

Simplify Kubernetes security and operations with IBM and Sysdig



Mike Mcgee
Global Sales Executive
IBM



Eric Carter
Director, Product Marketing
Sysdig
[@ercarter](#)

CEOs have a consistent top priority—harness digital transformation to jumpstart **growth, speed** time to market, and foster **innovation**

80%

of decision makers agree that **integrating processes across organizational boundaries** and legacy systems will accelerate digital transformation.

84%

of global executives say they won't achieve their growth objectives without **scaling AI**.

Imagine you are the Chief Information Officer of a Regional Bank

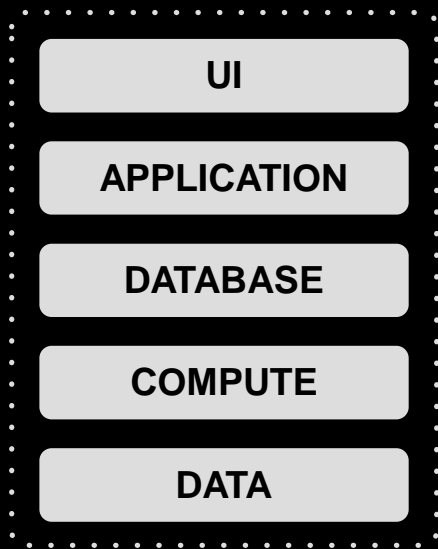
The CEO has asked your team to build
and deploy a new application for
mobile check deposits.

Your team is now responsible for building
and running an application architected on
cloud native
components and infrastructure...

