Virtual Training Partner Conference | 7-9 Sept, 2021

Foundations of Cybersecurity– The Impact of Linux & How to Prepare Students for Employment

John Walter, Solutions Architect

AGENDA

- Security in the Hybrid Cloud
- Starting with the operating system
- Secure-default container platform
- Automating compliance
- Q&A

Impacts of ineffective security

Security breaches are costly and threats are growing.

$3.92m

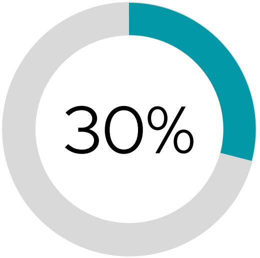
Average cost of a data breach in 2019

$1.22m

Savings in costs if a breach can be identified and contained in **200 days** or less

279 days

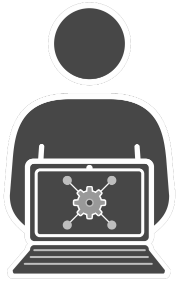
Average time to identify and contain a data breach in 2019



Likelihood of experiencing a breach within two years

Source:

IBM Security, “2019 Cost of a Data Breach Report,” 2019. ibm.com/security/data-breach



Security is a process, not a product

Foundations for a secure hybrid cloud

Operating system

Container platform

Automation tools

Security Consideration - Collaboration

Lines Of Business

Network

Security

Operations

Developers

Infrastructure

CONTAINER CHALLENGES

Container security

Image scanning, patching, and compliance

Day 2 management

Installations, upgrades, and maintenance
Integration of existing enterprise technology

Application delivery

Monitoring, metering, and management
Integration of existing developer tools

Red Hat OpenShift

Trusted enterprise Kubernetes

Continuous security, world-class support and services, and deep expertise to confidently run any application

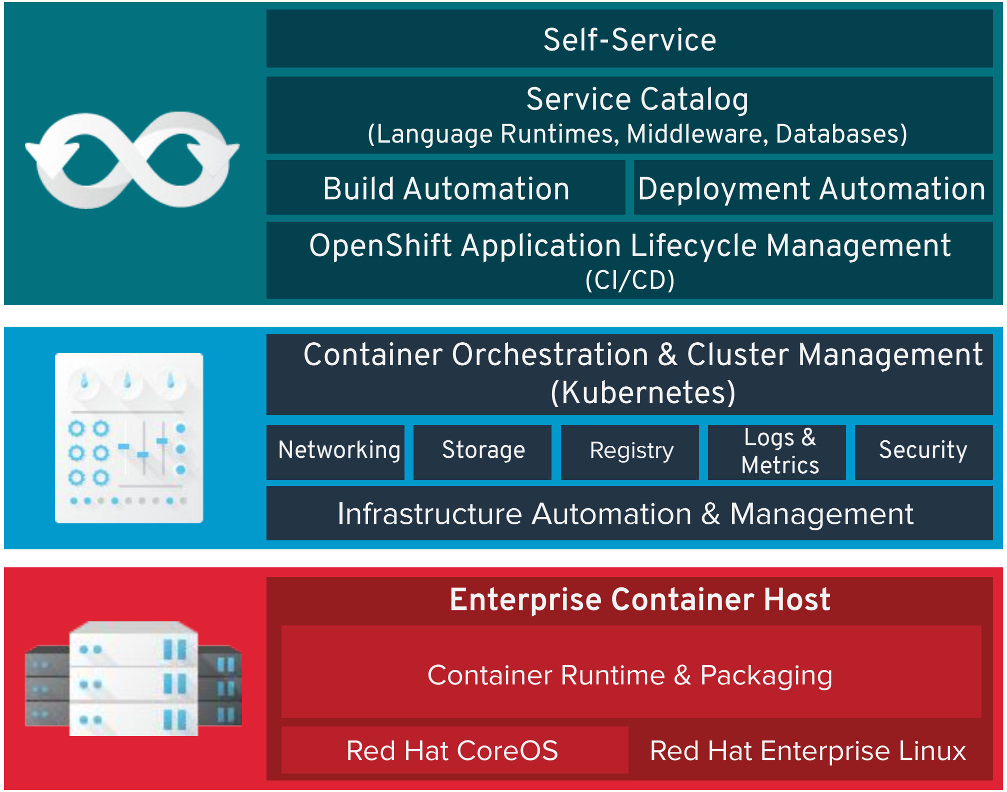
A cloud-like experience, everywhere

Full-stack automated operations on a consistent foundation across on-premises or hybrid cloud infrastructure

