Qualys.
ROCon 25
The Risk Operations Conference
APAC

Perimeters are so 2015

Expanding Risk Operations with **Identity Context**

Himanshu Kathpal
Vice President, Product Management,
Platform and Technologies

Agenda

Qualys. ROCon 25
The Risk Operations Conference
APAC

01 Identity is INDEED the new perimeter

02 Why identity exposures break risk operations

03 Introducing Qualys ETM Identity

04 ETM Identity Use Cases and Outcomes

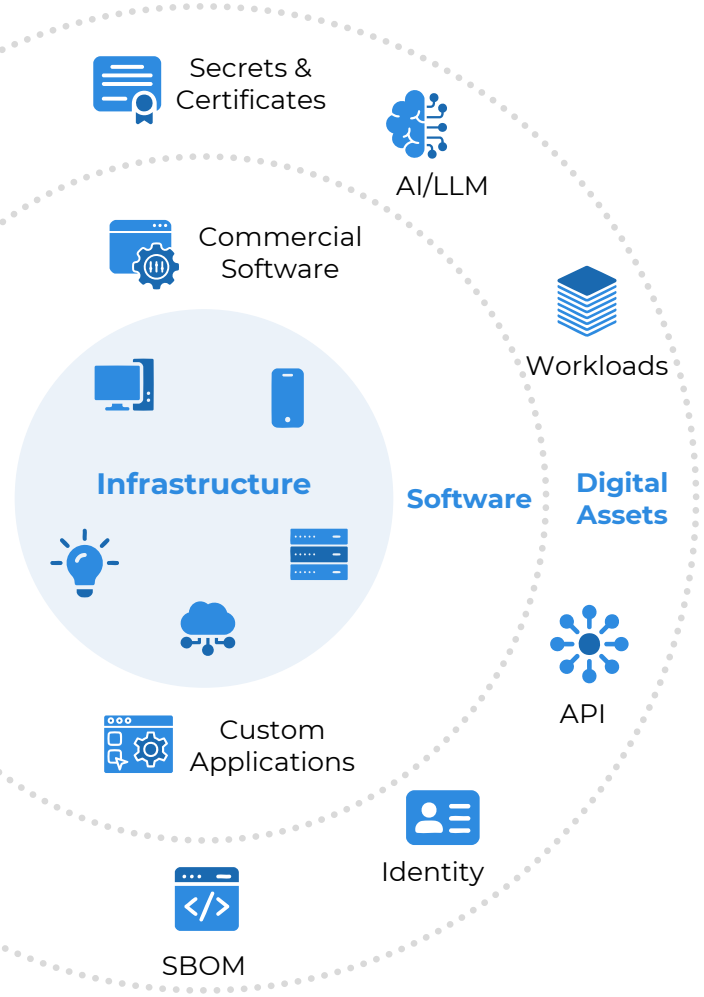
05 Demo

06 Industry leader, Ashish Bapana's experience for ISPM Solutions

Rapidly Expanding Identity Attack Surface

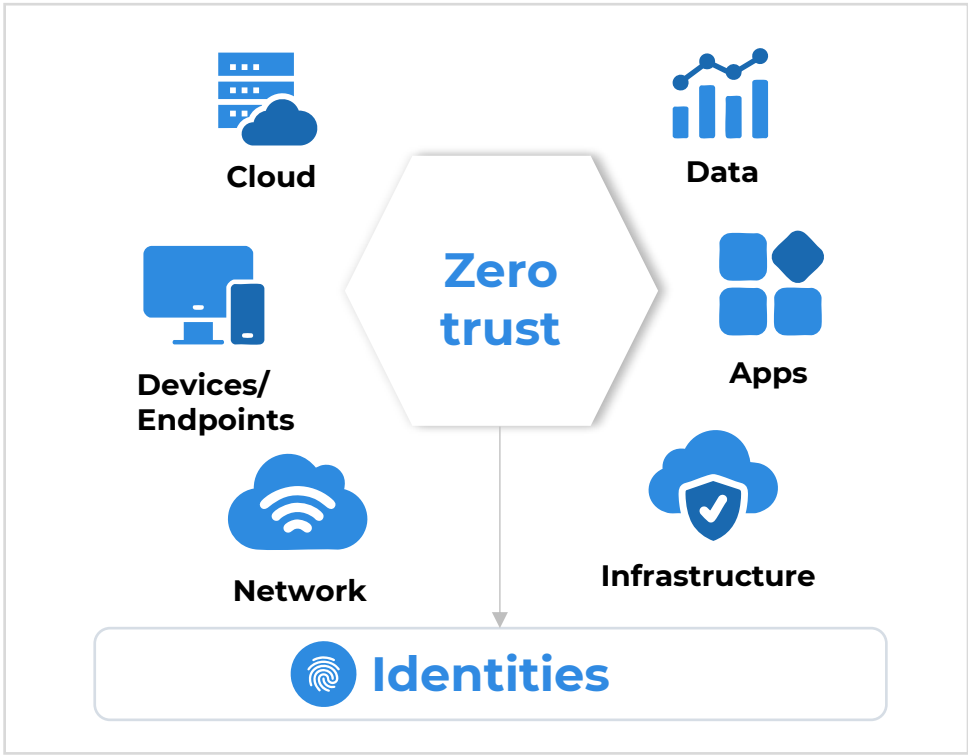
Qualys. ROCon 25 The Risk Operations Conference APAC

From Cloud to SaaS to IoT: Each Login Adds to Risk



Accelerated cloud adoption

Rise of SASE & ZTNA



Qualys.
ROCon 25
The Risk Operations Conference
APAC

Identity is INDEED the new perimeter

It's 2025, cybercriminals don't hack, they login

~80% of breaches involve credentials abuse

Threat actors now favour phishing, guessing, scraping, or buying credentials.

