Tackling security in the world of containers, cloud, and DevSecOps

Lucy Kerner
Director, Security Global Strategy and Evangelism
Red Hat
2021 Security Symposium Welcome

- Sessions are pre-recorded
- Please drop your Questions in the Q&A as we go along - Red Hatters will be available to answer your questions.
- Use the chat box to talk to each other and us!
- GOOGLE CHROME is the best browser for this experience
- The sessions will be on demand approximately 24 hours following the event, at the same link.
The Agenda:

11:00 a.m. - 11:45 a.m. CEST
**Tackling security in the world of containers, hybrid cloud, and DevSecOps**
Speaker: Lucy Kerner, Director, Security Global Strategy and Evangelism, Red Hat

11:45 a.m. - 12:30 p.m. CEST
**Discussing security challenges in a cloud-native world with BP and AT&T**
Panelists:
- Paul Costall, Head of Application Engineering Services, BP
- Rupesh Chokshi, Vice President, AT&T Cybersecurity +
Hosted by:
Lucy Kerner, Director, Security Global Strategy and Evangelism Director, Red Hat
Dave Sirrine, Principal Solution Architect, Red Hat

12:30 p.m. - 1:00 p.m. CEST
**Implementing a secure hybrid cloud using security and compliance automation**
Lucy Kerner, Director, Security Global Strategy and Evangelism Director, Red Hat
The Agenda Continued:

1:00 p.m. - 1:30 p.m. CEST
Data security in hybrid cloud
Speakers: Mark Thacker, Product Manager, Red Hat + Uday Boppana, Sr. Product Manager, Red Hat

1:30 p.m. - 2:00 p.m. CEST
Securing containers and Kubernetes in hybrid cloud
Speakers: Kirsten Newcomer, Director, Cloud and DevSecOps Strategy, Red Hat + Wei Dang, Sr. Director Product Management, Red Hat

2:00 p.m. - 2:30 p.m. CEST
Demystifying DevSecOps practices and tooling in container environments

2:30 p.m. - 3:00 p.m. CEST
Deep Dive Demo: Protecting cloud-native applications with Red Hat Advanced Cluster Security for Kubernetes
Speakers: Chris Porter, Director of Solutions Architecture, Red Hat

3:00 p.m. - 3:30 p.m. CEST
Maintaining compliance and governance in hybrid cloud
Speakers: Jason Burrell, OpenShift Security Lead, Red Hat + Umoja Thomas, Compliance Manager, Red Hat

#securitysymposium
Want more content?

red.ht/SecurityinfoEMEA

Security Workshops - Get hands on

red.ht/securityworkshops

Don’t miss Red Hat at Black Hat USA

red.ht/blackhat2021
Security Symposium

Tackling security in the world of containers, cloud, and DevSecOps

Lucy Kerner
Director, Security Global Strategy and Evangelism
Red Hat
What are some common causes of these security breaches?
“Through 2025, 99% of cloud security failures will be the [cloud] customer’s fault”

1 Gartner: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
Developers aren’t security experts but have more and more power over the application lifecycle

“The softest target in most organizations is the app layer and attackers know this…”¹

“Attackers try to find the path of least resistance… Currently, the application security vector of attack allows for efficient attacks with minimal costs…”²

Security is a **process**, **NOT** a product.

---

Bruce Schneier  
Cryptographer, security blogger and author
Security policy, process and procedures

Design

Identify security requirements and governance models

Built-in from the start

Build

Deploy to trusted platforms with enhanced security capabilities

Adapt

Revise, update, remediate as the landscape changes

Manage and automate

Automate systems for security and compliance

Run

Security must be continuous and holistic
Security throughout the stack and life cycle

Tested, certified, stable, and supported open source software
Defense In-Depth across the stack and lifecycle

Build, deploy, and run applications more securely on top of a hybrid cloud using DevSecOps practices.

Security built-into the foundation
Take a layered defense approach to security

People, Processes, and Technology

#1 Data Security
#2 Software supply chain security
#3 Cloud and containers security and management
#4 Maintaining compliance and governance
#5 People and Processes
Data Security
Security across the data life cycle - Hybrid Cloud
Data protection at each layer

- Image scanning, signing, and blueprinting
- Host hardening
- Platform delegation practices
- Applies equally to cloud VMs and Containers
Software Supply Chain Security
The year-long rash of supply chain attacks against open source is getting worse

Backdoors snuck into 12 OSS packages were downloaded hundreds of thousands of times.