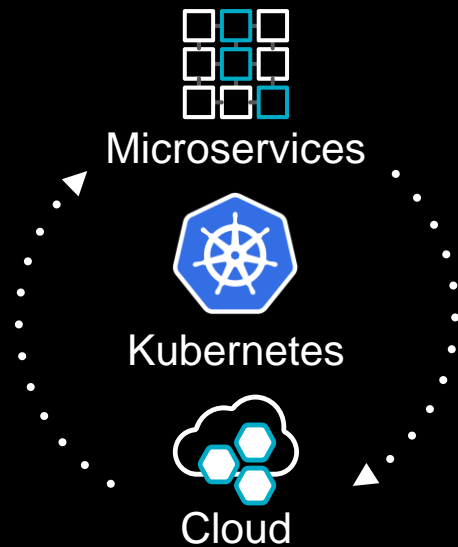
**NOW
WHAT?**



Turning to Kubernetes



- Innovate faster
- Gain cost efficiency
- Mitigate risk



Your job: Drive pilot through production ramp

IT Grappling with New Challenges

CIOs

Innovation vs. Security & Stability

2,000+ IT incidents per month

9 will be critical, costing
\$139k each on average

Costs compound with
regulatory & SLA penalties,
and customer impact

Negotiating Complexity & Scale

Dynamic container
environments require
automation to keep pace

Days to detect and diagnose
complex issues

Major outages can cost up to
\$420k per hour

DevOps Teams

Overwhelmed by disparate tools

Legacy tools leave you flying
blind in cloud native

Inconsistent alerts and data
across sources

No correlation between
performance and security

Workflows interrupted to
shift between tools

Skills & Burnout

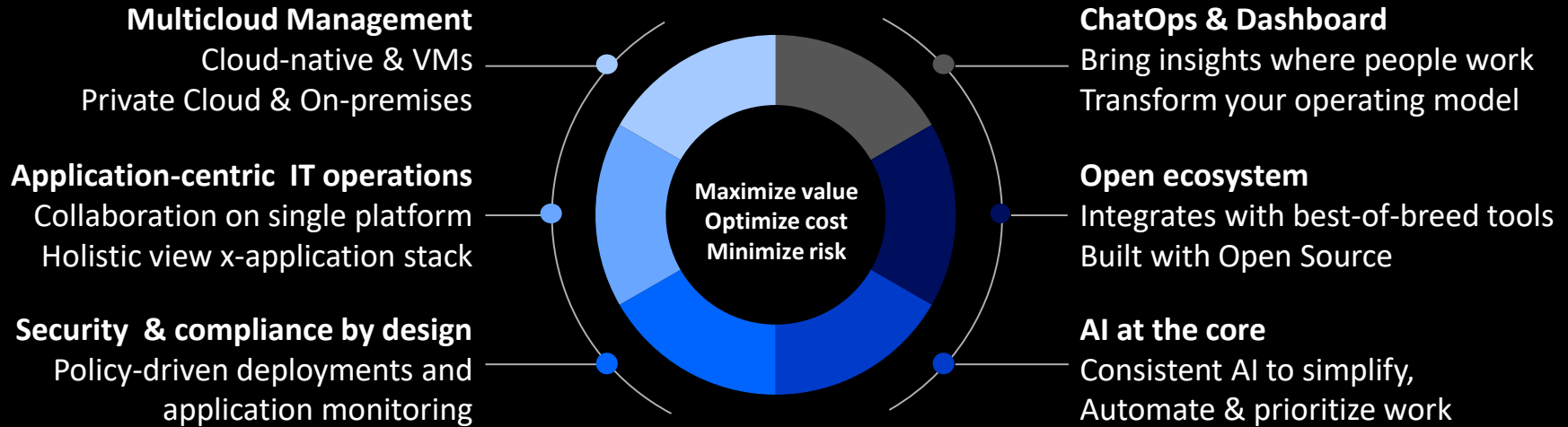
10% percent of FTEs **have 90%
of critical expertise**

Teams & CIOs struggle with
talent risk

Tasked with taking an active
role in security

23% percent of breaches are a
result of human error

As Development, Security and Operations converge, we need an intelligent and integrated approach to IT Operations