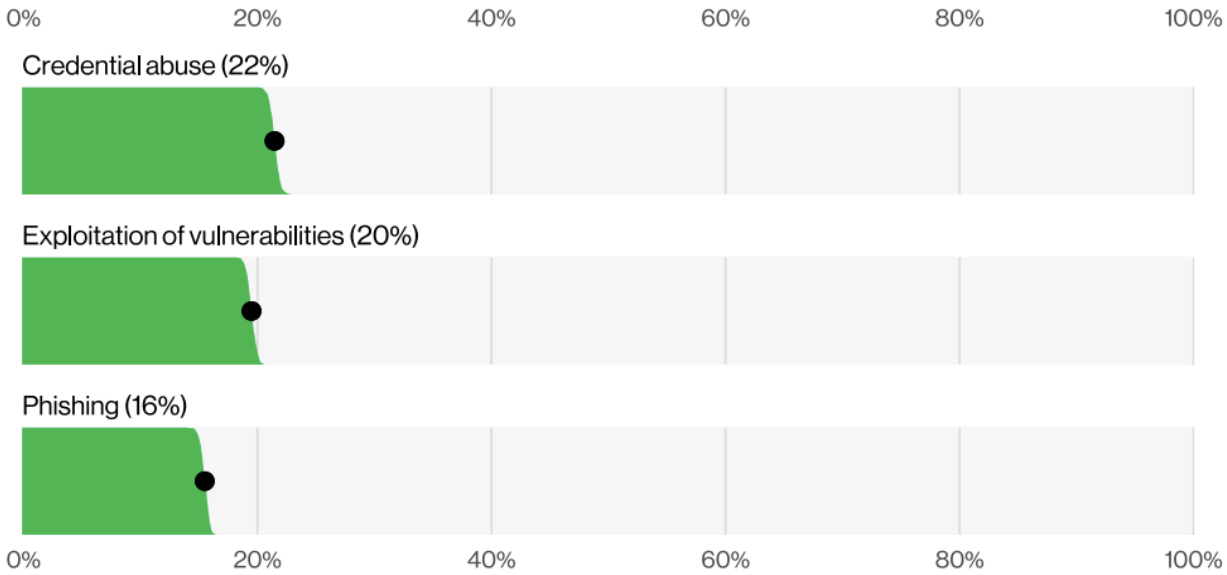
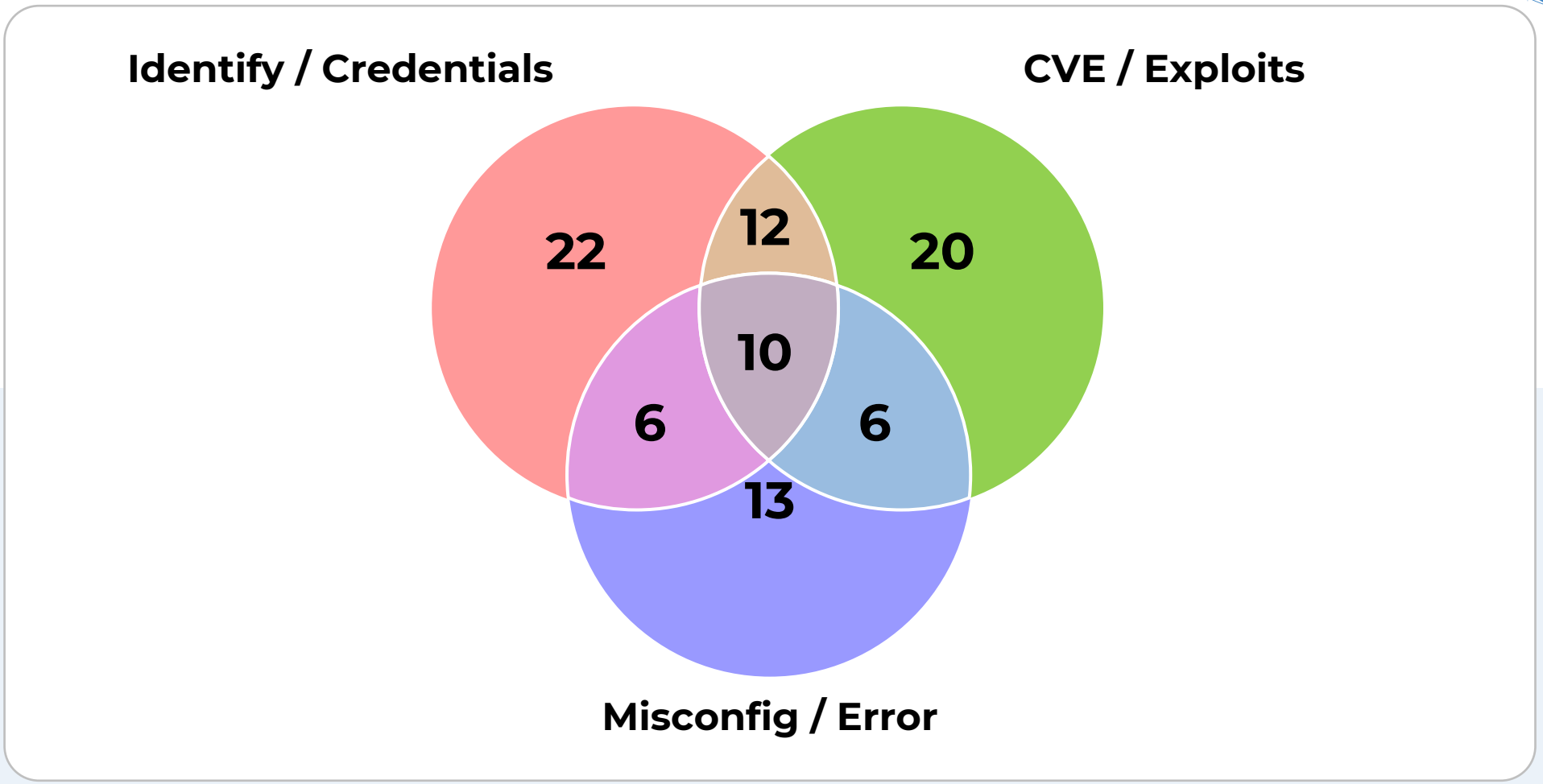


Figure 1. Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

2025 Verizon Data Breach Investigations Report

Hybrid attack vectors rule the roost

34% of the breach vectors are combination of Identity weaknesses, CVEs, & Misconfigs.



Modeled Overlap of Breach Vectors (DBIR 2025 + M-Trends 2025)

Stolen creds + missing MFA = terabytes & millions of $$$ out the door

Qualys. ROCon 25
The Risk Operations Conference
APAC

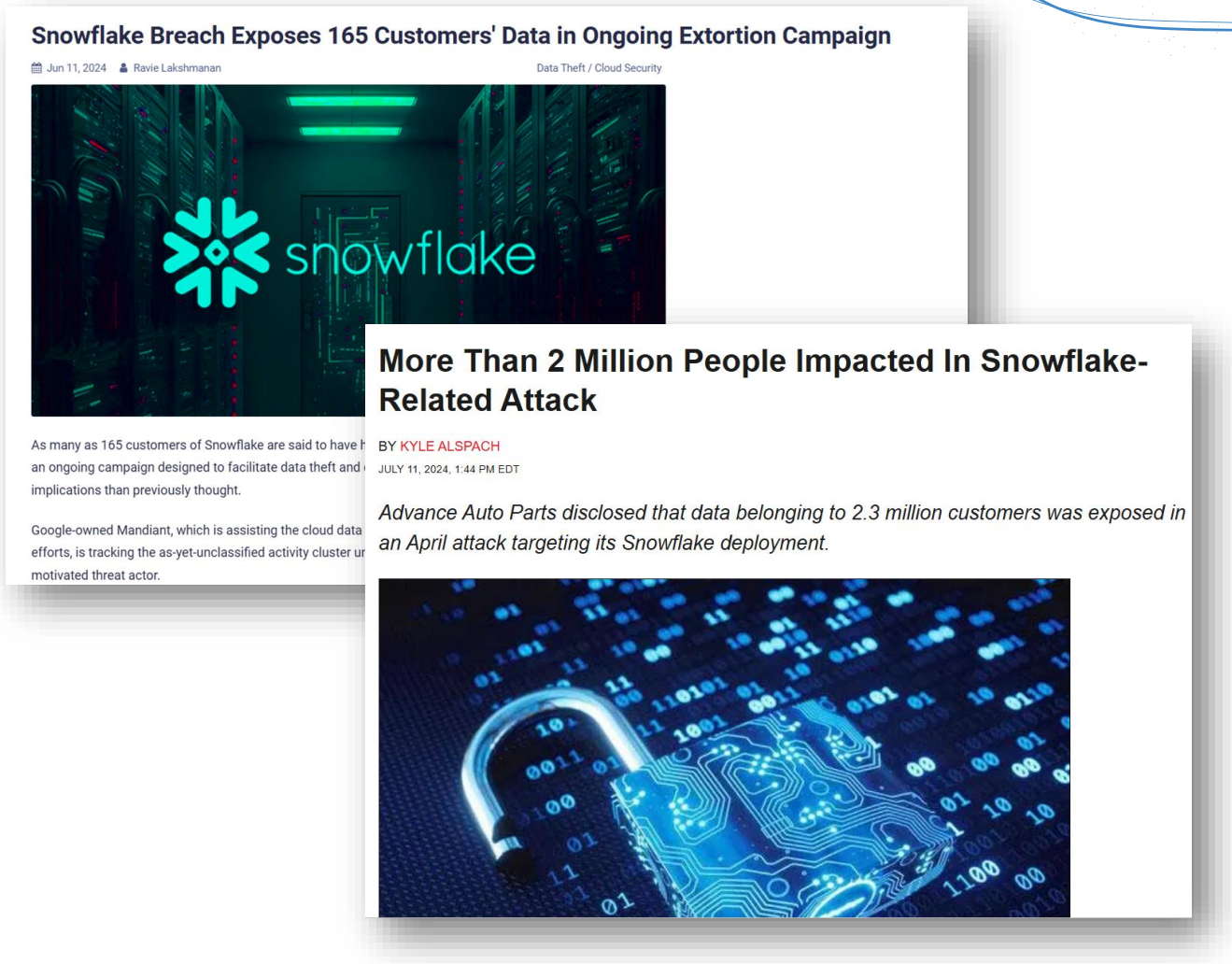
Snowflake: A watershed moment in cybersecurity industry