Empowerment for developers to innovate

Ability to get applications to production sooner with a wide range of technologies and streamlined workflows

ELEMENTS OF AN ENTERPRISE CONTAINER SOLUTION



Self-Service

Service Catalog
(Language Runtimes, Middleware, Databases)

Build Automation

Deployment Automation

OpenShift Application Lifecycle Management
(CI/CD)

Container Orchestration & Cluster Management
(Kubernetes)

Networking

Storage

Registry

Logs & Metrics

Security

Infrastructure Automation & Management

Enterprise Container Host

Container Runtime & Packaging

Red Hat CoreOS

Red Hat Enterprise Linux

AUTOMATED & INTEGRATED SECURITY

CONTROL
Application security

- Container content
- CI/CD pipeline
- Container registry
- Deployment policies

DEFEND
Infrastructure

- Container platform
- Container host multi-tenancy
- Network isolation
- Storage
- Audit & logging
- API management

EXTEND

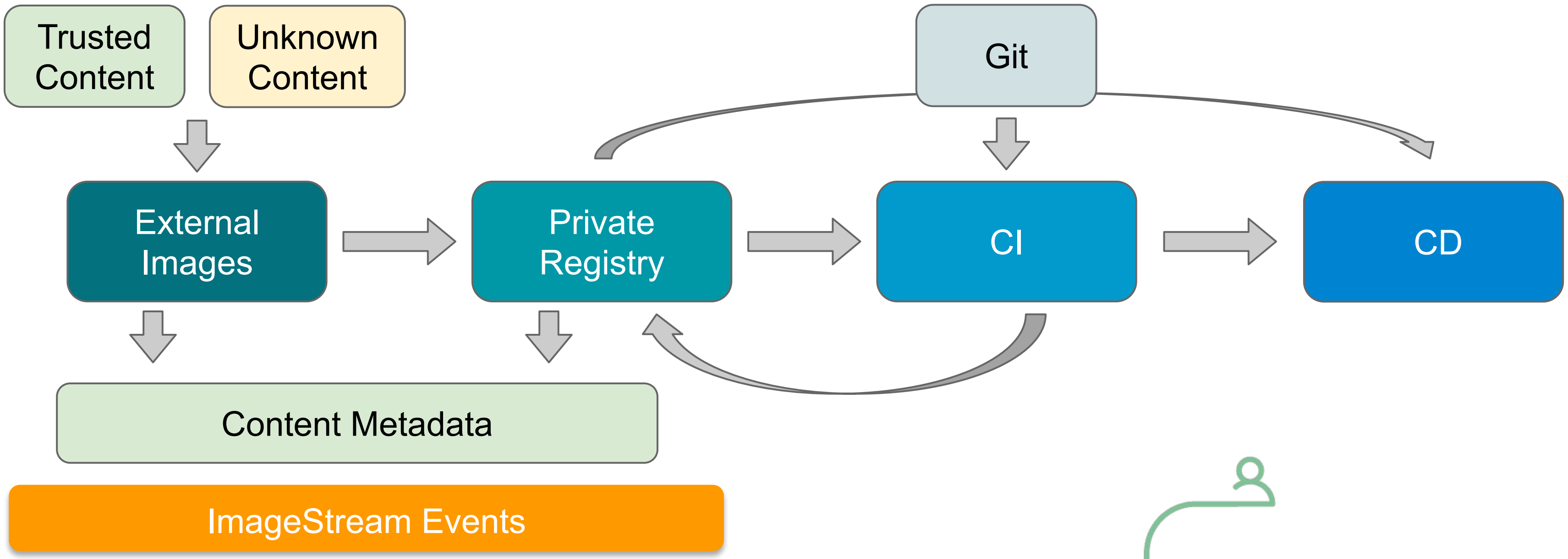
- Security ecosystem

CONTROL

Secure the Pipeline & the Applications

Container Content	CI/CD Pipeline
Container Registry	Deployment Policies

SECURE THE CONTAINER LIFECYCLE



DEFEND

Secure the Infrastructure

- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

CONTAINER HOST & MULTI-TENANCY THE OS MATTERS

Red Hat Enterprise Linux

Red Hat CoreOS

THE FOUNDATION FOR SECURE, SCALABLE CONTAINERS

A stable, reliable host environment with built-in security features that allow you to isolate containers from other containers and from the kernel.

Minimized host environment tuned for running Linux containers while maintaining the built-in security features of Red Hat Enterprise Linux..