IBM Cloud Pak for Multicloud Management

Applications, Security, Data, Operational Services

Single Control
Plane for apps &
infrastructure



Security &
Compliance
Management



Automate
with
AI & ML



Kubernetes Environments
OpenShift, IKS, AKS, GKE, EKS
Cloud Native Workloads



Virtual Environments
OpenStack, RHEV, VMware
Traditional Workloads



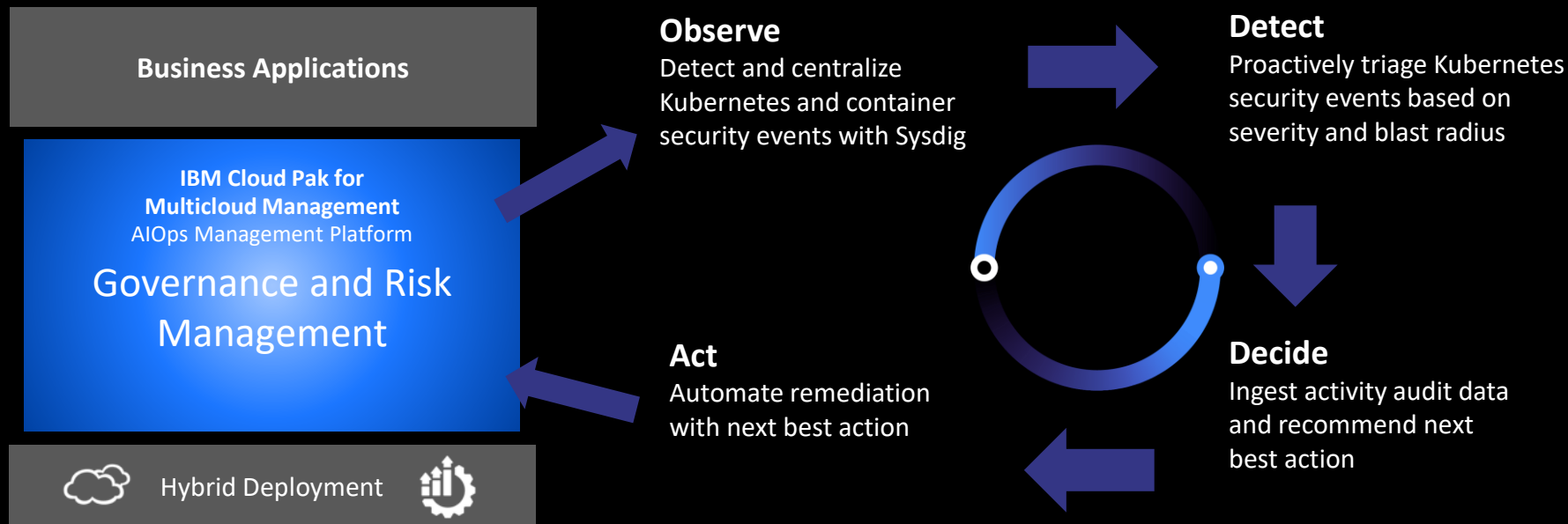
Kubernetes Security

IBM Cloud Pak for Multicloud Management with Sysdig container runtime security delivers **enterprise-ready, Kubernetes visibility & security** for hybrid cloud environments

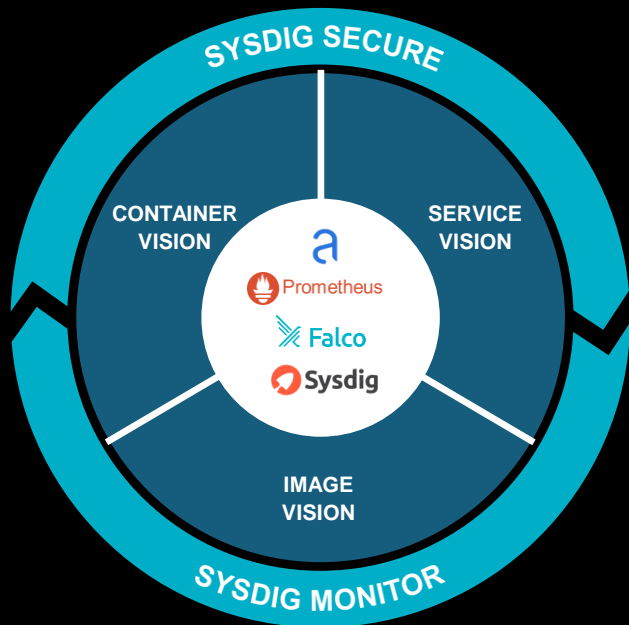
- **Detect and block threats** without impacting performance
- Enable **continuous compliance and audit** for standards like NIST, HIPPA, & PCI
- **Accelerate incident response** with automated remediation and detailed forensics data captures
- **Centralize security events** into the Cloud Pak for Multicloud Management Governance, Risk, and Compliance console for **a single-point of visibility**



