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**.

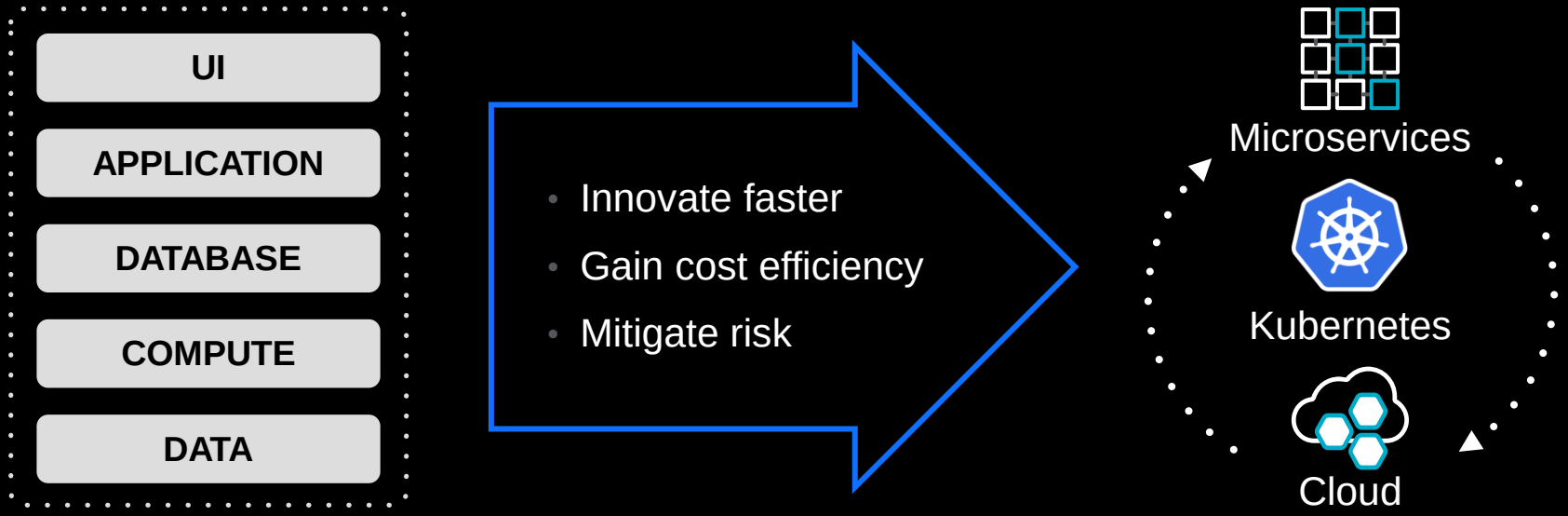
Imagine you are the Chief Information Officer of a Regional Bank

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



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

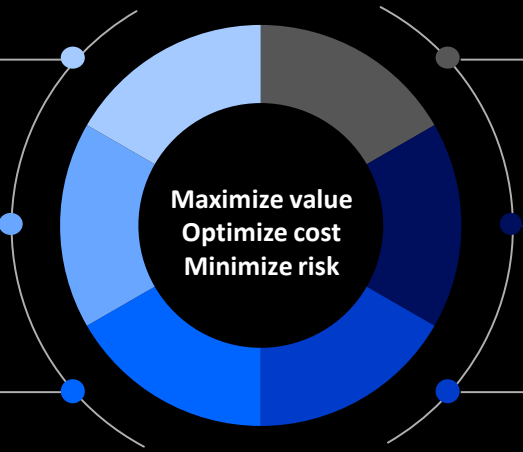
23% percent of breaches are **a result of human error**

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

Multicloud Management
Cloud-native & VMs
Private Cloud & On-premises

Application-centric IT operations
Collaboration on single platform
Holistic view x-application stack

Security & compliance by design
Policy-driven deployments and application monitoring



ChatOps & Dashboard
Bring insights where people work
Transform your operating model