Failure mode

- Info-stealer creds
- Password reuse
- No MFA on **Snowflake customer accounts**

Business Impact

- At-least **165 orgs** targeted
- Extortion ($0.3B-$1B)
- Massive data exfiltration (Ticketmaster, Santander, others)



Snowflake Breach Exposes 165 Customers' Data in Ongoing Extortion Campaign

Jun 11, 2024 Ravie Lakshmanan Data Theft / Cloud Security

As many as 165 customers of Snowflake are said to have h
an ongoing campaign designed to facilitate data theft and
implications than previously thought.

Google-owned Mandiant, which is assisting the cloud data
efforts, is tracking the as-yet-unclassified activity cluster u
motivated threat actor.

More Than 2 Million People Impacted In Snowflake-Related Attack

BY KYLE ALSPACH

JULY 11, 2024, 1:44 PM EDT

Advance Auto Parts disclosed that data belonging to 2.3 million customers was exposed in an April attack targeting its Snowflake deployment.

Why identity exposures break risk operations

Qualys. ROCon 25 The Risk Operations Conference APAC

- AD/Entra is the **core of blast radius**.
- Compromise means **persistence**, not entry.
- Identity sprawl is messy and creates **toxic combinations**.
- **Weaponizing exposures** has never been easier.

No identity risk **visibility**

Identity & asset risks **siloed**

Ambiguity in ownership

Lack of **audit trail**

Qualys ROCon 25
The Risk Operations Conference
APAC

Introducing

Qualys ETM Identity

Consolidates identity posture across your attack surface to ***measure***, ***communicate***, and ***eliminate*** identity risks.

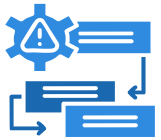
Operationalize Identity Risk Reduction

The loop every Risk Operations Center (ROC) needs for Identity Security

Qualys. ROCon 25 The Risk Operations Conference APAC





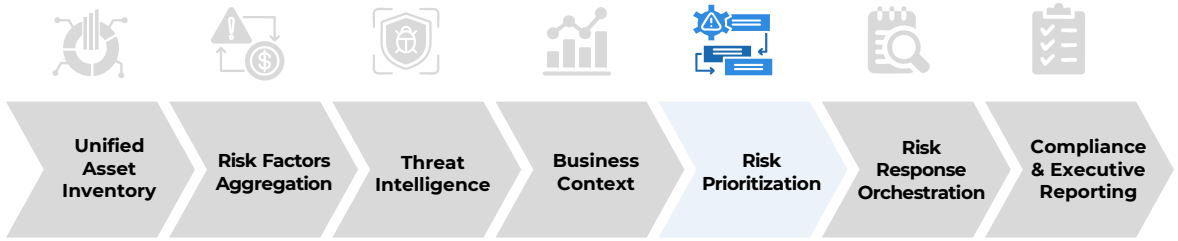


Unified Asset Inventory	Risk Factors Aggregation	Threat Intelligence	Business Context	Risk Prioritization	Risk Response Orchestration	Compliance & Executive Reporting
• Active Directory (AD) • Microsoft Entra ID • Okta • Ping Identity	• Qualys Agent (AD) • Native IdP/IDaaS Connector (Entra ID, Okta, Ping) • 3rd Party Tools (SailPoint, BloodHound, etc.)	25+ threat intelligence feeds including Qualys Live TI, MITRE ATT&CK, Talos, McAfee, CISA KEV, EPSS	• ServiceNow CMDB • BMC Helix CMDB • Qualys ETM Business Value / Risk Appetite / VAR	• Identity TruRisk™ • Identity Insights • Attack Path Analysis	• TruRisk™ Eliminate • AD Policy Controls • ITSM Workflows • Identity Actions • Custom playbooks • Integrity Monitoring	Audit-ready executive reporting DISA STIG, CIS M365 & more

How will you be

ROC Ready from Day 1

For Your Identity Infrastructure



Qualys. ROCon 25
The Risk Operations Conference
APAC

Microsoft Entra ID
okta
WIZ
SPECTEROPS
Creators of BloodHound
Quest
tenable

500K
ALL IDENTITIES

10k (2%)
Risky Identities

98% Reduction

1.2k (<1%)
Business context and asset context

99% Reduction

THREAT INTELLIGENCE

Weak policies (credentials, MFA etc.), External exposure of credentials, Excessive privileges creating attack paths to crown jewels

ASSET CONTEXT

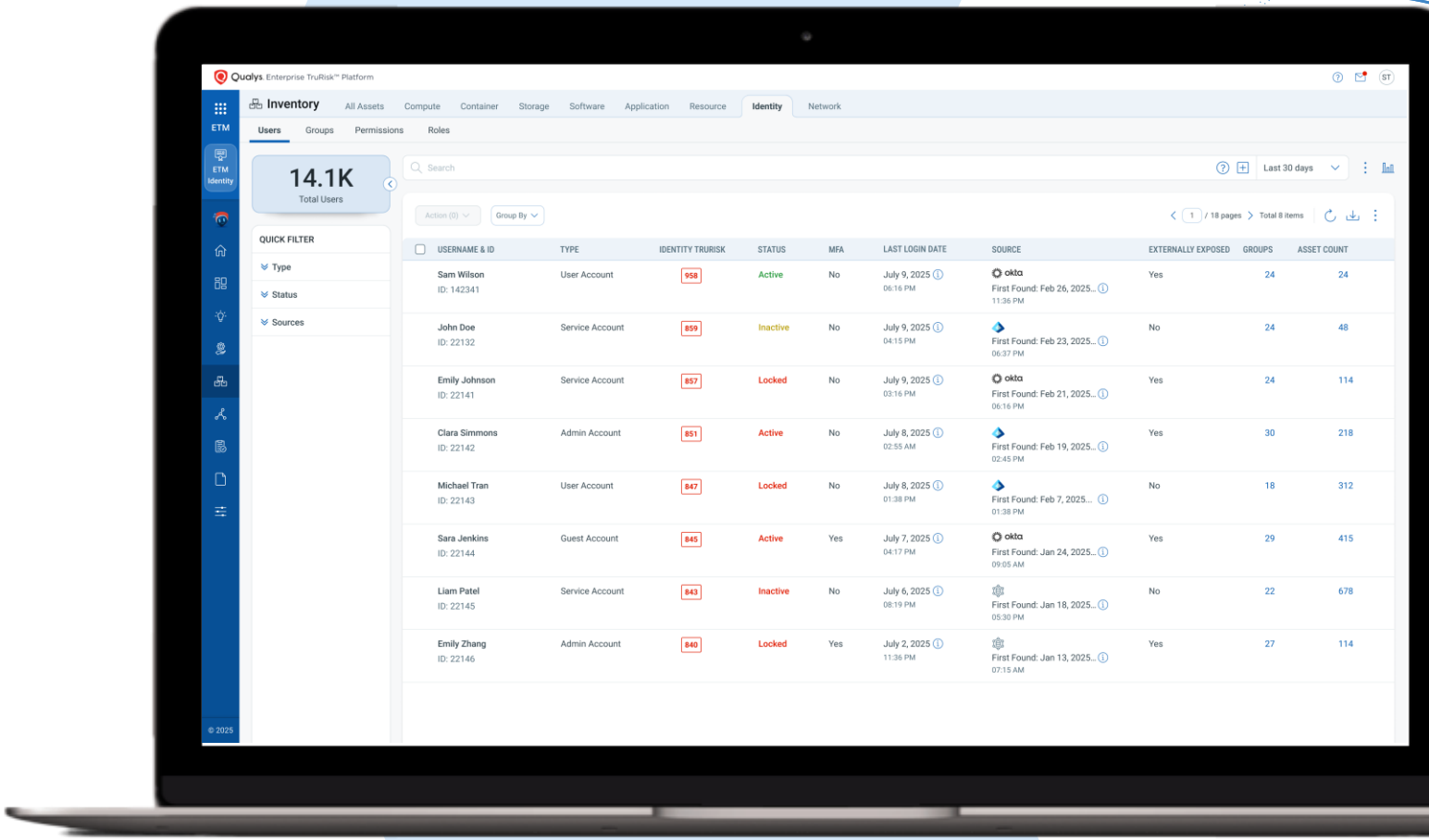
Business criticality of Identities (privileged identities), Asset vulnerabilities and misconfigs connected to these Identities