SELinux

Kernel namespaces

Capabilities

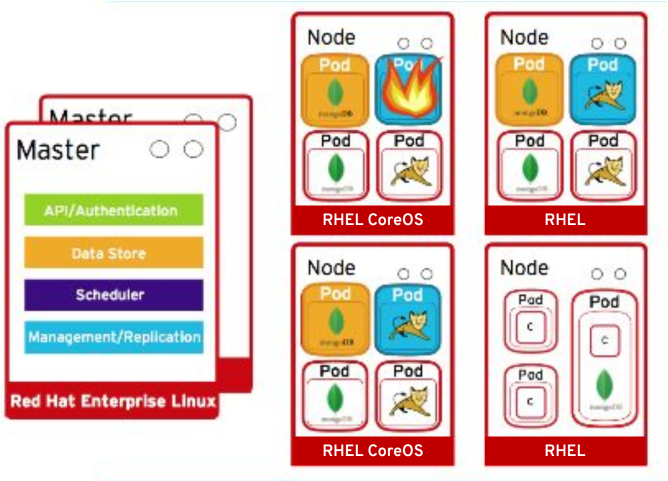
Cgroups

Seccomp

SECURING THE CONTAINER PLATFORM

Use a container orchestration platform with integrated security features including

- Role-based Access Controls with LDAP and OAuth integration
- Secure communication
- Platform multitenant security
- Integrated & extensible secrets management
- Logging, Monitoring, Metrics