Open ecosystem
Integrates with best-of-breed tools
Built with Open Source

AI at the core
Consistent AI to simplify,
Automate & prioritize work

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

IBM public cloud | AWS | Microsoft Azure | Google Cloud | Private

sysdig 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 & IBM

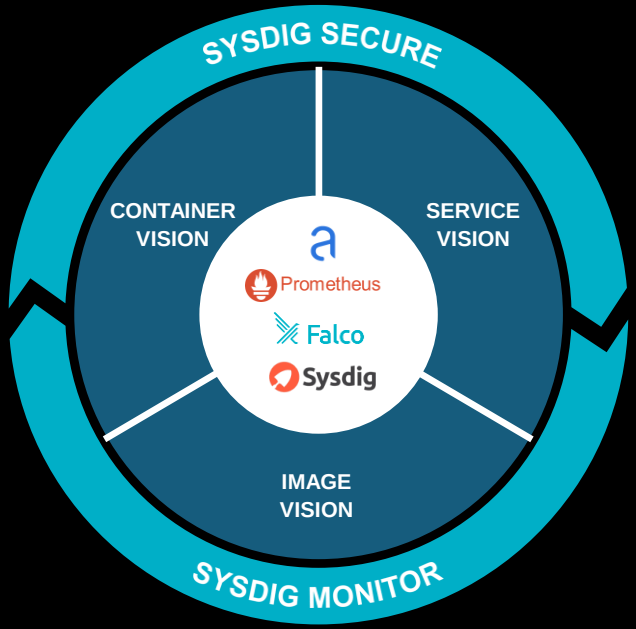
Observe
Detect and centralize Kubernetes and container security events with Sysdig

Detect
Proactively triage Kubernetes security events based on severity and blast radius