Extend Security Intelligence with Sysdig



Sysdig Secure DevOps Platform



Embed security and
validate compliance



Maximize performance
and availability



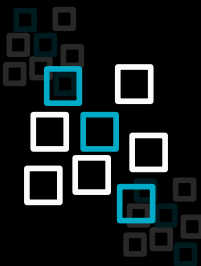
Get results quickly

Ship cloud apps faster with container visibility and security

Three key container challenges solved by Sysdig



Containers block visibility



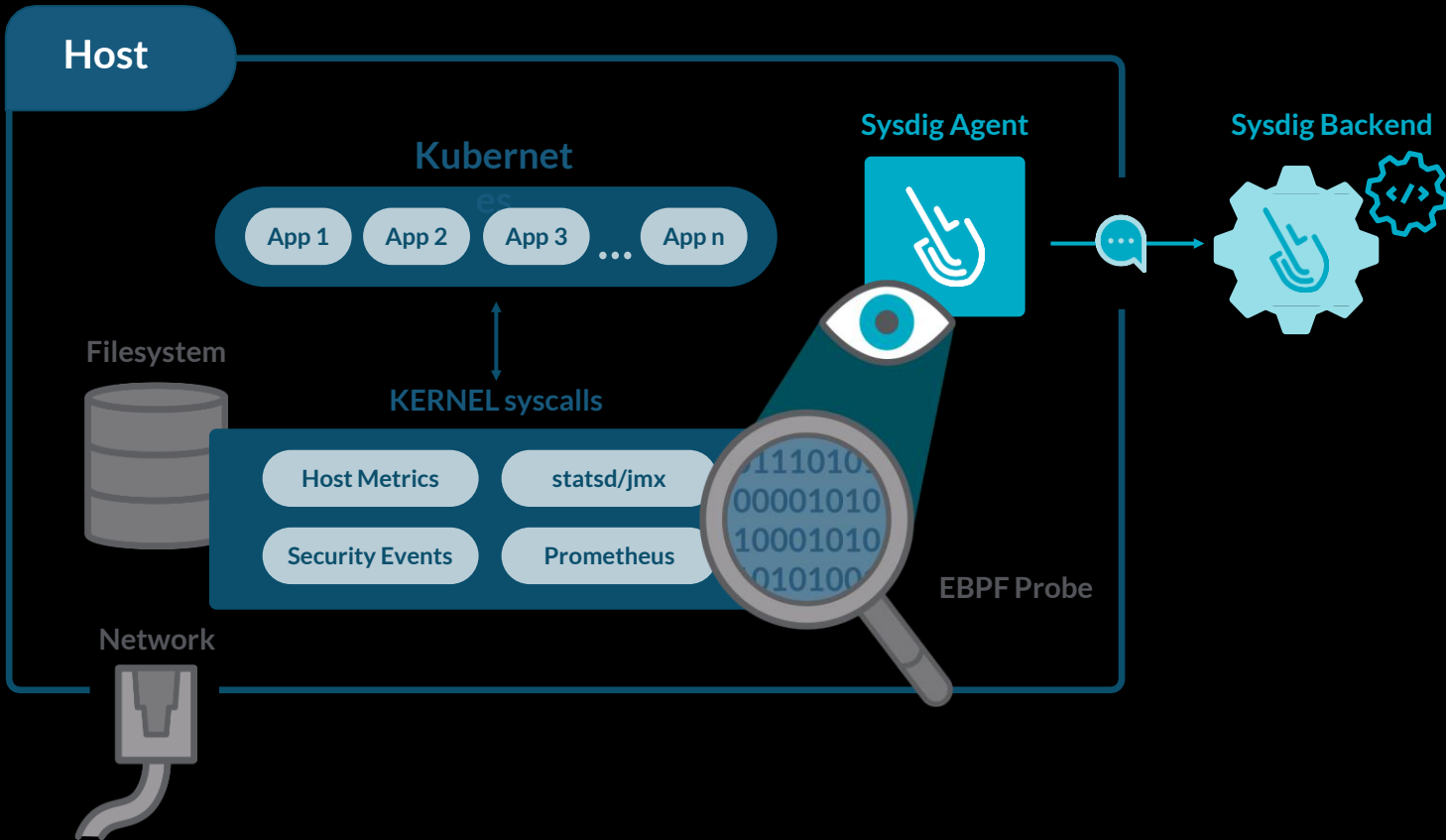
Security and operations fail
without Kubernetes context