Qualys ROCon 25
The Risk Operations Conference
APAC

Unified Asset Inventory | Risk Factors Aggregation | Threat Intelligence | Business Context | Risk Prioritization | Risk Response Orchestration | Compliance & Executive Reporting

Comprehensive visibility across AD, Entra ID, IdPs, IDaaS, PAM

- Collect human/machine identities with attributes, memberships, tokens, keys.
- Classify externally exposed identities, guest users, shadow admins and infra.
- Manage tech-debt from EOL/EOS, unauthorized packages, baselines.
- Map ownership & lineage with versioned inventory for audit and Zero Trust.

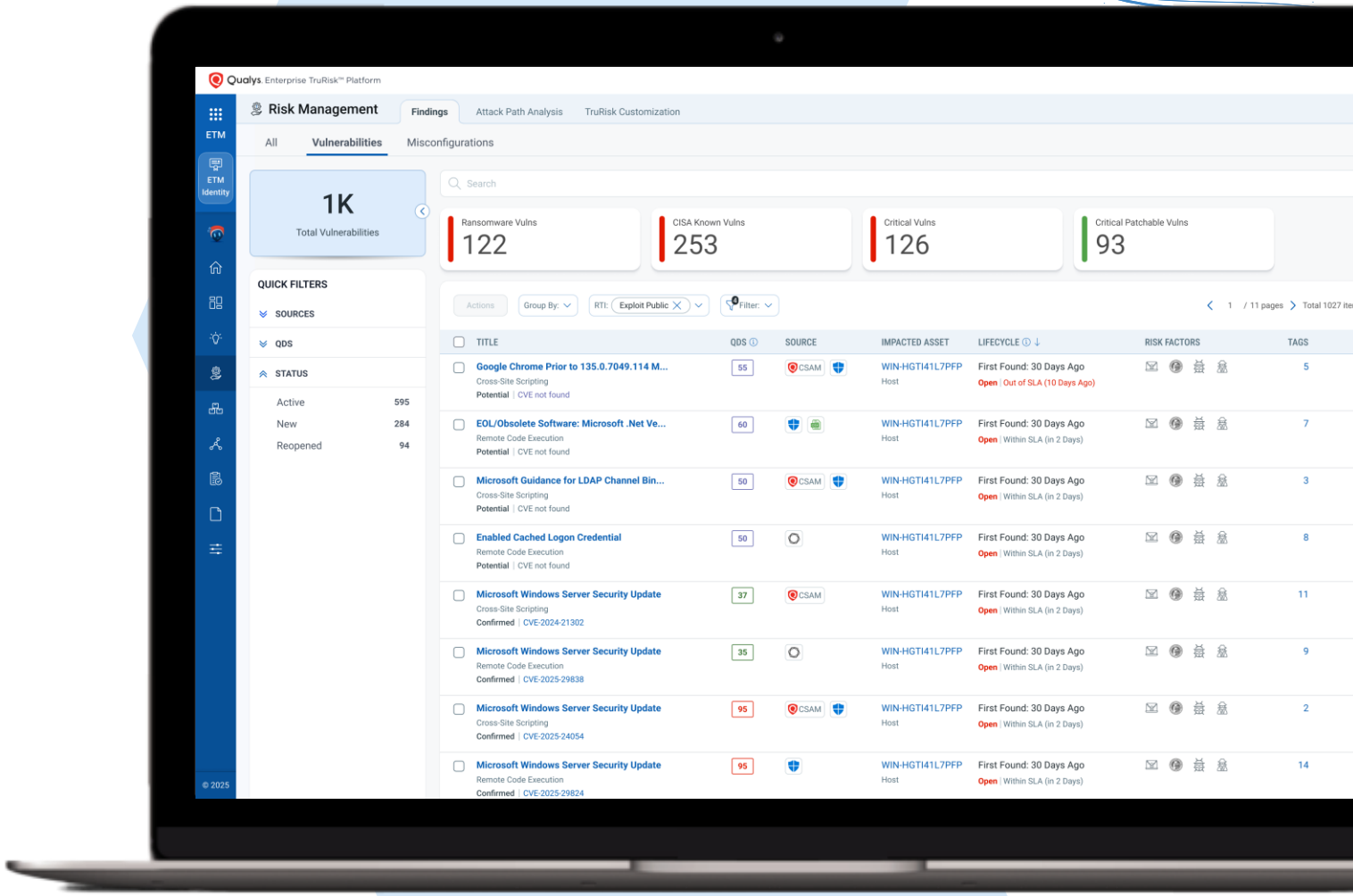


Qualys ROCon 25
The Risk Operations Conference
APAC

Unified Asset Inventory | Risk Factors Aggregation | Threat Intelligence | Business Context | Risk Prioritization | Risk Response Orchestration | Compliance & Executive Reporting

Unify identity posture into a single cyber-risk view with Agentic AI

- Detect CVEs, misconfigs, IORs via prebuilt scripts.
- Ingest 3rd-party findings (BloodHound, PingCastle, IdP/IDaaS exports).
- Dedupe, enrich signals with **25+ threat-intel and directory sources.**
- Assess against DISA STIG, CIS M365, and Zero-Trust controls.

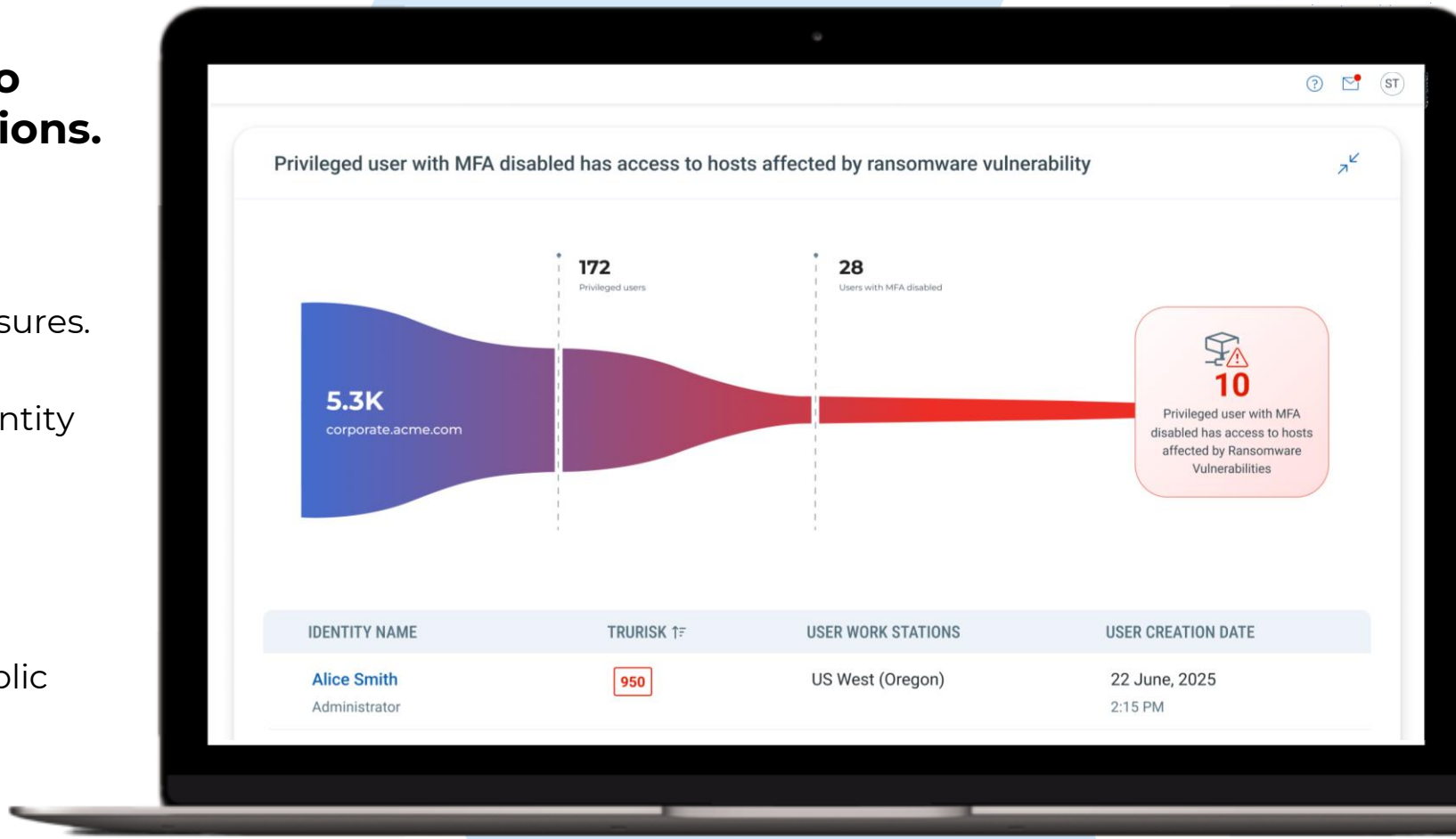


Unified Asset Inventory | Risk Factors Aggregation | Threat Intelligence | Business Context | **Risk Prioritization** | Risk Response Orchestration | Compliance & Executive Reporting

Qualys. ROCon 25
The Risk Operations Conference
APAC

Convert identity risk signals into prioritized, business-impact actions.

- Correlate privileged users, MFA gaps, stale/service accounts with asset exposures.
- Surface toxic combinations linking identity and asset risks for next best action.
- Actionable insight cards
  - Privileged user without MFA on zero-day hosts
  - Admin with weak password on public webservers.

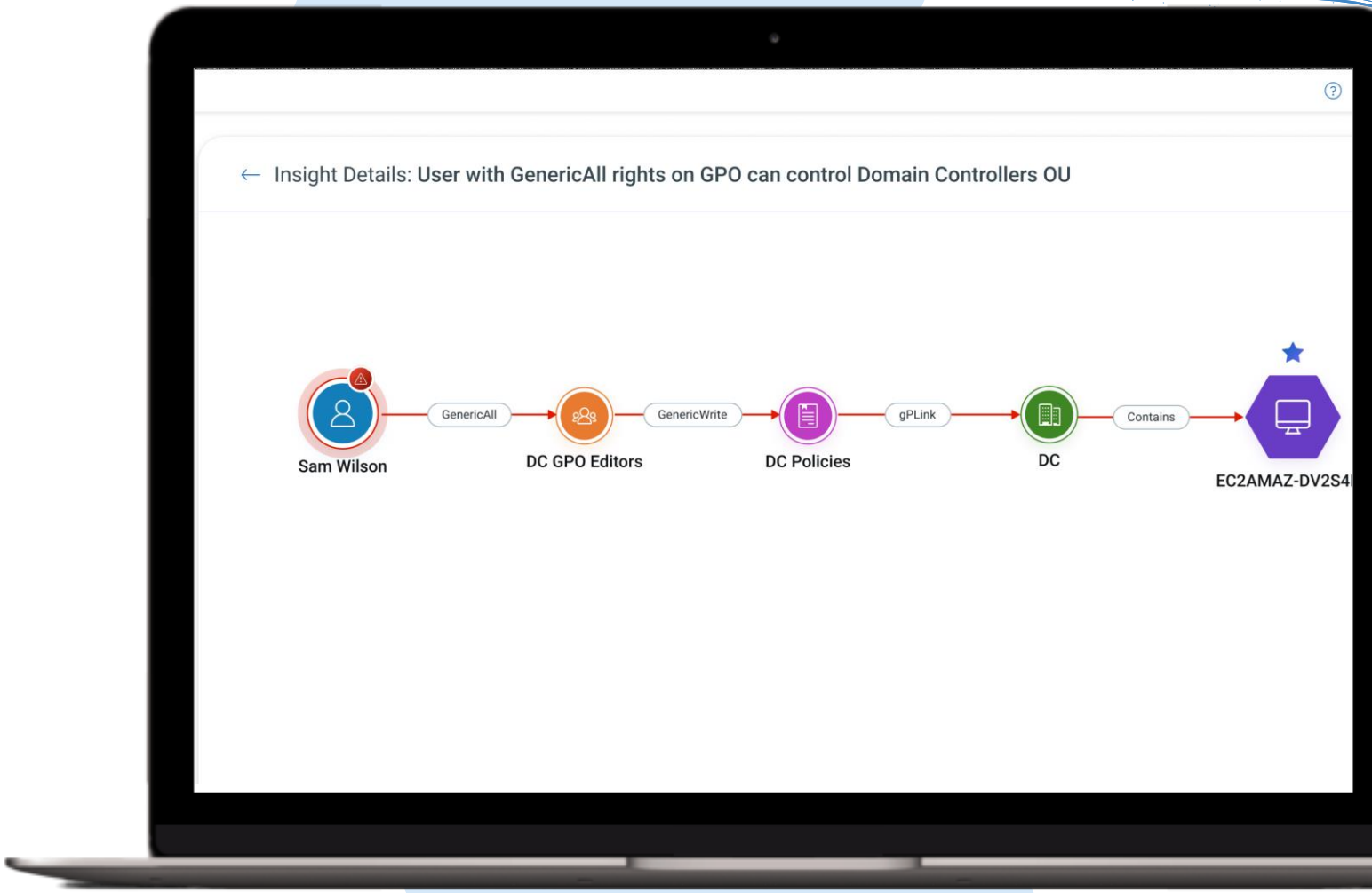


Unified Asset Inventory | Risk Factors Aggregation | Threat Intelligence | Business Context | Risk Prioritization | Risk Response Orchestration | Compliance & Executive Reporting

Qualys. ROCon 25
The Risk Operations Conference
APAC

Expose hidden AD relationships and lateral routes to prioritize attack paths.

- Visualize privileges, GPO influence, cross-domain hops to find exploitable paths
- Protect Crown Jewels by focusing on highest-impact routes.
- One-click fixes (remove rights, enforce MFA, disable/quarantine) with verification.
- Rank paths by Identity TruRisk™, asset criticality, and tech debt.

