

# Welcome to the Webinar!

**SECURITY**  
BOULEVARD

## **How I Achieved Security Discipline and Governance Across AWS, Azure, and GCP**

**Jack Roehrig**  
**CISO**



# Meet Our Expert Panel



**Moderator**

**Charlene O'Hanlon**

**Managing Editor  
Security Boulevard**



**Jack Roehrig**

**CISO  
Turnitin**



**Patrick Pushor**

**Technical Evangelist  
Orca Security**

# About Orca Security



**Orca gives you workload-level visibility across 100% of your AWS, Azure, and GCP assets without agents.**

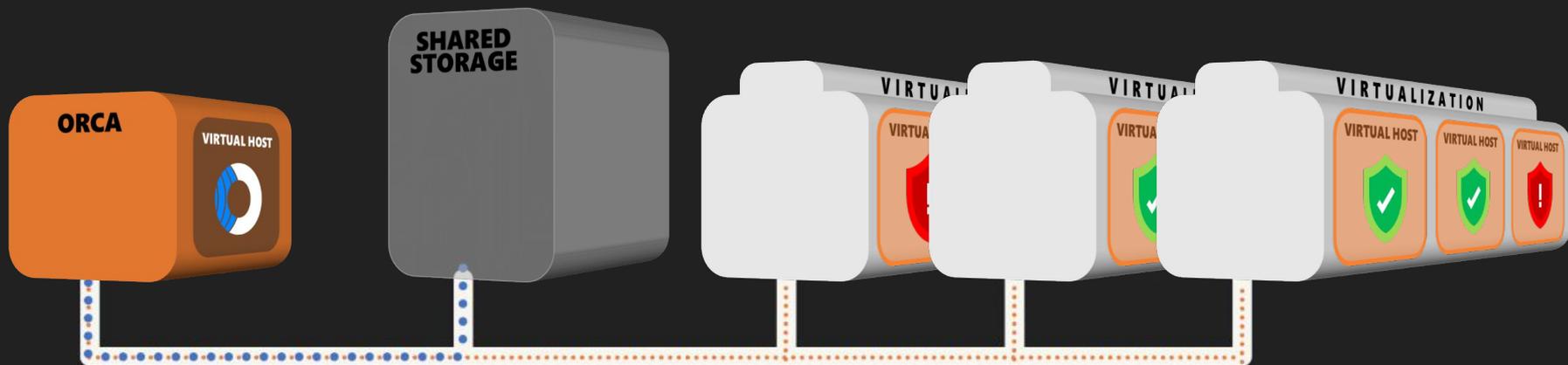
Instant-on, no hassle, impact-free deployment