Containers disappear and leave
no trail

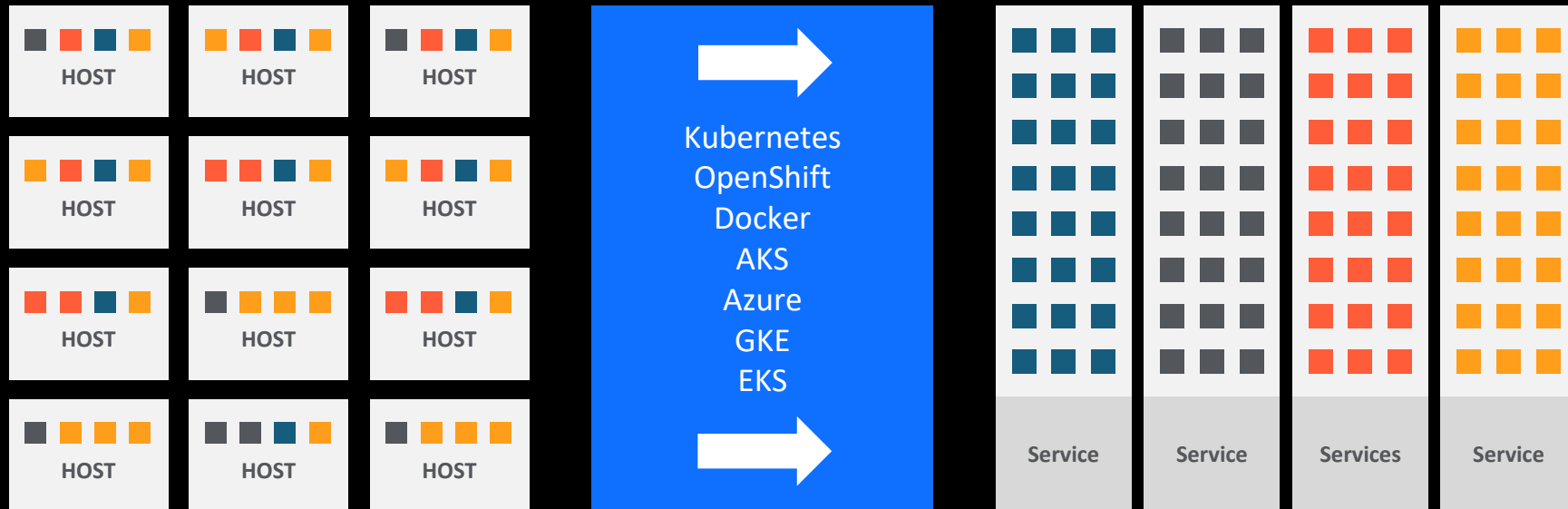
Instrumenting for Container Visibility

ContainerVision™



Enriching data with Kubernetes context

ServiceVision™



Clearly see security data by service, pod, namespace, deployment, etc.

Identify and Block Threats in Production

The screenshot displays the Falco security dashboard interface. On the left is a dark sidebar with navigation icons for Overview, Image Scanning, Benchmarks, Policies, Events, Activity Audit, Captures, and Get Started. The main panel is titled 'Events' and shows a list of security events. The selected event, 'Terminal shell in container', is highlighted in blue. A detailed view of this event is shown on the right, including its severity (High), event ID, and a description of the shell spawned in a container. Below the description are tags for 'container', 'PCI_DSS_10.2.1', 'shell', and 'mitre_execution'. The bottom of the dashboard features a timeline and a 'Live' status indicator.

Events

Legacy Events Feed

Edit Scope

Search by event title and label

High Med Low Info All Types

Filters...

4:18:04 AM **Terminal shell in container**
1 capture | kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=terminal-shell-in-container and

4:14:04 AM **Launch Suspicious Network Tool in Container**
kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=suspicious-network-tool and kubernetes.d

3:20:01 AM **Ingress Object Without TLS Cert Created**
kubernetes.cluster.name=demo-kube-aws

1:15:04 AM **Create/Modify Configmap With Private Credentials**
kubernetes.cluster.name=demo-kube-aws

08/12/2020

10:55:04 PM **Access Cryptomining Network**
kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=crypto-mining-demo and kubernetes.deplo

10:55:04 PM **Access Cryptomining Network**
kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=crypto-mining-demo and kubernetes.deplo

10:55:03 PM **Access Cryptomining Network**
kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=crypto-mining-demo and kubernetes.deplo

3:15:10 PM **Sensitive Info Exfiltration**
1 capture | kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=sensitive-info-exfiltration and k

Load Older...