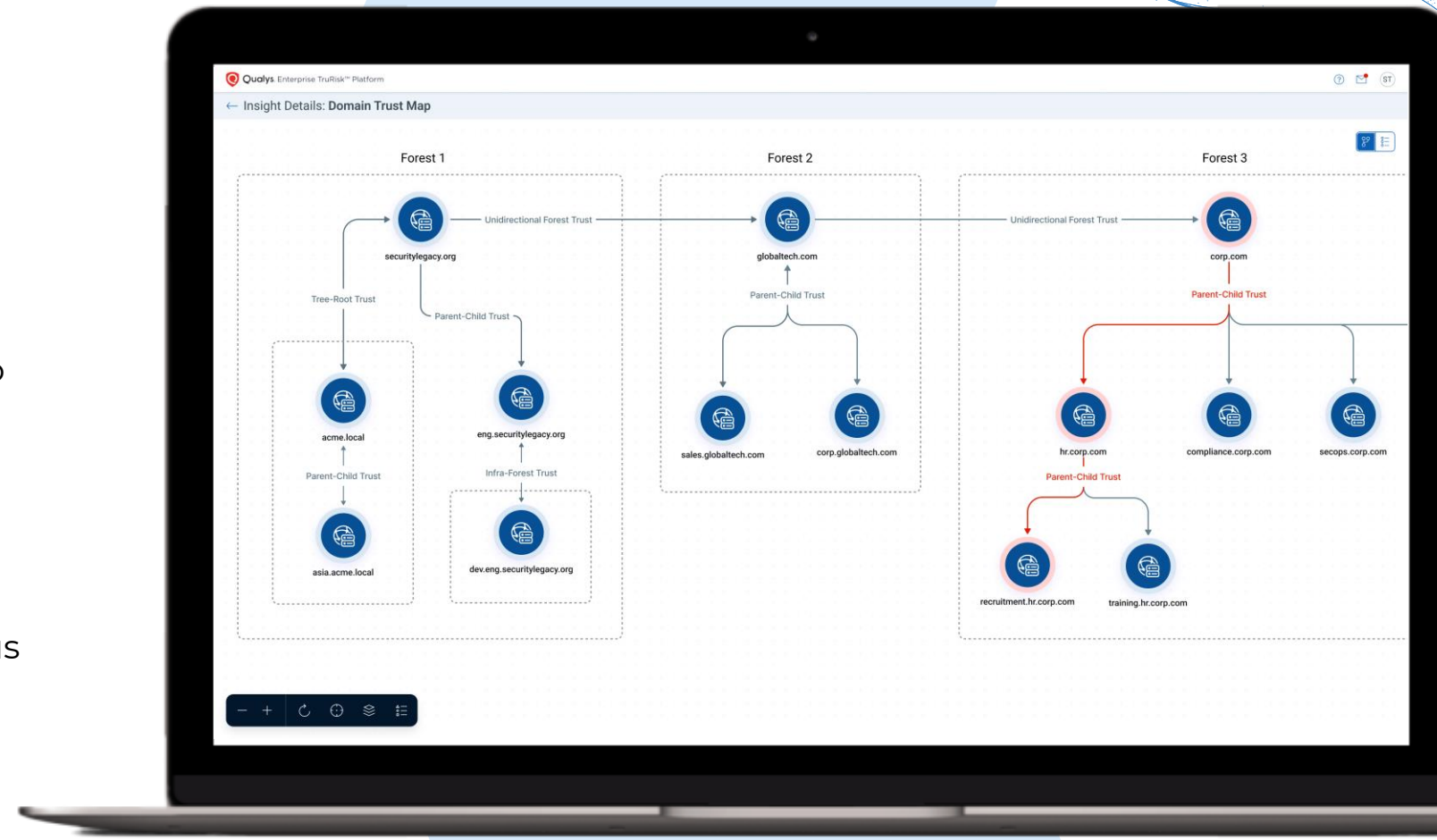


Unified Asset Inventory | Risk Factors Aggregation | Threat Intelligence | Business Context | Risk Prioritization | Risk Response Orchestration | Compliance & Executive Reporting

Qualys ROCon 25
The Risk Operations Conference
APAC

Detect hidden AD lateral paths and harden inter-domain/forest trusts to block easy traversal

- Map forests, domains, and trust types to spot risky trusts.
- Expose Tier-0/DC routes by correlating trusts with privilege paths.
- Rank weak trusts to collapse blast radius fast with one-click fixes.



Qualys. ROCon 25
The Risk Operations Conference
APAC

Unified Asset Inventory | Risk Factors Aggregation | Threat Intelligence | Business Context | **Risk Prioritization** | Risk Response Orchestration | Compliance & Executive Reporting

Sam Wilson

5 ICS

+100 **Identity misconfiguration**

+100 **Over Privileges**

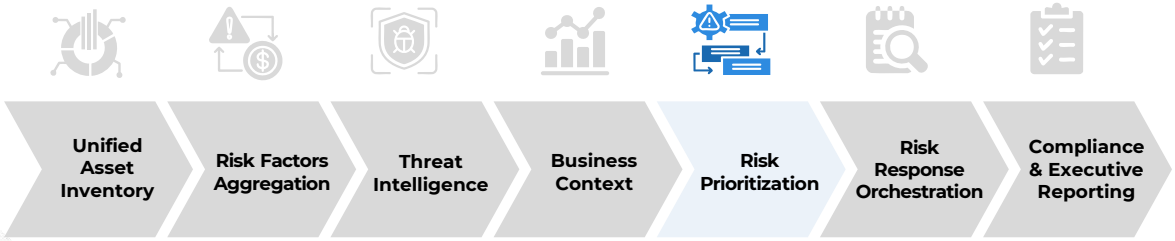
+100 **Cross Path and Attack path**

+200 **Externally Exposed**

IMMUNITY · REVERSING LABS · GREYNOISE INTELLIGENCE · CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY · McAfee · VDE · MITRE ATT&CK · GitHub · MISP Threat Sharing · PZ PROJECT ZERO · CANADIAN CENTRE FOR CYBER SECURITY · Square Security · metasploit · Kaspersky Industrial CyberSecurity · Google · EPSS · TALOS · packet storm · FIREEYE

950

Critical



Qualys. ROCon 25
The Risk Operations Conference
APAC

345

Low

TruRisk™ Score

+220

- Vulnerabilities
- Misconfigurations
- Identities

+110

- Internet Facing

+210

- Business critical/PCI or sensitive data
- No EDR Present

885

Critical

TruRisk™ Score

Unified Asset Inventory | Risk Factors Aggregation | Threat Intelligence | Business Context | **Risk Prioritization** | Risk Response Orchestration | Compliance & Executive Reporting