Decide
Ingest activity audit data and recommend next best action

Act
Automate remediation with next best action

Sysdig Secure DevOps Platform



Embed security and validate compliance

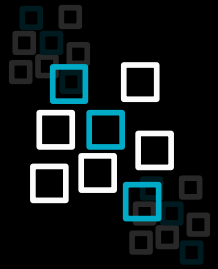
Maximize performance and availability

Get results quickly

Ship cloud apps faster with container visibility and security

Three key container challenges solved by Sysdig

Containers block visibility

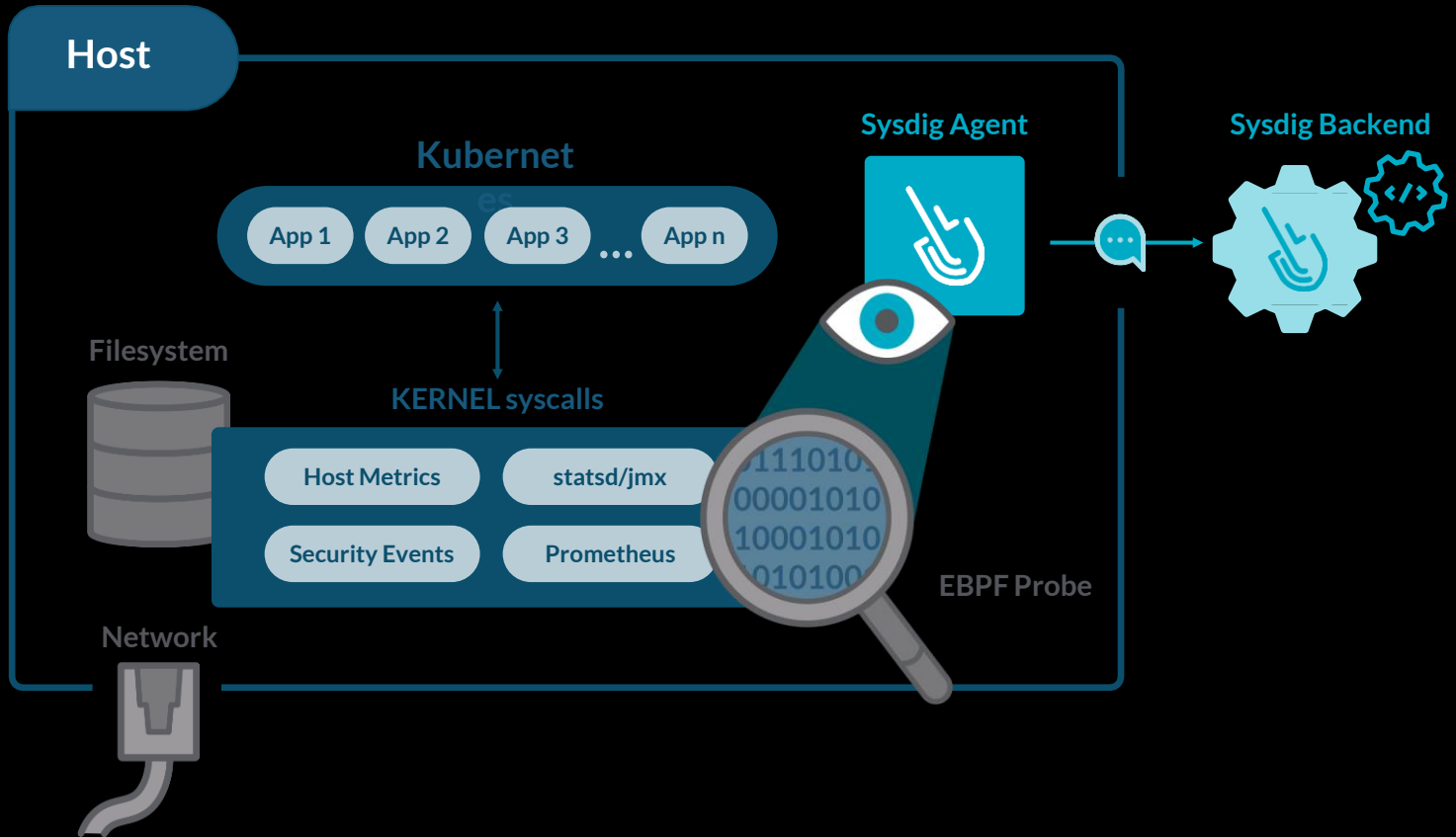


Security and operations fail without Kubernetes context

Containers disappear and leave no trail

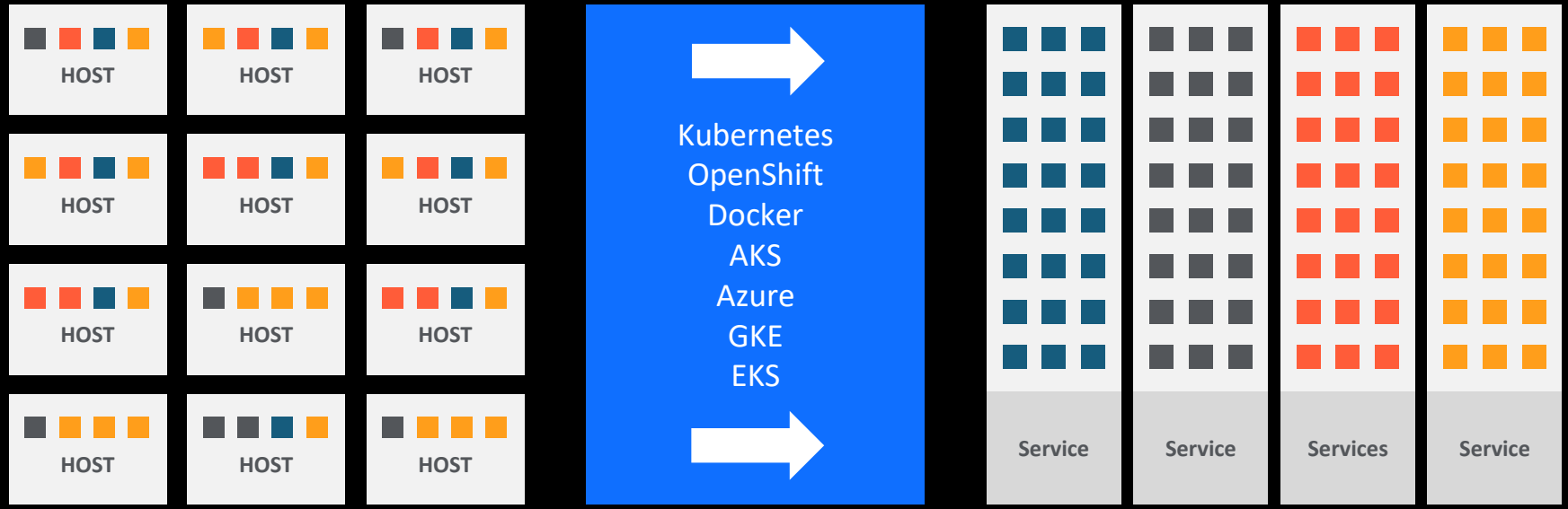
Instrumenting for Container Visibility

ContainerVision™



Enriching data with Kubernetes context

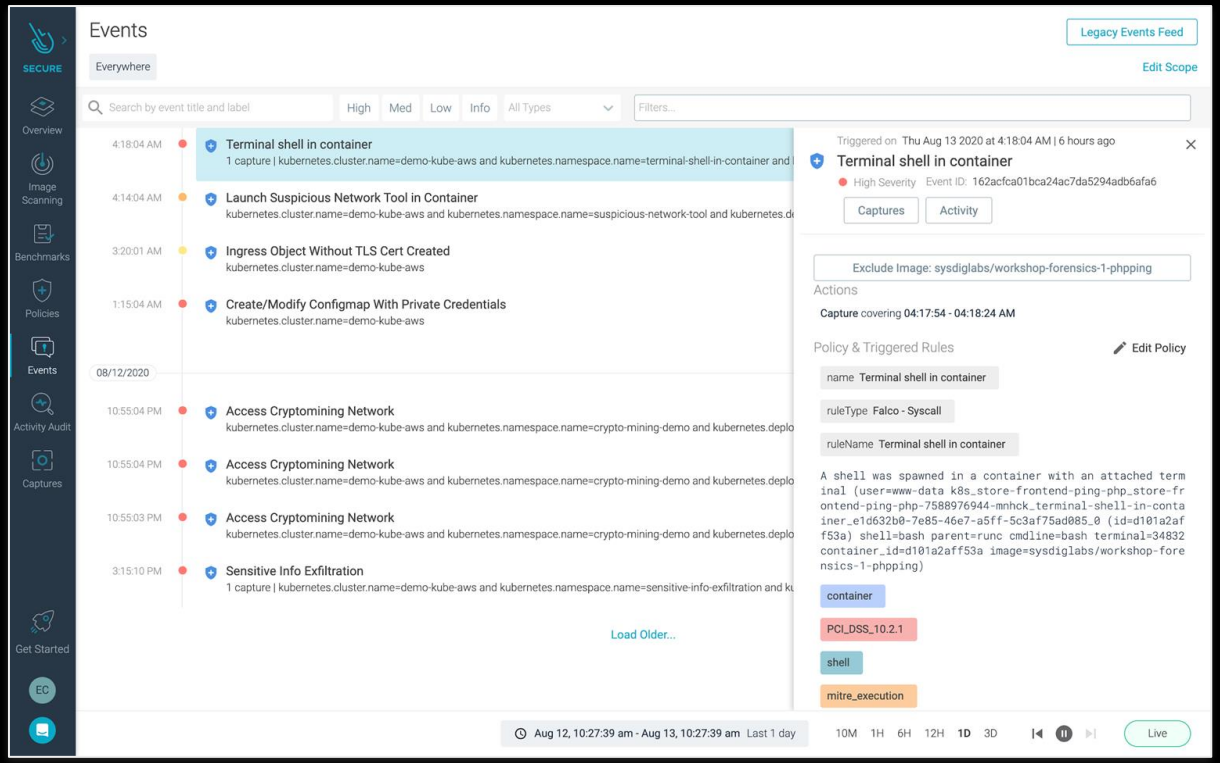
