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linting</td>
<td>Lightweight, heavily customized, CI friendly</td>
</tr>
<tr>
<td>Static analysis</td>
<td>Control flow and taint flow analysis, slower, requires heavy tuning</td>
</tr>
<tr>
<td>Binary analysis</td>
<td>Full service review, out-of-hand but can serve as a CI gate</td>
</tr>
</tbody>
</table>
Considerations

Consider the constraints:
- Time to tune vs useful results
- Deadlines
- $$$
- Tech stack support
- CI integration
- Deployment model
Threat modeling

Design-focused security review of the software's architecture.
Threat modeling

Design-focused security review of the software's architecture.
Empower the developers
Empower the developers

- Does this change affect any of the sensitive data in our service?
- Does this change introduce a new way to access the system?
- Does this change impact any existing security controls?
- Does this change have the possibility of affecting our users?
- What's the worst thing that could happen?
CI tooling

Build tools are the new AD

Take care of

Malicious builds
CI tooling

Build tools are the new AD

- Permissions to/from
- Patching
- Credential handling
- Pivot potential

Take care of

Malicious builds
Take care of

- Minimize who/what can make changes in the CI environment
- Limit the permissions of the CI workers
- Make sure you have a patching plan
Malicious builds

CI can be used as a channel to backdoor products and the build server itself
Malicious builds

CI can be used as a channel to backdoor products and the build server itself

Analyze what you build and that it operates as expected
Malicious builds

CI can be used as a channel to backdoor products and the build server itself.

Analyze what you build and that it operates as expected.

https://github.com/srcclr/build-inspector
Red teaming

Asynchronous adversarial analysis of environment and business

Typically tries to look at risk from a systems-perspective
Tactics

Table top exercises

Out-of-band full-scope analysis
Tactics

- Table top exercises
- Out-of-band full-scope analysis
- Enumeration of organization/department wide canonical risks
Considerations

- Stakeholders need to be primed and bought in
- Full scope removes your bias and lets your red team be creative
- Think through what you do if something happens
- How do you want to handle the results?
BUILDING SYSTEMS ON SHAKY GROUNDS
10 TACTICS TO MANAGE THE MODERN SUPPLY CHAIN
Supply chain risk management

Looking beyond the SDLC
Marketing

- What tools are being used to and how are they controlled?
- What data is being collected and used?
- Who has access to marketing data/tools?
- Where are all the places marketing tools are integrated?
Marketing

- What tools are being used to and how are they controlled?
- What data is being collected and used?
- Who has access to marketing data/tools?
- Where are all the places marketing tools are integrated?

If you got a GDPR request to be forgotten, would you be comfortable only working with engineering?
What to do about it

Risk rank your marketing function:
- IAM for tools
- Monitor/control data usage
- Consider threat model for integrations
What to do about it

Risk rank your marketing function:
- IAM for tools
- Monitor/control data usage
- Consider threat model for integrations

**Most important**
Start a conversation and engage the team about their goals
Sales

Sales teams set the tone and expectations with a customer

- What tools are they using?
- What data are they using?
- What commitments are they making and why?
- How might those commitments land you in hot water?
Security in contracting

Legal language is important when things really hit the fan.

Your customers

Your suppliers
Security in contracting

Legal language is important when things really hit the fan.

Focus on:
- Language with your customers - data use, commitments, etc.
- Your vendors and their commitments
When it's your customers

Push for less strict commitments in writing that can be used against you.
When it's your customers

Push for less strict commitments in writing that can be used against you.

- Security audits or assessments to be performed no more than annually at customer’s expense
- Notification of **confirmed** security breaches to occur within <X> days
- Customer
- Patches and vulnerabilities will be addressed in a timeline that is commensurate with business risk
When you're the customer

Try to get things in writing so that you have a mechanism for accountability.
When you're the customer

Try to get things in writing so that you have a mechanism for accountability.

- Notification of data breaches to occur within 24 hours
- External penetration tests to be conducted on vendor services and vulnerabilities identified from those tests, remediated
- Vendor to assess its own suppliers for possible risks
- Service level agreement in place
- Timely notification of significant changes to service levels, security program, or service architecture
- Provider will address vulnerabilities in a timely manner to minimize risk
- Provider will adhere to your security policies as provided
Vendor risk assessments

Vendors can be categorized and assessed by risk:
• What do they manage?
• How essential are they to your business/value prop?
• What happens if they go away tomorrow?
Tracking down vendors

- Talk to people across teams
- CASB
- VPN/firewall logs
- Finance team - follow the $$$
# Tracking down vendors

- Talk to people across teams
- CASB
- VPN/firewall logs
- Finance team - follow the $$$

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Name</td>
<td>Owner</td>
<td>SSO Integrated</td>
<td>Annual Cost</td>
<td>Last Vendor Assessment</td>
<td>Level of Reliance</td>
<td>Risk Score</td>
</tr>
</tbody>
</table>
Assessment tools

There are plenty of online resources; don't reinvent the wheel:

- Vendor security alliance
- Cloud Security Alliance CAIQ
- Google VSAQ project
- Commercial solutions
- Third party certified SOC-2 or ISO reports
Incident response

IR has the potential to influence brand, consumer confidence, bottom line, and much more.
Incident response

IR has the potential to influence brand, consumer confidence, bottom line, and much more.

Have a plan, test it, improve it. Be sure to include customer notifications, PR, and legal.
BUILDING SYSTEMS ON SHAKY GROUNDS
10 TACTICS TO MANAGE THE MODERN SUPPLY CHAIN
Wrapping up

Security teams don't have the luxury of focusing on narrowly scoped problems

Align yourself with others by focusing on all the ways that your organization produces value
Priorities

Figuring out what to do is just as important as figuring out what not to do and sticking to it
Priorities

Figuring out what to do is just as important as figuring out what not to do and sticking to it

It depends on your specific context
Priorities

Figuring out what to do is just as important as figuring out what not to do and sticking to it

**It depends on your specific context**

- Focus on one thing at a time
- Really operationalize each thing before moving on to the next
We're hiring!

Veracode is continuing to build its research team out. Interested? Let's chat!
We're hiring!

Veracode is continuing to build its research team out. Interested? Let's chat!

https://searchjobs.ca.com/job/Burlington-Principal-Security-Researcher-MA-01803/483404200/

Thank you!

https://veracode.com
@veracode

https://robert-wood.com
@HolyCyberBatman
BUILDING SYSTEMS ON SHAKY GROUNDS
10 TACTICS TO MANAGE THE MODERN SUPPLY CHAIN