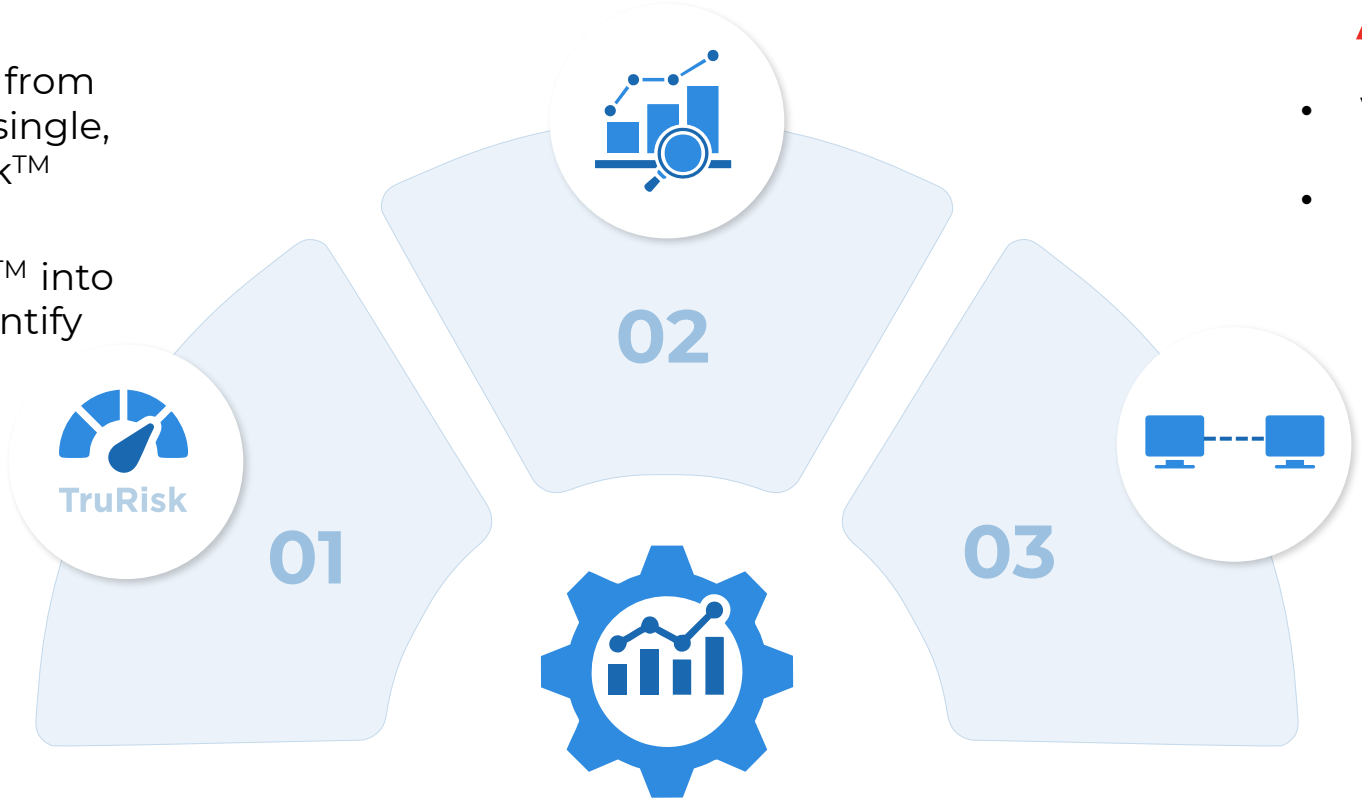
Qualys. ROCon 25
The Risk Operations Conference
APAC

Identity Insights

- Correlate signals from tech-debt
- Calculate toxic combinations of asset risks and identity risks

Identity TruRisk™

- Integrates identity risks from multiple sources into a single, intuitive Identity TruRisk™ score for each user
- Roll up Identity TruRisk™ into overall TruRisk™ to quantify risk in business terms



Attack Paths

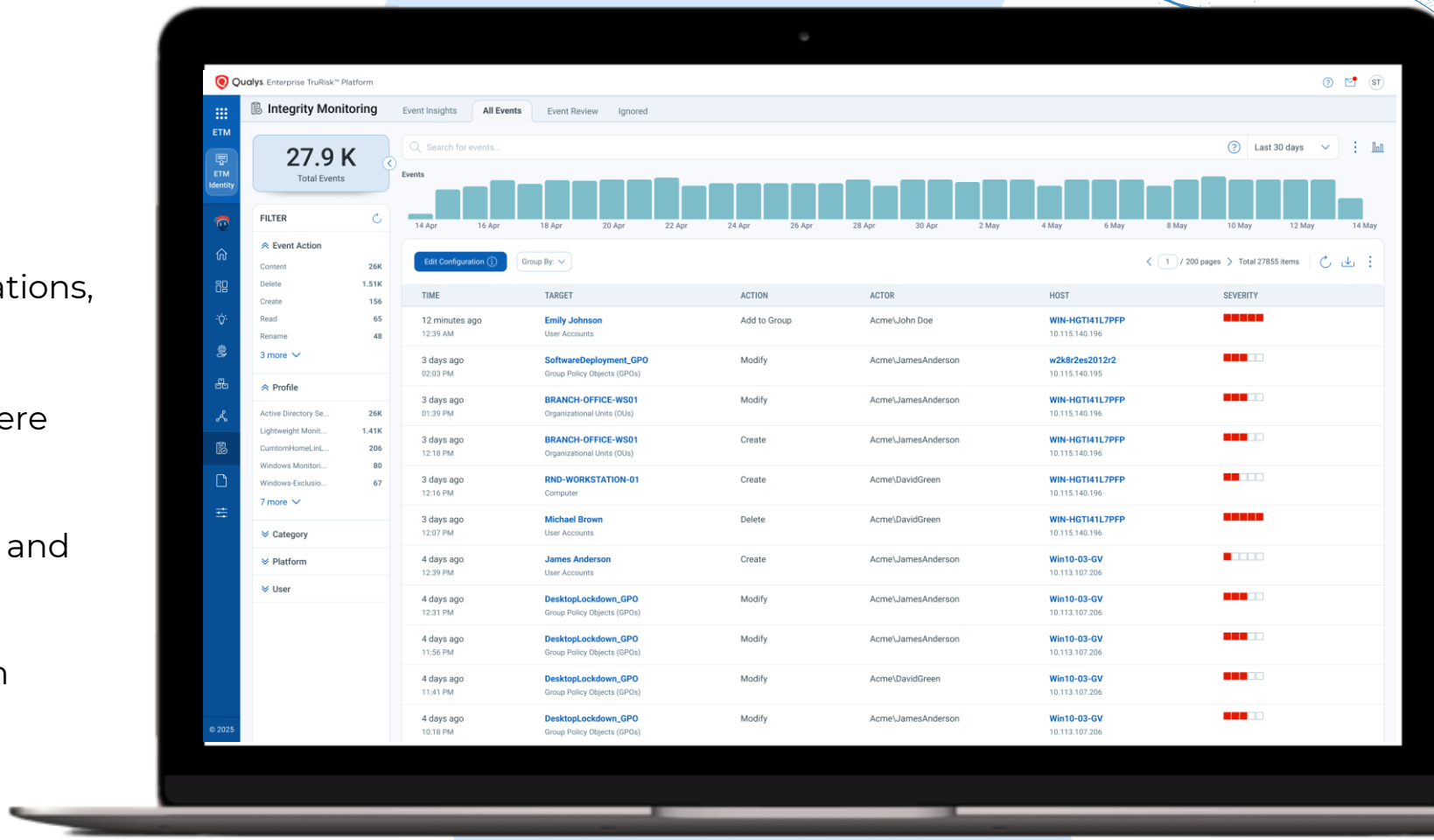
- Visualize attack paths and prioritize based on TruRisk™.
- Understand blast radius impact of key accounts

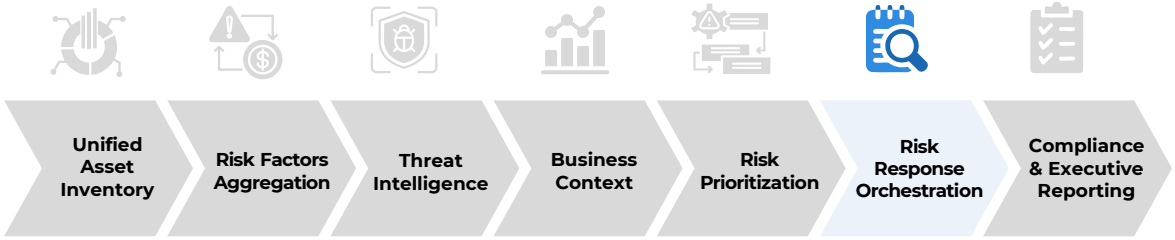
Qualys ROCon 25
The Risk Operations Conference
APAC

Unified Asset Inventory | Risk Factors Aggregation | Threat Intelligence | Business Context | Risk Prioritization | Risk Response Orchestration | Compliance & Executive Reporting

Real-time identity change detection with attribution, forensics, and audit trail.