Triggered on Thu Aug 13 2020 at 4:18:04 AM | 6 hours ago

Terminal shell in container

High Severity Event ID: 162acfa01bca24ac7da5294adb6afa6

Captures Activity

Exclude Image: sysdiglabs/workshop-forensics-1-phpping

Actions

Capture covering 04:17:54 - 04:18:24 AM

Policy & Triggered Rules

Edit Policy

name Terminal shell in container

ruleType Falco - Syscall

ruleName Terminal shell in container

A shell was spawned in a container with an attached terminal (user=www-data k8s_store_frontend-ping-php_store_frontend-ping-php-7588976944-mnhck_terminal-shell-in-container_e1d632b8-7e85-46e7-a5ff-5c3af75ad085_8 (id=d01a2af53a) shell=bash parent=runc cmdline=bash terminal=34832 container_id=d01a2aff53a image=sysdiglabs/workshop-forensics-1-phpping)

container

PCI_DSS_10.2.1

shell

mitre_execution

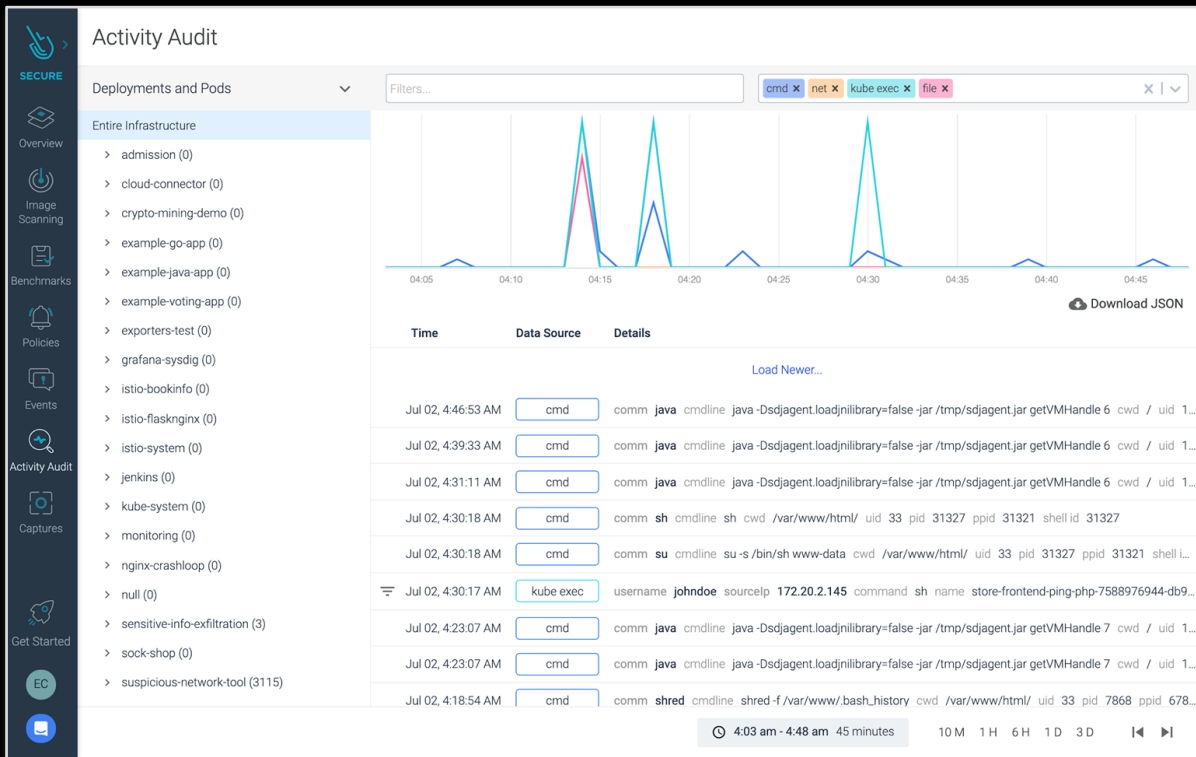
Aug 12, 10:27:39 am - Aug 13, 10:27:39 am Last 1 day

10M 1H 6H 12H 1D 3D

Live

- Configure policies to detect suspicious runtime behavior and anomalies
- Built on open-source Falco
- Apply remediation actions
- Create syscall captures for forensics

Audit Activity



- Capture & index user and service activity
- Filter by file, network, command and Kubectl activity
- Comply with SOC2, PCI, ISO, HIPAA, etc.