ServiceVision™



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

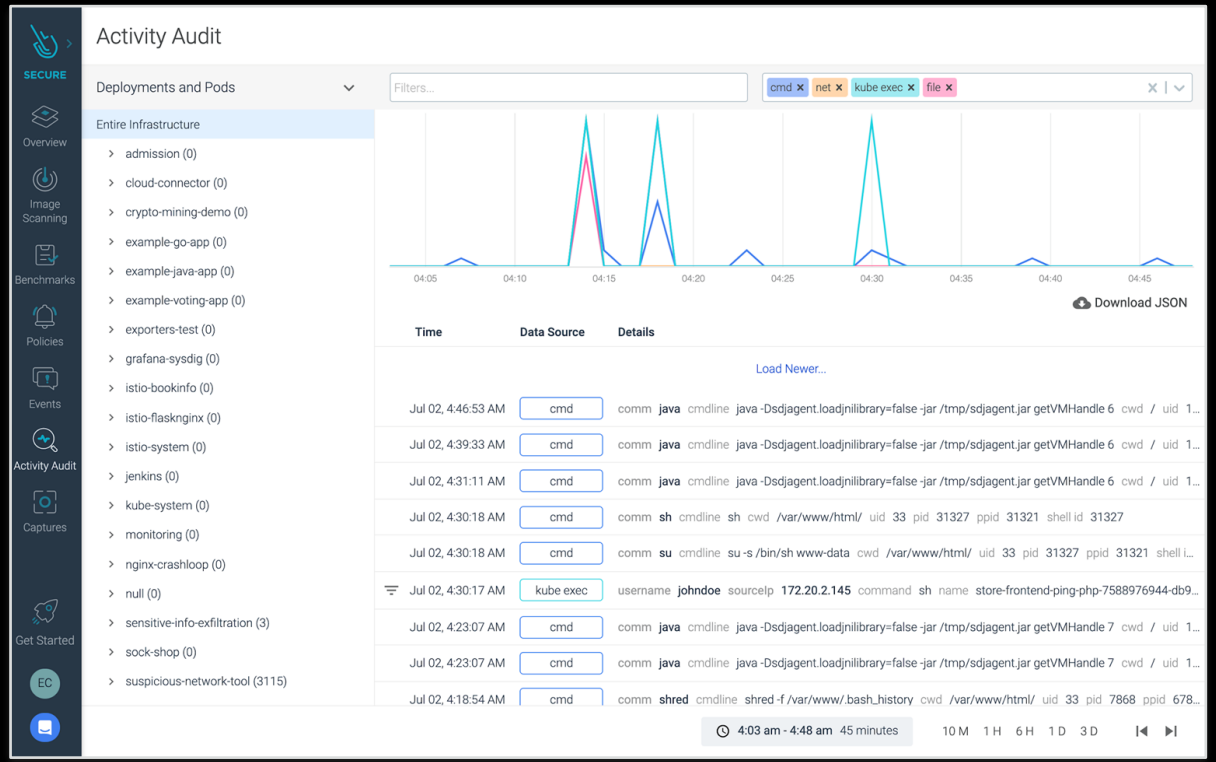
12

Identify and Block Threats in Production



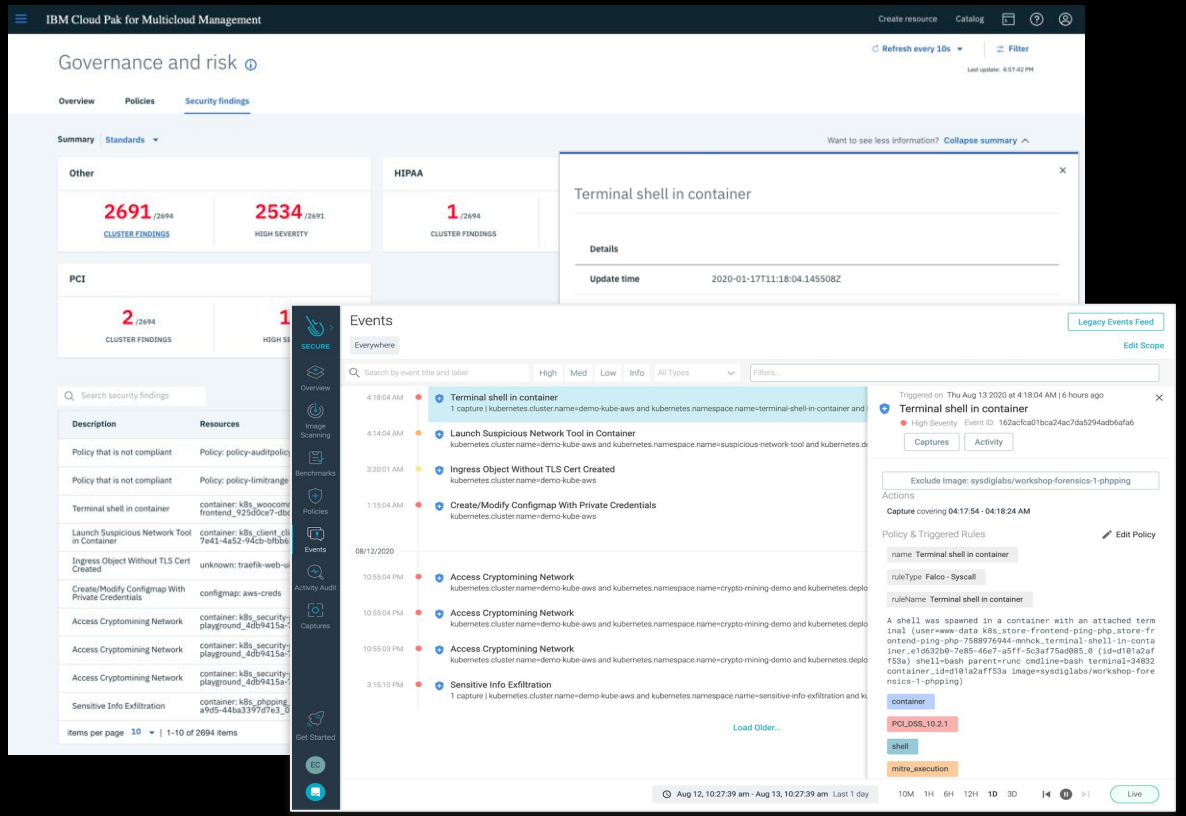
- Configure policies to detect suspicious runtime behavior and anomalies
- Built on open-source Falco
- Apply remediation actions
- Create syscall captures for forensics