- Monitor AD objects for privilege escalations, MFA disablement, policy tampering.
- Record who changed what, when, where across AD objects/registry/schema.
- Event-driven alerts reduce dwell time and speedy response.
- Audit trail of changes and remediation actions for compliance.





Qualys. ROCon 25
The Risk Operations Conference
APAC

Identity Actions

One-click actions: disable/quarantine, enforce MFA, reduce privileges, remove toxic rights.

Customize for your needs

Build custom controls & playbooks with CAR, aligned to approvals.

Isolate

Quarantine devices/accounts; allow only trusted apps until risk is removed.

01

Patch + Fix

Remediate identity vulnerabilities & misconfigurations with 200+ AD controls & scripts.

02

03

Mitigate

Use policy hardening & compensating controls when patching isn't feasible.

04

05

ITSM Workflows

Scale via SNOW/Jira (auto-open/advance/close) with evidence.

06

07

Validate & Re-score

Confirm fixes, update Identity TruRisk™, roll into org TruRisk™.

One solution for unified identity risk management

Qualys. ROCon 25
The Risk Operations Conference
APAC

De-risk human and machine identities for reduced identity-driven attack surface

Cut tool sprawl with unified risk telemetry into a single view for frictionless risk orchestration

Make faster decisions with one risk language for board-ready prioritization.

Eliminate the most exploitable attack paths first using closed-loop remediation.

Qualys. ROCon 25
The Risk Operations Conference
APAC

Let's take a closer look with a demo

Qualys ETM Identity

Qualys ROCon 25
The Risk Operations Conference
APAC

Scan QR Code for a no-cost 30-day trial.

Learn more **qualys.com /identity**

Scan QR code and get early access

Talk to our experts for **personalized consultation**.

Qualys.
ROCon 25
The Risk Operations Conference
APAC

LTIMindtree

Enterprise Identity Concerns

Ashish Bapana
Sr. Manager, CyberSecurity

LTIMindtree

Qualys. ROCon 25
The Risk Operations Conference
APAC

Ashish Bapana

Sr. Manager

Cyber Security

3+ years at LTIMindtree

Extensive experience across spectrum of IT and CyberSecurity

- 8+ years of experience in Cyber Security Domain
- ~12 years of experience in IT.

LTIMindtree

Qualys. ROCon 25
The Risk Operations Conference
APAC

November 2022

Mumbai, India
Headquarters

85,000
Employees

Our purpose:

Build Future, Faster, Together

One of the fastest growing CyberSecurity practice.

Active Directory Security

LTIMindtree

Qualys. ROCon 25
The Risk Operations Conference
APAC

AD Concerns

- Passwords remain a weak link
- Active directory service accounts
- Excessive Permissions
- Active Directory Certificate Security

Clouds Everywhere

Multi-Cloud Hybrid Environments

- **Multiple Identity Stores**
- **Independent On-Prem and Cloud IDP**
- **Lack of a holistic offering**

Cyber Security Compliance

LTIMindtree

Qualys. ROCon 25
The Risk Operations Conference
APAC

Name your regulation or favorite acronym

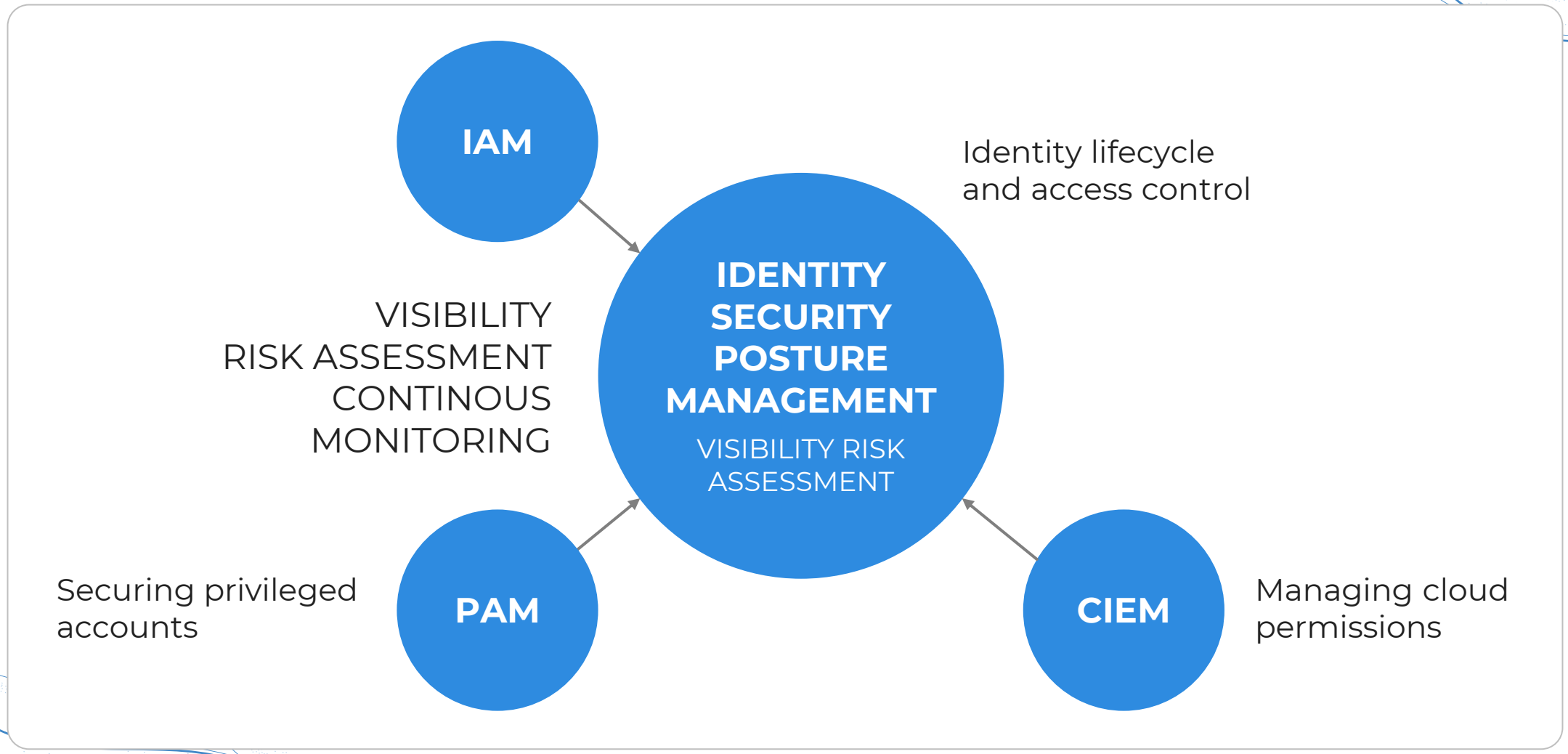
Constantly changing and new regulations

While necessary it does add a lot of burden

Similar controls across key regulations (HIPPA, SOC 2, Etc.)

- Strong authentication
- Access controls
- Password management
- Least privilege

How ISPM fits into Identity Security ecosystem



What Do We Need

LTIMindtree

Qualys. ROCon 25 The Risk Operations Conference APAC

Coverage against misconfigurations in cloud IDS solutions

Monitor active directory in real time for suspicious configuration changes

Establish comprehensive KRI measures

Clearly and transparently prioritize identity-related security weaknesses

A complete approach to identity security as part of overall risk management.

LTIMindtree

Qualys. ROCon 25
The Risk Operations Conference
APAC

Ashish Bapane

Sr. Manager
LTIMindtree

www.linkedin.com/in/ashishbapana/

www.ltimindtree.com

Scan Here

Qualys®

ROCon 25

The Risk Operations Conference

APAC