DAN GOODIN - 8/21/2019, 7:35 AM

A rash of supply chain attacks hitting open source software over the past year shows few signs of abating, following the discovery this week of two separate backdoors slipped into a dozen libraries downloaded by hundreds of thousands of server administrators.
Tainted, crypto-mining containers pulled from Docker Hub

Security companies Fortinet and Kromtech found seventeen tainted Docker containers that were essentially downloadable images containing programs that had been designed to mine cryptocurrencies. Further investigation found that they had been downloaded 5 million times, suggesting that hackers were able to inject commands into insecure containers to download this code into otherwise healthy web applications. The researchers found the containers on Docker Hub, a repository for user images.
Do you have the resource to manage open source?

Undermanaged open source can have costly impacts

1 in 10
OSS downloads are vulnerable\(^1\)

430% YOY growth
in cyber attacks targeting open source software projects\(^1\)

$25M
the predicted cost of a recent supply chain attack\(^2\)

$2B
the cost of a data breach that resulted from an unpatched bug\(^3\)

Source:
1. State of software supply chain
2. SolarWinds Expects Cyber Incident Costs Up To $25 Million in 2021
3. Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement
Security consideration for open source software

How do you find out about new vulnerabilities in the software you use?
Do you know all of the open source software you use?
How do you assess the security impact to the software you have?
How do you address a fix to the software you use?
Do you have the appropriate expertise in-house to assess and remediate security issues in open source software?
Who do you go to if you need critical and immediate support?
Red Hat’s software supply chain security

Reducing risk and making open source consumable for the enterprise

- Upstream first & community leadership
- Red Hat bugzilla package review
- Track packages for release in Fedora®
- Packages selected for inclusion into Red Hat® Enterprise Linux®
- Security scanning
- Continuous security updates
- Secure distribution
- All packages are digitally signed
- Extensive QE testing per release
- Compiler flags set for hardening and security
Red Hat Universal Base Image (UBI)

Trusted:
- Libraries
- Packaging format
- Core Utilities
- Security Response
- Patching
- Performance Response
- Technical Support
- More
Why Standardize

Standard operating environments improve containers too

- No Standard Operating Environment
  - 8 different versions of glibc
  - 3 different versions of musl
  - 11 different versions of openssl

- Standardized on Universal Base Image 8
  - 1 version of glibc
  - 1 version of openssl
DevSecOps at scale with containers and Kubernetes

Containers make it easier to deliver applications faster

Kubernetes makes it easier to manage containerized applications

Control
Application
Security

Protect
The Platform

Detect & Respond
At Runtime

Build
Package

Design
Adapt

Deploy
Adapt

Run
Manage
| Partners Extend and Enhance Red Hat functionality to Secure the entire DevOps Lifecycle |

<table>
<thead>
<tr>
<th>Vulnerability &amp; Config Mgmt</th>
<th>Identity &amp; Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAST, SCA, IAST, DAST, Config Mgmt, Image Risk</td>
<td>Authn, Authz, Secrets Vault, HSM, Provenance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Network Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory Compliance Audit &amp; Controls</td>
<td>CNI, Policies, Traffic Controls, Service Mesh, Packet Analysis, API, Visualization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Controls</th>
<th>Runtime Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection and Encryption</td>
<td>Admission Control, Behavioral, Threat Defense</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit &amp; Monitoring</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Monitoring, SIEM, Forensics</td>
<td>SOAR, Automatic resolution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Red Hat Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Host, Container Platform, Namespace Isolation, k8s &amp; Container Hardening</td>
</tr>
</tbody>
</table>
Cloud and containers security and management
History of Achieving Secure Operations

Evolving how you tackle security and IT operations at scale

1.0 Multiple Sysadmins per Server
2.0 Multiple Servers per Sysadmin
3.0 Clustered Services & Filesystems
4.0 Services & Monitoring System
5.0 Kubernetes Operators

- Automation
- Culture change
- Continuous delivery
- Advanced deployment techniques
- Self service and auto scaling
- Microservices serverless
- API first
- Cloud native
- AI/ML

DevSecOps at Scale
Maintaining compliance and governance
Security practices, policies, and tools haven’t fully caught up with cloud technologies

“According to analyst firm McKinsey, a full 78 percent of more than 100 firms recently surveyed are NOT reconfiguring their security tools when migrating to the cloud”

Source: B. Cameron Gain for themewstack.io, Microservices Security: Probably Not What You Think It Is, Mar 2018
https://thenewstack.io/microservices-security-probably-not-what-you-think-it-is/
People and Processes
Approaches to people and process challenges

- Formal security education and certification programs
- Security roles in app dev and vice versa
- Establish culture of cross-training and cross-collaboration
- Be strategic with hiring
- Take a hard look at security tooling and resources
- Implement a consistent automation strategy across organization
Key Takeaways
Take a layered defense approach to security

People, Processes, and Technology

#1 Data Security
#2 Software supply chain security
#3 Cloud and containers security and management
#4 Maintaining compliance and governance
#5 People and Processes
Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.