EXTEND

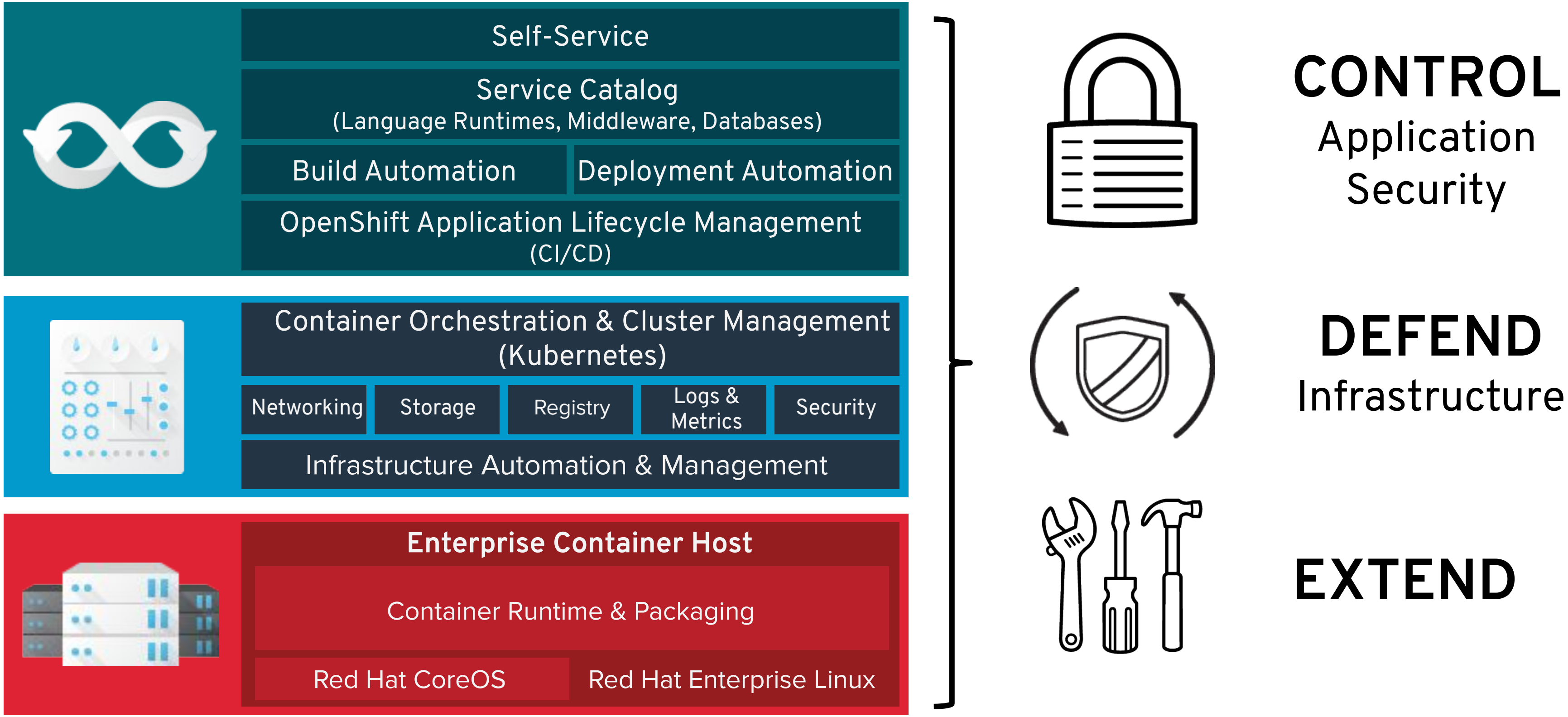
Leverage the Ecosystem

THE SECURITY ECOSYSTEM

For enhanced security, or to meet existing policies, integrate with enterprise security tools, such as

- Identity and Access management / Privileged Access Management
- External Certificate Authorities
- External Vaults / Key Management solutions
- External Hardware Security Modules (HSM)
- Filesystem encryption tools
- Container content scanners & vulnerability management tools
- Container runtime analysis tools
- Security Information and Event Monitoring (SIEM)

BRINGING IT ALL TOGETHER



Self-Service

Service Catalog
(Language Runtimes, Middleware, Databases)

Build Automation | Deployment Automation

OpenShift Application Lifecycle Management
(CI/CD)

Container Orchestration & Cluster Management
(Kubernetes)

Networking | Storage | Registry | Logs & Metrics | Security

Infrastructure Automation & Management

Enterprise Container Host

Container Runtime & Packaging

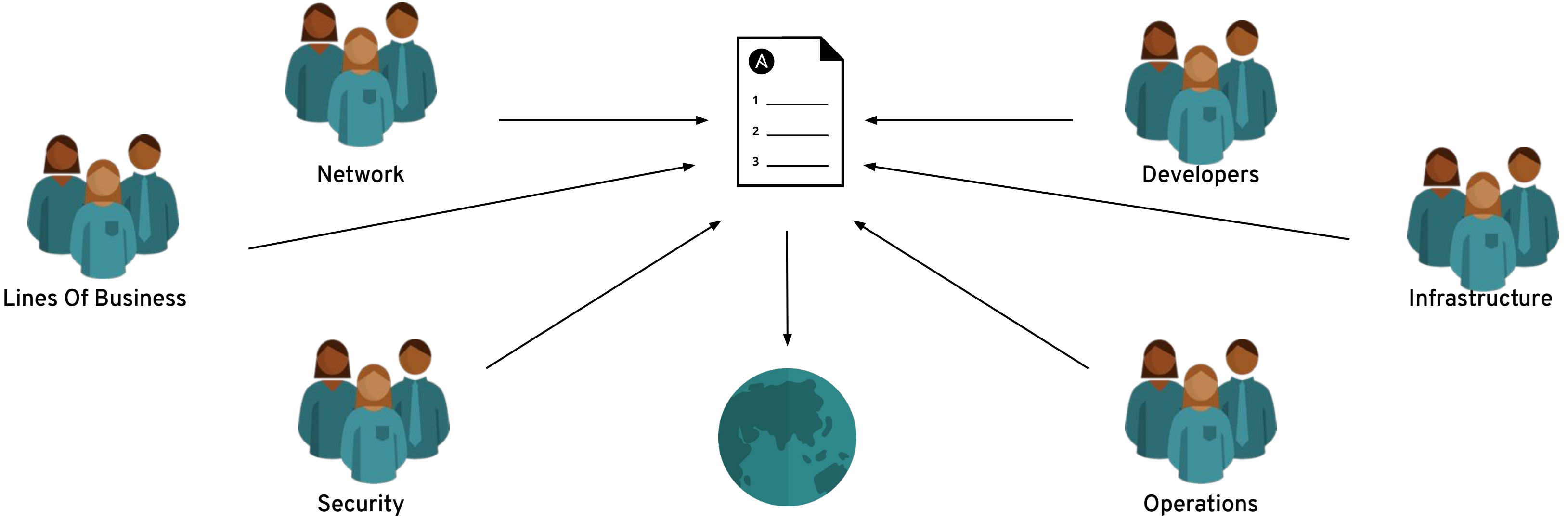
Red Hat CoreOS | Red Hat Enterprise Linux