Complete coverage, no overlooked assets

Deeper inspection, down to the data layer

Reduces thousands of security alerts to the critical few that matter

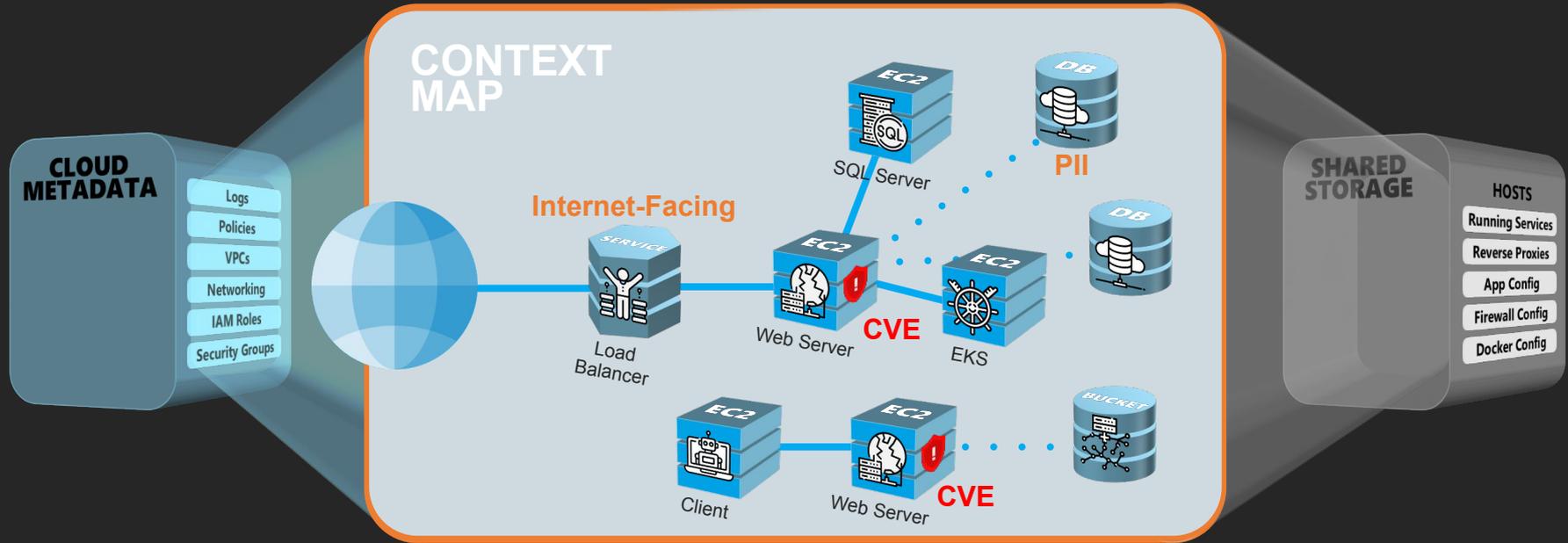
# SideScanning™ Technology



All hosts are continuously  
analyzed and protected

No Agent needed!

# Understanding Context



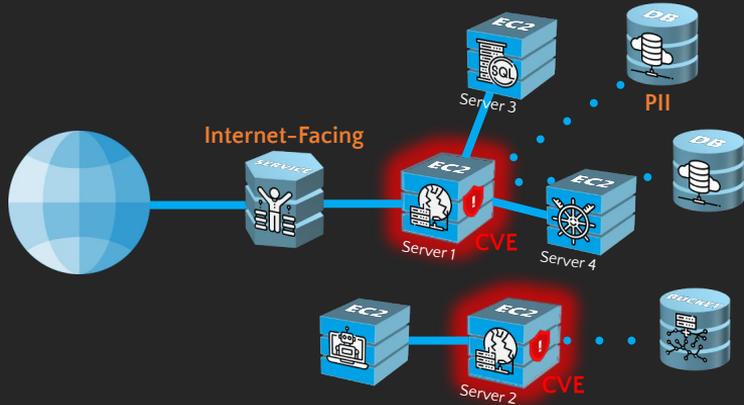
● Discover Cloud assets

● Identify asset roles

● Identify connectivity

● Identify Vulnerabilities

# Understanding Context

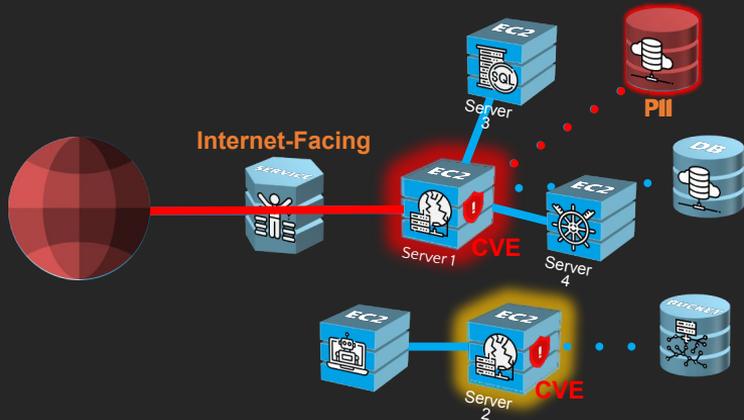


## AGENTS LOG

	Asset	Service	Issue	Type	Score
!	Server 1	Apache	CVE-2018-1176	RCE	High 8.8
!	Server 2	Apache	CVE-2018-1176	RCE	High 8.8
✓	Server 3	SQL	--	--	None
✓	Server 4	EKS	--	--	None

Identical Severity Score

# Understanding Context



## ORCA LOG

	Asset	Service	Issue	Risk	Score
🚨	Server 1	Apache	CVE-2018-1176	Internet-facing PII Exposure	Imminent
🛡️	Server 2	Apache	CVE-2018-1176	Internal server	Medium
✅	Server 3	SQL	--	--	None
✅	Server 4	EKS	--	--	None