Centralize Security Events in Cloud Pak for Multicloud Management

The screenshot displays the IBM Cloud Pak for Multicloud Management interface, specifically the 'Governance and risk' section under 'Security findings'. The top navigation bar includes 'Overview', 'Policies', and 'Security findings'. The main content area shows a summary of security findings categorized by 'Other', 'HIPAA', and 'PCI'. The 'Other' category shows 2691 findings, with 2534 of high severity. The 'HIPAA' category shows 1 finding. The 'PCI' category shows 2 findings. A detailed view of a 'Terminal shell in container' event is shown, including its details and a list of related events. The 'Events' section lists various security events, such as 'Terminal shell in container', 'Launch Suspicious Network Tool in Container', 'Ingress Object Without TLS Cert Created', 'Create/Modify Configmap With Private Credentials', 'Access Cryptomining Network', and 'Sensitive Info Exfiltration'. A detailed view of the 'Terminal shell in container' event is shown, including its actions and policy rules.

IBM Cloud Pak for Multicloud Management

Governance and risk

Overview Policies Security findings

Summary Standards

Other

2691/2694 CLUSTER FINDINGS

2534/2694 HIGH SEVERITY

HIPAA

1/2694 CLUSTER FINDINGS

PCI

2/2694 CLUSTER FINDINGS

1/2694 HIGH SEVERITY

Terminal shell in container

Details

Update time 2020-01-17T11:18:04.145508Z

Events

Search by event title and label

High Med Low Info All Types

4:18:04 AM Terminal shell in container

1 capture | kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=terminal-shell-in-container and

4:14:04 AM Launch Suspicious Network Tool in Container

kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=suspicious-network-tool and kubernetes.deployment.name=suspicious-network-tool

3:20:01 AM Ingress Object Without TLS Cert Created

kubernetes.cluster.name=demo-kube-aws

1:15:04 AM Create/Modify Configmap With Private Credentials

kubernetes.cluster.name=demo-kube-aws

08/12/2020

10:55:04 PM Access Cryptomining Network

kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=crypto-mining-demo and kubernetes.deployment.name=crypto-mining-demo

10:55:04 PM Access Cryptomining Network

kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=crypto-mining-demo and kubernetes.deployment.name=crypto-mining-demo

10:55:03 PM Access Cryptomining Network

kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=crypto-mining-demo and kubernetes.deployment.name=crypto-mining-demo

3:15:10 PM Sensitive Info Exfiltration

1 capture | kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=sensitive-info-exfiltration and kubernetes.deployment.name=sensitive-info-exfiltration

Terminal shell in container

Triggered on Thu Aug 13 2020 at 4:18:04 AM 6 hours ago

High Severity Event ID: 162a3ca01bca24ac7d6d294ab6af65

Captures Activity

Exclude Image: sysdiglabs/workshop-forensics-1-phping

Actions

Capture covering 04:17:54 - 04:18:24 AM

Policy & Triggered Rules

name Terminal shell in container

ruleType Falco - Syscall

ruleName Terminal shell in container

A shell was spawned in a container with an attached terminal (user=www-data kube.store.frontend-ping-php.store.frontend-ping-php-7588976944-mehck-terminal-shell-in-container-e16832b0-7e85-46e7-a5ff-5c3a775a0885_0 (id=d81a2af753a) shell-bash parent=run cndLine=bash terminal=34832 container_id=d81a2af753a image=sysdiglabs/workshop-forensics-1-phping)