CONTROL
Application Security

DEFEND
Infrastructure

EXTEND

Automating Security Compliance

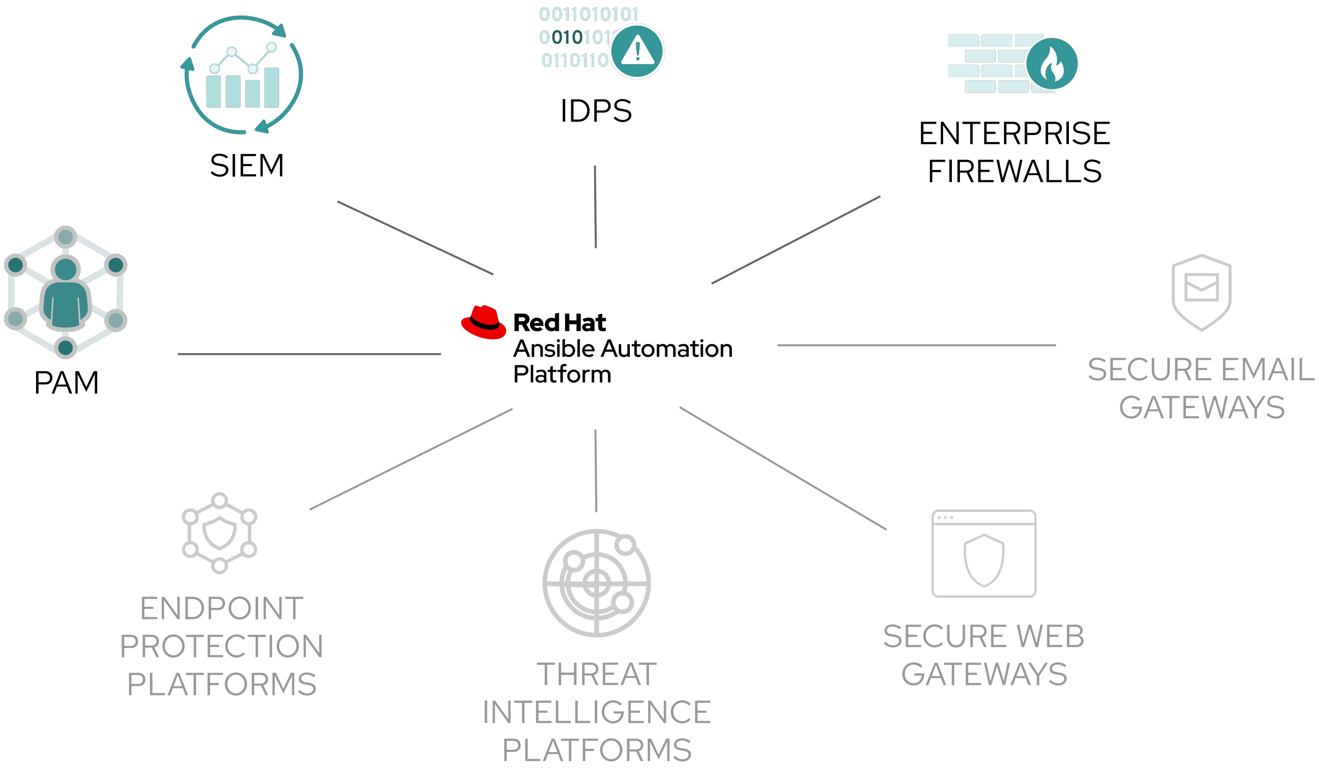


‘Lack of automation and orchestration’ ranked second and **‘Too many tools that are not integrated’** ranked third on the list of SOC challenges.

SANS Institute

Source:
The Definition of SOC-cess? SANS 2018 Security Operations Center Survey

What Is Ansible security automation?



Red Hat Ansible Automation Platform

SIEM

IDPS

ENTERPRISE FIREWALLS

PAM

SECURE EMAIL GATEWAYS

ENDPOINT PROTECTION PLATFORMS

THREAT INTELLIGENCE PLATFORMS

SECURE WEB GATEWAYS

What Is Ansible security automation?

Ansible security automation is our expansion deeper into the security use case. The goal is to provide a more efficient, streamlined way for security teams to automate their various processes for the identification, search, and response to security events. This is more complex and higher-value than the application of a security baseline (PCI, STIG, CIS) to a server.

Ansible security automation is a supported set of Ansible modules, roles and playbooks designed to unify the security response to cyberattacks.

Is It A Security Solution?

No. Ansible can help Security teams “stitch together” the numerous security solutions and tools already in their IT environment for a more effective cyber defense.

By automating security capabilities, organizations can better unify responses to cyberattacks through the coordination of multiple, disparate security solutions, helping these technologies to act as one in the face of an IT security event.

Red Hat will not become a security vendor, we want to be a security enabler.

Q&A

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.

- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHat