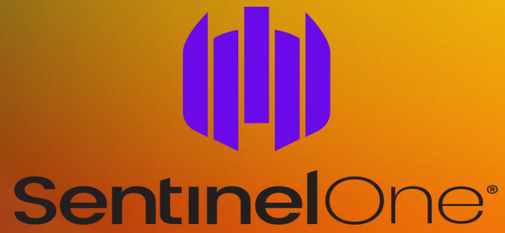

AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT075



Using AI to thwart cloud ransomware

Holly Bittinger

Communications Specialist
SentinelOne

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sidescanning Alone is Insufficient for Cloud Workload Protection

- Daily scans will not catch real-time incidents
- Does nothing for behavioral, process-level incidents
- More frequent scans are cost-prohibitive



Workload Compromise	Lateral Movement	Exfil & Encrypt
Opportunistic Actors	Expand Target Base	Ransomware
Programmatic compromise in **MINUTES**	Expansion and persistence in **MINUTES**	Subversion in **SECONDS**

Role of CWPP in Cloud Defense in Depth

AppSec

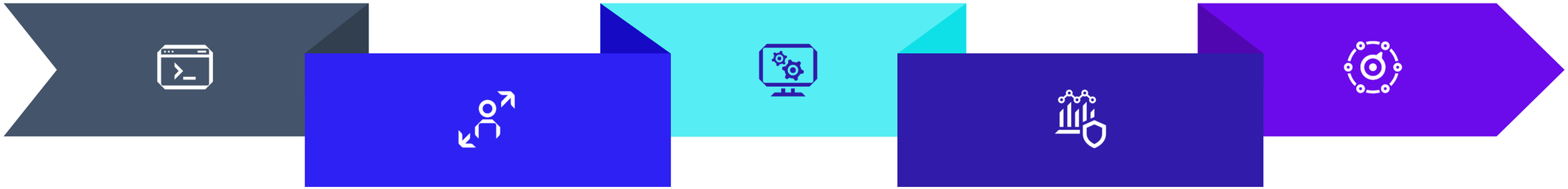
Software vulns, SAST, DAST, image scanning, “shift left”

CSPM

Config management, IaC templates, drift management, etc.

CWPP

Runtime protection, detection, response for workloads



CIEM

Identity and entitlements for human and machine roles

CDS

Data security, malware scans of object storage, etc.

© 2022 SentinelOne. All Rights Reserved.

Examples of Runtime Incidents

Ransomware

- Focus on Linux: DarkRadiation
- RaaS (Ransomware as a Service)
- Second only to crypto mining

Crypto Mining Malware

- Computationally intensive
- You lose control of your infrastructure
- You keep the bill

146%

YoY increase in new Linux ransomware code variants

Source: X-Force Threat Intelligence Report, 2022

© 2022 SentinelOne. All Rights Reserved.

Machine-Speed Detection & Response

vs machine-speed adversaries



Static AI/ML

- File inspection
- Parsing file structures
- Entropy
- Opcode histograms

ML algorithms learn good from bad
Unsupervised doesn't require feature labeling



Behavioral AI

- OS process monitoring
- Event linking
- Adds new dimension: TIME
- Extensive context

AI learns *how* programs behave (good & bad)
AI improves over time (observability)

© 2022 SentinelOne. All Rights Reserved.