Severity Score according to context

# Sample Customers



## Enterprise

Top 10 Global  
Consultancy

Top 5 Private  
Equity Firm

Big 4 Professional  
Sports League

Top 5 Global  
Hotel Chain

## Mid-Market

**fiverr**<sup>®</sup>

**LIONBRIDGE**

 **AROUNDTOWN**<sup>SA</sup>

**turnitin**

 **MRS**

## Cloud

**people.ai**

**NG**  **DATA**

**Qu**  **bole**

 **SISENSE**

 **Fyber**

## Fintech

  
**LIVE OAK BANK**

  
**North American**<sup>®</sup>  
BANCARD

  
**paidy**

**cake**

**Rapyd**

Type of Scanner / Capabilities

Agents

Unauthenticated Network Scanner

Authenticated Scanner

Cloud Security Posture Manager



Type of Scanner / Capabilities	Agents	Unauthenticated Network Scanner	Authenticated Scanner	Cloud Security Posture Manager	ORCA security
Risk to Scanned Assets	MEDIUM	HIGH	MEDIUM	NONE	NONE
Security Visibility Depth	HIGH	LOW	HIGH	LOW	HIGH
Security Visibility Breadth	LOW	MODERATE	LOW	HIGH	HIGH
Vulnerability Detection	YES	MODERATE	YES	NO	YES
Malware Detection	YES	NO	NO	NO	YES
INFRA, OS, Apps, & Data Inventory	YES	NO	NO	NO	YES
Cloud Level Misconfiguration Detection	NO	NO	NO	YES	YES
Scan Stopped Machines	NO	NO	NO	N/A	YES

“Tenable and Qualys both felt like they loosely bolted their legacy enterprise products onto the cloud. That doesn’t work well because you still have to deal with agents and contend with technology that isn’t meant for serverless or containers.”

**Jeremy Turner**  
Senior Cloud Security Engineer





## Hi, I'm Jack!

**Beauty-school dropout**

**Over 25 years of InfoSec and DevOps experience**

**'Greenfielded' InfoSec programs for over a dozen companies**

**Dual DevOps/Security roles**

**Data privacy nerd**

**Passion for ethical impact**



# Hi, I'm Jack!

Global CISO experience in:

- Education
- Healthcare
- Advertising
- Social networking
- Search
- SaaS
- B2B
- Media

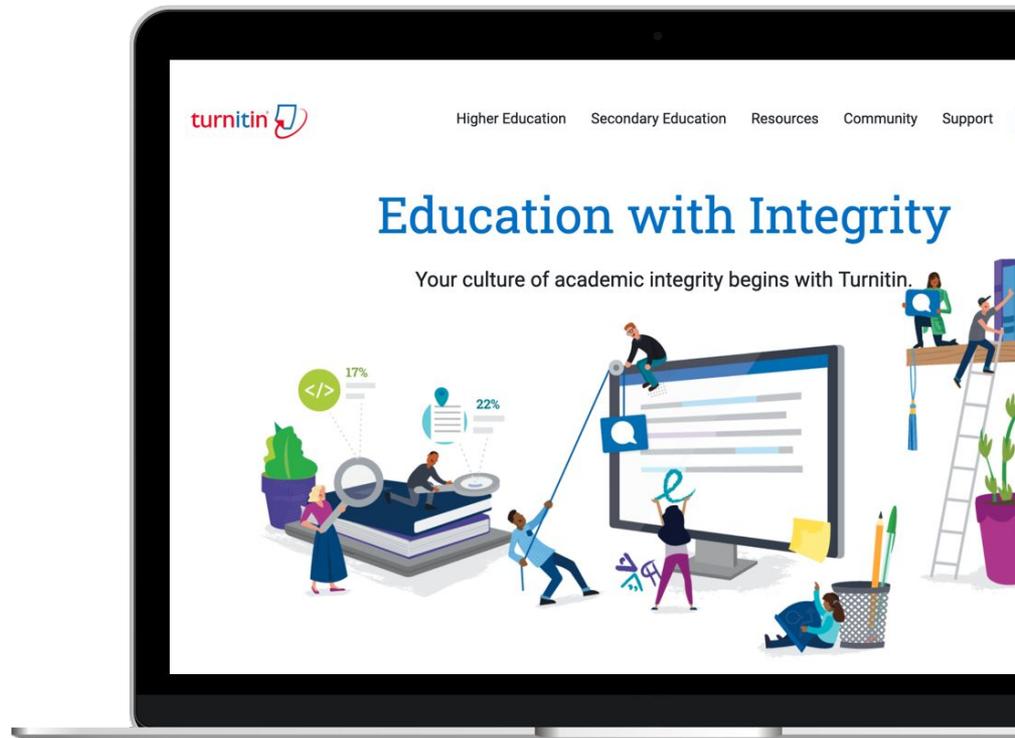
# About Turnitin

Among many other things, we focus on similarity (plagiarism) detection

Huge database of free-form submissions

Not just essays!

- Index the internet like Google
- Store licensed content
- Corporate customers
- Government customers



# About Turnitin

≈ 1.3 BILLION submissions!

Tens of millions of users in over 150 countries

Paid SaaS solution. No advertisers

Turnitin needs strong security and data privacy practices



# State of data privacy and security in education

Academic institutions continue to be targeted by hackers.

- Large infrastructure deployments (more attack space).
- Understaffed and can't afford enterprise security programs.
- High-bandwidth internet connections.
- Can't prioritize keeping software up-to-date.
- Students tend to abuse shared infrastructure.

All of these characteristics make institutions a prime target for hackers to build infrastructure, extort money, and steal sensitive data. Some just want to disrupt!

# Security Challenges at Turnitin

2017

Greenfield security program began just under three years ago

2019

Pivoted from four-year private-equity-backed firm to indefinite-term variable-runway. **Huge change in risk appetite!**

2020

Tricky cloud migration requiring user adoption  
**launching now**



# Security Challenges at Turnitin

**Customers are passionate about data privacy**

**Unique target: misunderstood, often-hated, and a honeypot of data**

**Complex, delicate infrastructure. Difficult to maintain; compromised governance and SoD**



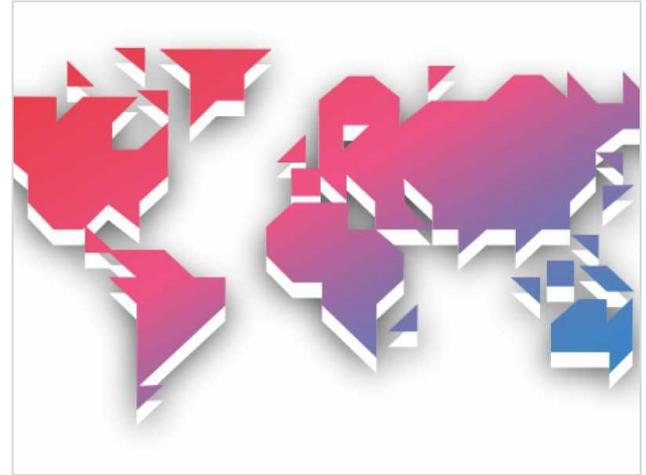
# Security Solutions at Turnitin

**Holistic program in-place:** soft solutions prioritized with technical solutions

**Security culture:** everyone thinks about security in their own roles

**Security from day one:** every employee receives personal onboarding from Jack

**Risk-based approach:** emphasis on discovery and prioritization of issues



# Cloud Security Solutions at Turnitin

## Cloud Migration Needs

Complicated, lift-and-shift cloud environment

Needed fast awareness of risks in production for go/no-go development

## Cloud Security and Governance Stack

Orca Security

Host-based IDS

Whitesource for our CI/CD pipeline

Various tools and services to audit application security

Configuration management for patch deployment (to fix what Orca finds)

# Cloud Security Solutions at Turnitin



**Orca Security enables us to..**

- Identify risks in ungoverned cloud accounts
- Identify misuse of PII/personal data on production infrastructure
- Satisfy various compliance requirements
- Routinely govern bad employee behavior (PII storage, key storage, password storage, etc.)
- Enforce sane credential use
- Discover assets across multiple cloud service providers and many accounts
- Profile the risk of potential acquisitions (M&A due diligence)

# How Orca Security Empowers Turnitin

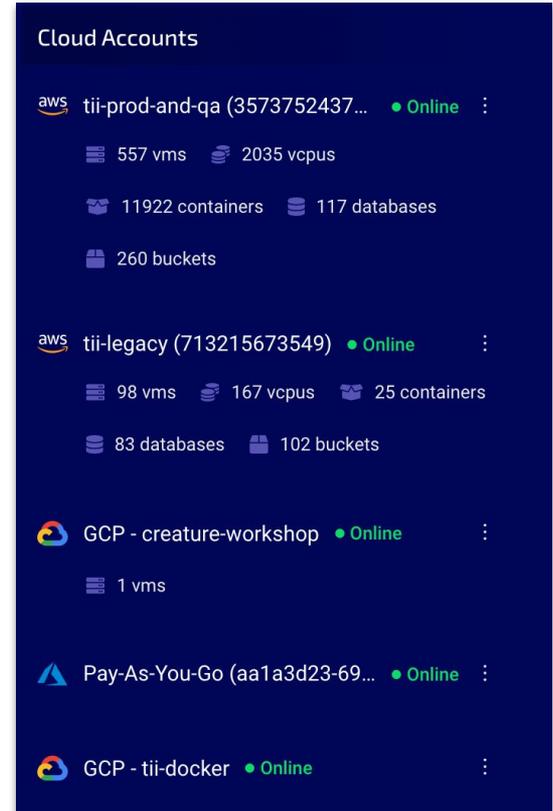
*It's agentless. The skeletons are always in the closets I can't open.*

Installs quickly, profiles risk immediately

Profiles machines regardless of my access

Eliminates friction with DevOps

Enables easy management of many cloud accounts



# How Orca Security Empowers Turnitin

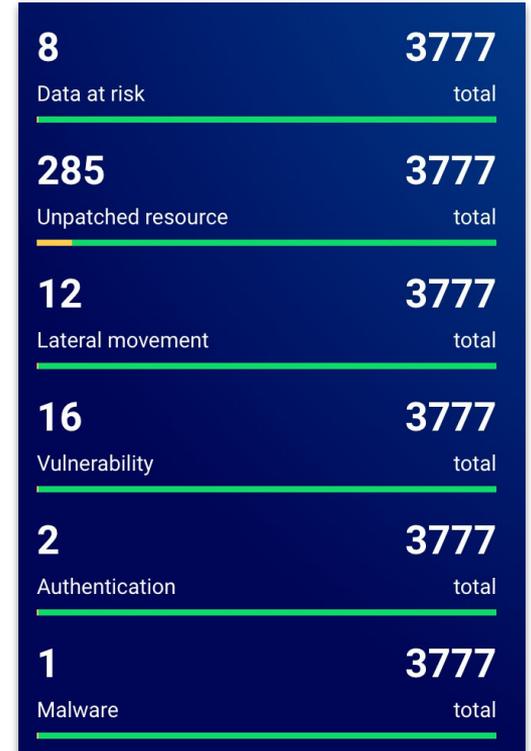
*It aggregates risk so I don't have to.*



Easy-to-consume risk categories

Aggressive data granularization

Enables pragmatic risk consumption



# How Orca Security Empowers Turnitin

*It identifies improperly-handled PII, which can illuminate data segregation risks.*

Discovers PII where it shouldn't exist

Enables insight into who is managing sensitive data

Empowers governance of data segregation policies



## Personally Identifying Information – accounts

Email addresses found on an internet-facing asset

Modification time: 2020-06-05 06:21:25

File: /var/pd/tests/INTS-5651/accounts\_to\_deconfigure.csv

### Email addresses (Masked):

- ka\*\*\*\*\*@bcc.cuny.edu
- wj\*\*\*\*\*@kings.edu
- dc\*\*\*\*\*@westmont.edu
- ms\*\*\*\*\*@wlu.ca
- ir\*\*\*\*\*@taism.edu.om
- tt\*\*\*\*\*@athabascau.ca
- t.\*\*\*\*\*@kingston.ac.uk
- nj\*\*\*\*\*@gateway.ac.uk
- tr\*\*\*\*\*@ubalt.edu
- rt\*\*\*\*\*@britishschool.be

# How Orca Security Empowers Turnitin

*It helps me govern the goofy things that people do.*

Description: the private key "/home/jmiller/.s

Private key file: /home/jmiller/.ssh/id\_rsa

Public keys:

- /home/jmiller/.ssh/authorized\_keys (cas
- /home/jmiller/.ssh/authorized\_keys (ops
- /home/jmiller/.ssh/authorized\_keys (cas
- /home/jmiller/.ssh/authorized\_keys (cas
- /home/jmiller/.ssh/authorized\_keys (cas
- /home/jmiller/.ssh/authorized\_keys (ops
- /home/jmiller/.ssh/authorized\_keys (db-
- /home/jmiller/.ssh/authorized\_keys (cas
- /home/jmiller/.ssh/authorized\_keys (ops
- /home/jmiller/.ssh/authorized\_keys (cas
- /home/jmiller/.ssh/authorized\_keys (cas
- /home/jmiller/.ssh/authorized\_keys (cas

Enumerates lateral movement from stored private keys

Snitches on the lazy bash users

Makes employees think (know) that I'm omniscient

Password in shell history

The asset contains credentials in shell history, found in clear text.

# How Orca Security Empowers Turnitin

*It highlights risks of potential acquisitions without being invasive.*

Acquisitions tend to be mostly in the cloud

Orca integrates quickly into cloud accounts

Orca aggregates risk at a high-level

Orca creates executive-level reporting in seconds



# How Orca Security Empowers Turnitin

*It alerts me of new risks in ungoverned cloud accounts.*

Watches over hundreds of clouds

Categorizes new risks and alerts me about them

Illuminates the chaos; enables practical visibility

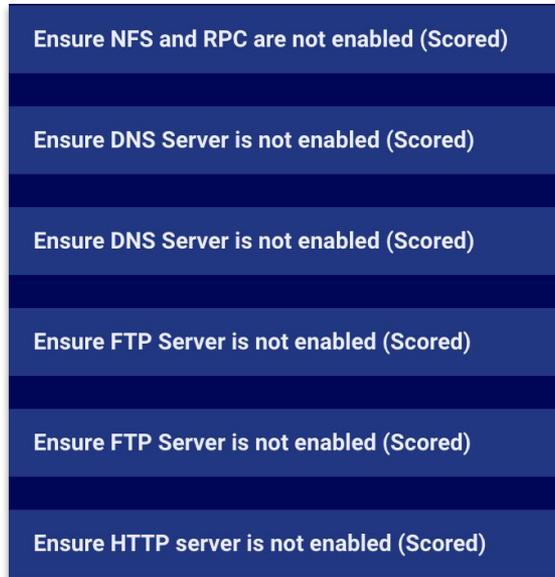
 orca-23163	<b>Unpatched Host OS</b>
 cacenp-sato-dpr-process Running	We have found 520 vulnerabilities

- AWS - 357375243774
- AWS - 713215673549
- Azure - db89e8d97561-941efd1d9d51
- GCP - ai-sales-training-jan-2019
- GCP - alteryx-connector-230416
- GCP - archive-11b93
- GCP - banded-meridian-257501
- GCP - blog-1569561133494
- GCP - bonsai-demo



# How Orca Security Empowers Turnitin

*It provides evidence to my auditors.*



**Watches over hundreds of clouds**

**Categorizes new risks and alerts me about them**

**Illuminates the chaos; enables practical visibility**



# How Orca Security Helps Reduce Friction with DevOps

## My DevOps Engineers...

- Were skeptical
- Hate agents
- Loved the quick deployment
- Like the simple UI and easy-to-consume risks, but hate being outed for insecure practices
- Eager to enable DevOps governance



# How Orca Security Helps Reduce Friction with DevOps

## The Shift-Left Security Approach

### Shift-left isn't just about guardrails, controls, and policies: it's culture

- At the core of every holistic security program is motivating a culture of security
- Omnipresent tools (like Orca) that highlight poor security in real-time help shift culture
- Tools that drown out useful data with noise are ineffective

### Orca Security aggregates the risk and eliminates the noise

- One of my first initiatives at Turnitin was to eliminate false-positive alerts
- Our on-call and support engineers couldn't prioritize the chaos
- Orca's risk-aggregation and risk-correlation solution eliminate the noise
- This allows engineers to focus on what's important



# What, No SIEM?

## *Alert fatigue and the ubiquitous SIEM...*

### **Mature company problems - SIEMs are ineffective**

- I was once quoted \$6MM for a SIEM from Splunk
- I managed infrastructure that produced tens of terabytes of relevant logs a day
- I had a team of  $\approx$  40 employees across six departments
- **Who has time for all that data ingestion, aggregation, and routing?!**

### **Modern tools prioritize risks & reduce SIEM insanity**

- Several tools in our stack do this well
- These tools store informational/trivial logs in their own systems, for limited time
- Higher-severity and higher-priority logs are pumped to Slack (free, long-lived, auditable)
- Critical-severity logs are sent to alerting infrastructure for business-hours or after-hours response

# Tips from the Field - Full Scope Governance

## Governed assets introduce less risk than ungoverned. Because they're governed...

- It's a catch-22
- DevOps engineers spend too much time in the wild west; lassoing rogue assets and herding "pets"
- Infrastructure are cattle, not pets...

## Full-scope governance - from stochasm to determinism

- Some tools work on discovered assets - unknown gap
- Some tools discover assets - known gap that needs to be closed
- Some tools govern the assets they discover - closed gap

## Nothing is perfect, but I work with risk, not absolutes

- Unknown gaps make understanding risks difficult
- Known gaps make understanding risks much easier
- Auto-governed, auto-discovered gaps mitigate risk

# Tips from the Field - SoD and a Kitchen Full of Cooks

## More mature-company problems

- Mature companies have many orphaned products and features
- These generally require hands-on support directly from engineers; they lack operational governance

## Even more mature-company problems

- Mature companies have a smaller appetite for risk and a bellies full of sensitive data
- Least-privilege is essential for managing sensitive data; especially when there are “too many cooks”

## Mature-company solutions

- Effective PII/personal-data discovery assists with enforcement of SoD and least-privilege
- When guardrails aren't feasible, throwing up roadblocks will mitigate risks effectively
- Roadblocks enforce policy and satisfy audit

# Tips from the Field - Minimizing Duplicative PII/PD

## Malicious actors tend to be lazy; lazy in a good way

- Why break into Fort Knox when the janitor has a big batch of bullion in his bunk?
- Duplicative personal data stored outside of regulated areas is a honeypot for bad bees

## Why is personal data stored duplicatively?

- Well-intentioned contributors unknowingly violate SoD for testing, migrations, or manual work
- And they rarely clean up their messes

## Mature-company solutions

- Monitoring for and destruction of rogue personal data eliminates attack vectors
- Tools like Orca Security monitor this in real-time, with full-scope governance
- DevOps can target, and destroy



# Tips from the Field - Lateral (diagonal?) Breach

## Once a perimeter is broken, lateral breach tends to be much, much easier

- Everyone knows this
- Almost no one has an effective east-west ZTN with port-level granularity control. They do exist, though, and are bad-ass

## Cross-cloud, cross-SaaS, breach

- In a ZTN world, lateral breach has new meaning
- Using different techniques, a breach into one asset makes breaching other zero-trust assets easier

## Mature-company solutions

- Monitor for stored SaaS and cloud credentials in infrastructure assets
- Don't skimp on the SSO tax
- Enforce MFA on those cloud accounts



# Tips from the Field - Improve Password Strength

**10 character minimum, 1 of these (#!'^~--~\$Я), none of these (\$?\*%), etc**

- Neat
- Complex password or password complexity?

## **What is a weak password?**

- One that I can guess. One that I can find in a hash table. One that has been breached
- I maintain my own breach database with over 25 billion rows

## **How are passwords discovered by hackers?**

- Querying breach databases for unique user identifiers to see what passwords they've used
- Hashed password searches - finding similar users and correlating metadata to guess
- Breaching email accounts with known passwords and resetting unknown passwords
- Hash-table lookups
- Cracking - I assume is still a thing?

# PRODUCT DEMO



# Q&A

Don't forget to sign up for an Orca Demo  
and Free Trial at <https://orca.security/demo>



**Moderator**

**Charlene O'Hanlon**

**Managing Editor  
Security Boulevard**



**Jack Roehrig**

**CISO  
Turnitin**



**Patrick Pushor**

**Technical Evangelist  
Orca Security**