container

PCI_DSS_10.2.1

shell

mitre_execution

Aug 12, 10:27:39 am - Aug 13, 10:27:39 am Last 1 day

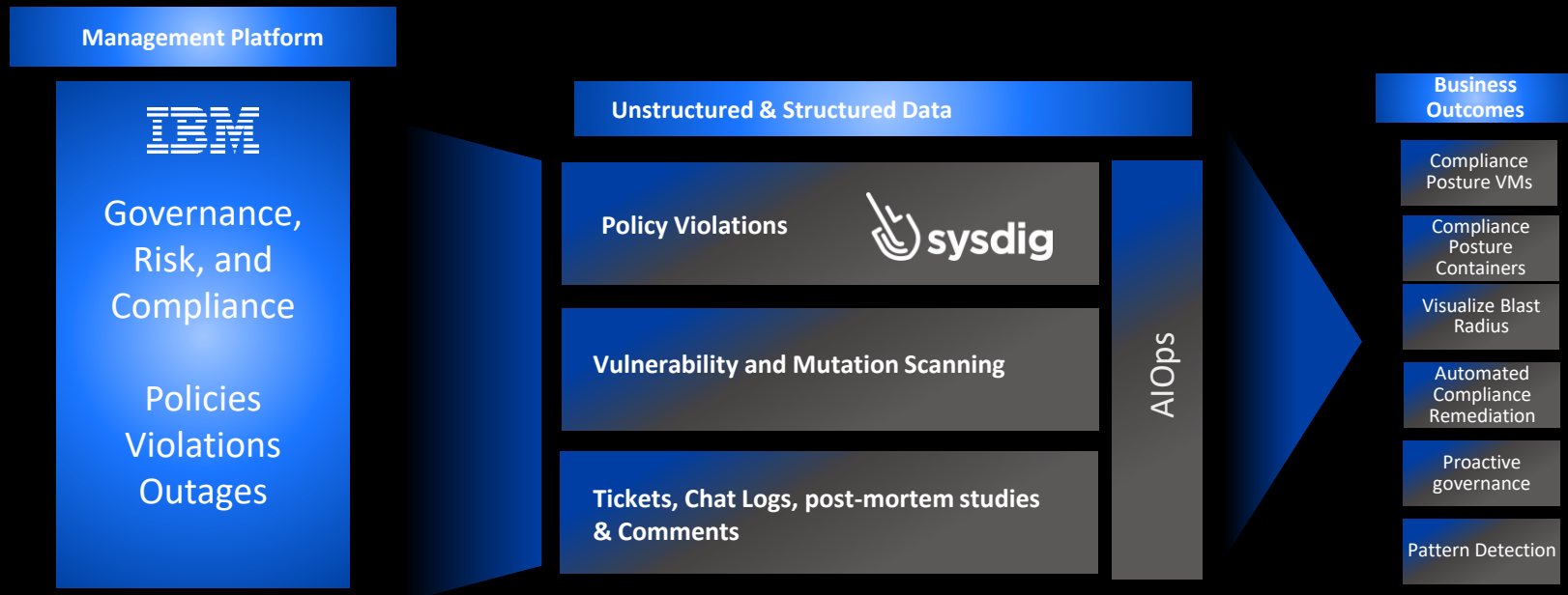
10M 1H 6H 12H 1D 3D

Live

- See detailed container and Kubernetes security events in central console
- Launch in context to Sysdig Secure for deeper analysis
- Leverage Sysdig detected signals with IBM AI

AIOps Creates Smarter GRC Management

Manage Risk with Structured and Unstructured Data



AIops Creates Smarter GRC Management

1. Accurately identify emerging problems (resolve if possible)
2. Get incidents properly assigned, with context
3. Diagnose problems fast in dynamic and complex environments



The Impact of AI

Efficiency, cost savings and a foundation built in DevSecOps to gain meaningful business value from IT operations

\$420k
saved*

by reducing outage costs by
1 hour

50%
less cost

in labor by up-skilling
IT operators with
AI-powered insights

25%
more initiatives

Get job done faster and
focus on new initiatives.

*Potential impact

Thank you



Learn more:

IBM Cloud Pak for Multicloud Management with AIOps

<https://www.ibm.com/cloud/cloud-pak-for-management>

Sysdig Secure DevOps Platform

<https://sysdig.com/platform>

Join the community

<https://community.ibm.com/>