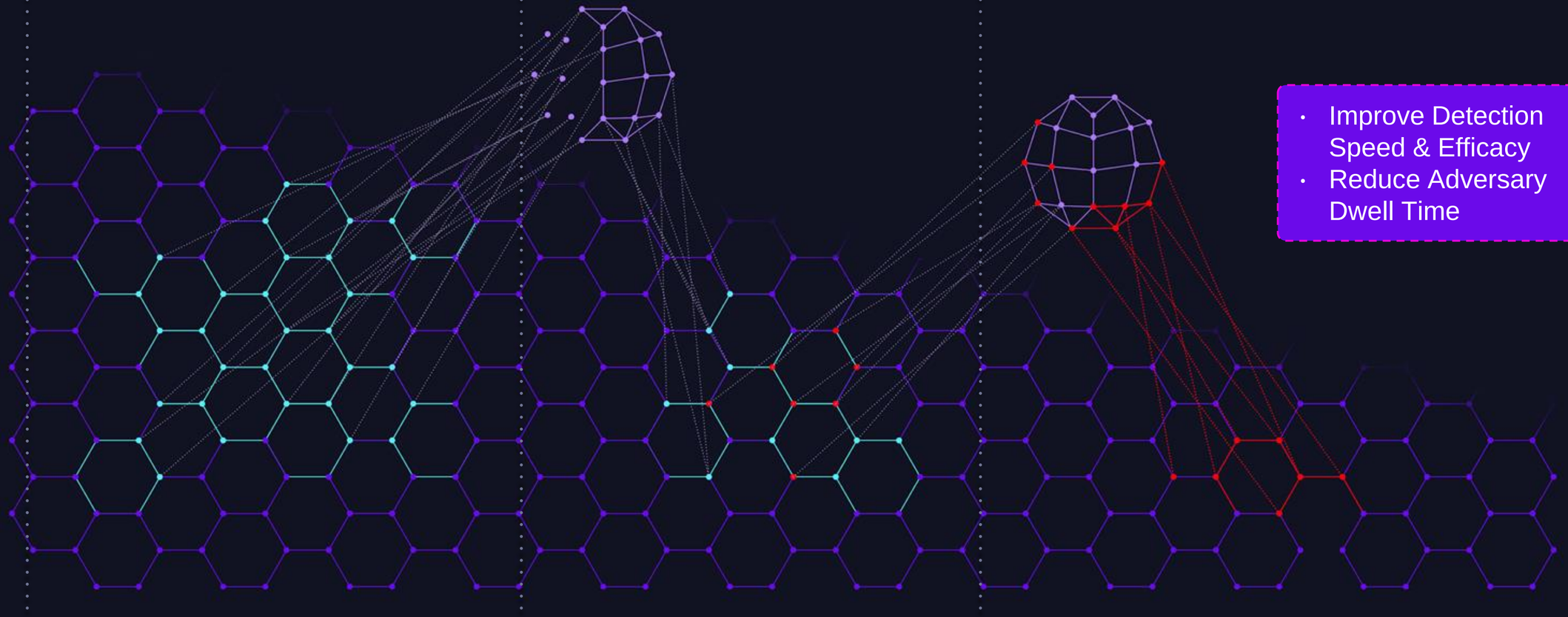
CWPP Delivers High SNR Forensic Details

Trillions
of Rows of Raw Data

Millions
of Enriched Storylines

Handful
of Actionable Incidents

- Endpoint
- Email
- Web Gateway
- Network
- Firewall
- Cloud
- Identity

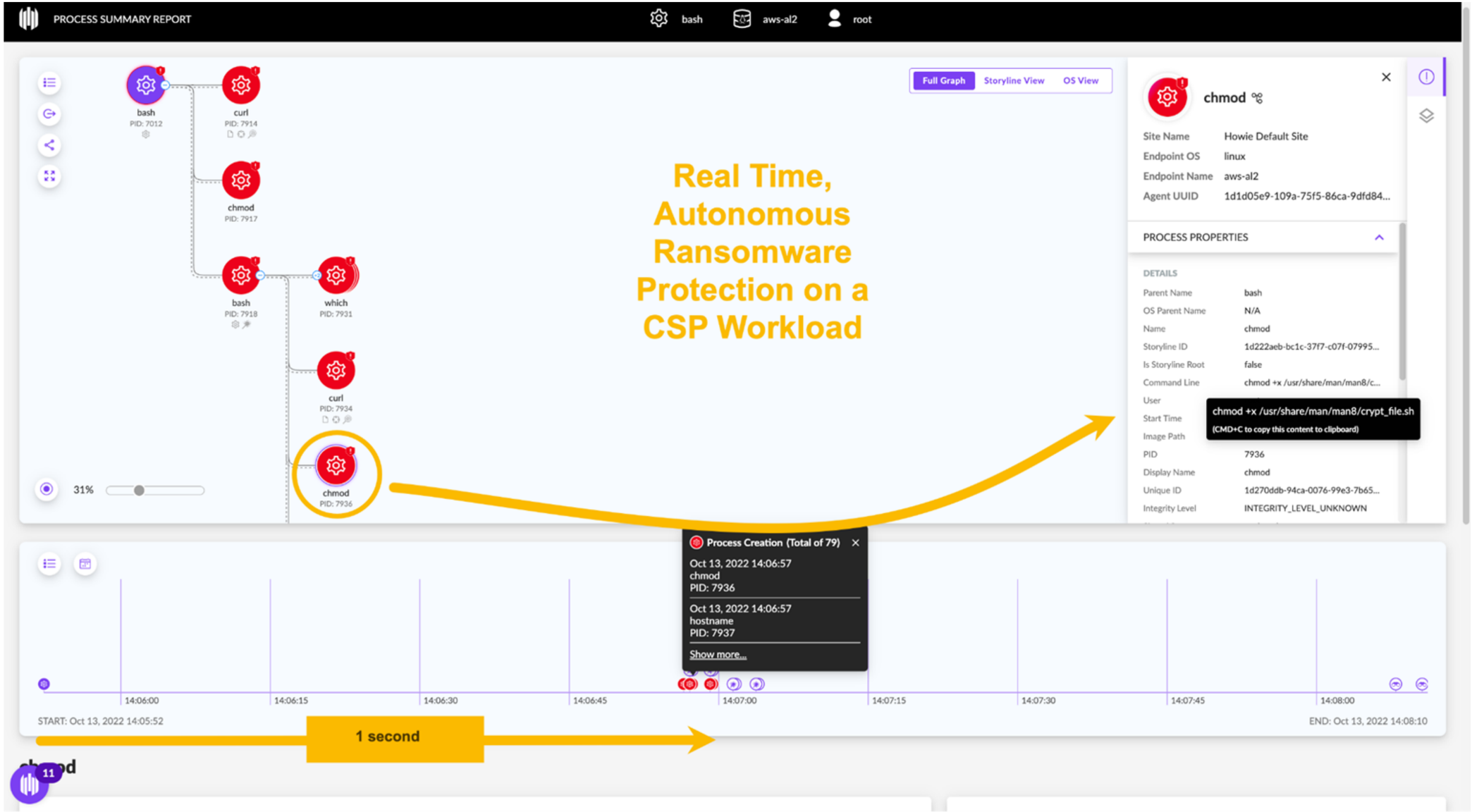


- Improve Detection Speed & Efficacy
- Reduce Adversary Dwell Time

SentinelOne

© 2022 SentinelOne. All Rights Reserved.

Storyline™ of a Ransomware Incident



Singularity™ Cloud

Cloud Workload Security for Server/VM/Kubernetes

Outcomes

- Runtime security for workloads in AWS and data center
- Cloud-first architecture, no kernel dependency hassles
- Easy to deploy, manage, and update
- One security umbrella for cloud and endpoints
- One-click response and remediation
- Coverage for many OSes, including Amazon Linux 2022





Singularity™ Cloud

- Multi-OS workload coverage, scale, and reliability
- Simple procurement process
- AWS Enterprise Discount Program (EDP)
- Support for FedRAMP Moderate workloads in AWS GovCloud

aws PARTNER

Competencies

- **Public Sector**
- **Security**

AWS Disaster Recovery

Amazon S3

AWS Security Hub

Amazon Elastic Kubernetes Service (Amazon EKS)

Amazon Elastic Kubernetes Service Anywhere (Amazon EKS-A)

Amazon Inspector

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Container Service (Amazon ECS)

Amazon Elastic Container Service Anywhere (Amazon ECS-A)

docker

Windows Server

AWS Security Competency

AWS Marketplace

FedRAMP

SentinelOne

© 2022 SentinelOne. All Rights Reserved.

Summary: The Case for CWPP

01

CWPP Stops What Others Might Not

Ransomware
Cryptominers
Runtime-loaded malware

02

AI-Driven EDR for Runtime Defense

Real-time
Behavioral
Amazon EC2, Amazon ECS, Amazon EKS

03

Persistent Forensic Detail

Auto-correlated
Enriched telemetry
Threat hunting

04

Better Security, SOC Productivity

Catch more
Deliver more
Stress less

To learn more or connect with an expert
www.sentinelone.com

SentinelOne

© 2022 SentinelOne. All Rights Reserved.

Thank you!





Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.