Audit Activity



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

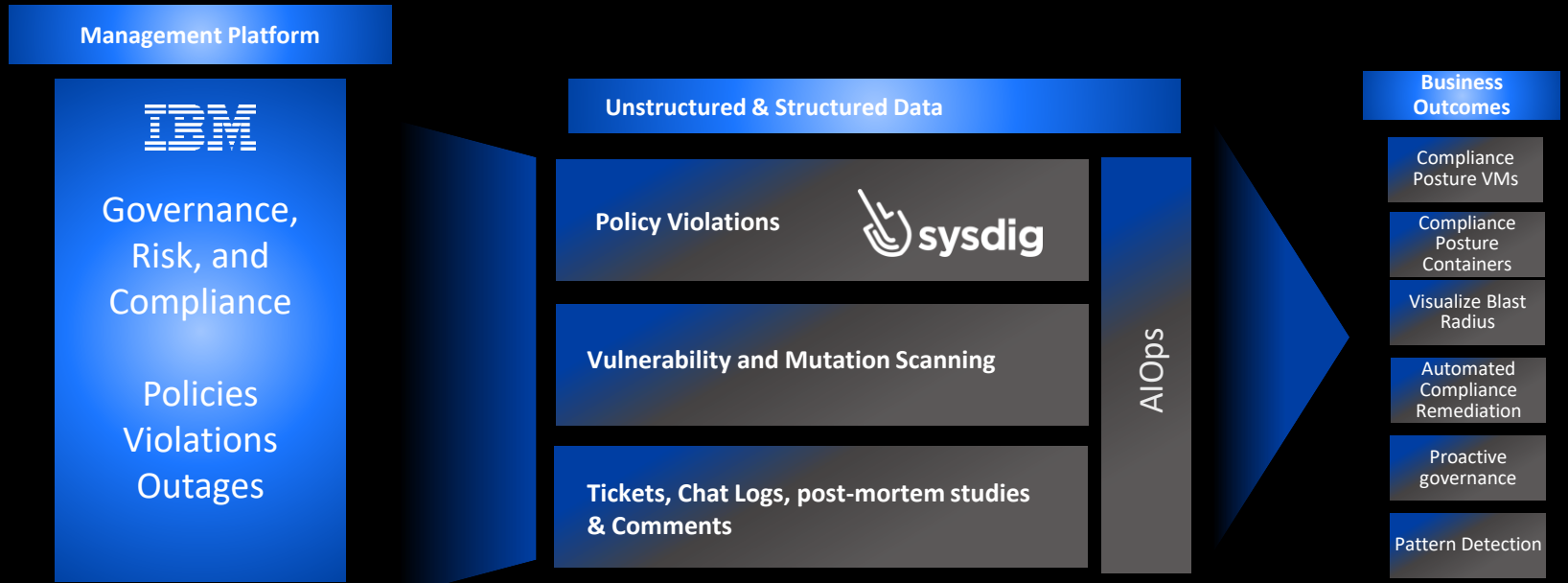
Centralize Security Events in Cloud Pak for Multicloud Management



- 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

Connect, Observe and Ingest → **Reduce Noise and Incidents** → **Get Relevant Context** → **Collaborate** → **Automate Response Permanently Fix**

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/