Qualys
ROCon 26
The Risk Operations Conference
EMEA

AI Risk: Don't Fall Behind

Work differently, not harder.



Qualys ROCon 26
The Risk Operations Conference
EMEA



Dilip Bachwani
CTO & EVP



Andrew Nelson
Senior Security
Solutions Architect

AI Is Everywhere. And Most of It Is Invisible.

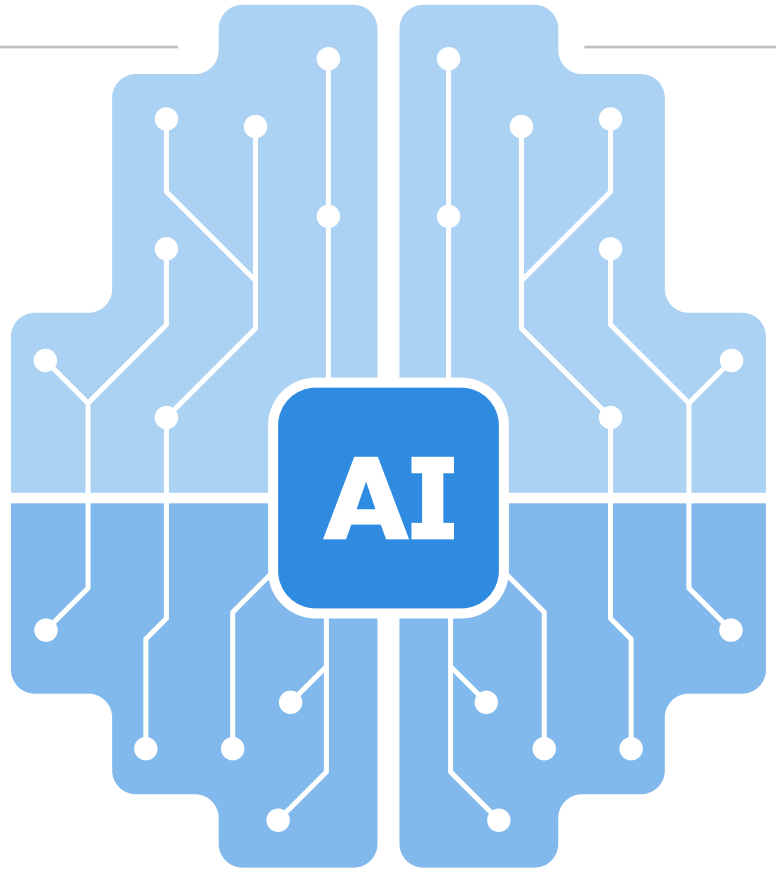
Qualys ROCon 26 The Risk Operations Conference EMEA

Workforce

- ChatGPT, Copilot, Gemini in daily use
- Shadow AI — unapproved tools, personal accounts
- Sensitive data leaking through prompts
- No visibility into usage or policy compliance

Developers

- AI coding assistants (Copilot, Cursor, Claude)
- Auto-generated PRs bypassing review
- AI embedded in CI/CD pipelines
- Vulnerable patterns in generated code



Workload

- GPU clusters & ML infrastructure sprawl
- Public-facing model serving endpoints
- Unpatched AI frameworks & runtimes
- Misconfigured model APIs & storage

Dev & Pipeline

- AI-generated code shipping to production
- Untrusted ML pipeline dependencies
- Poisoned training data in public datasets
- Model supply-chain risk in registries

The Visibility Gap Widens Every Day

From Chat to Autonomous

Enterprise AI evolved faster than any technology before it — and each wave extended the attack surface.

Qualys ROCon 26 The Risk Operations Conference EMEA

WAVE 01

2022 - 2023

LLMs Alone

- Chat, content, summarization
- Closed-box: only trained knowledge
- Prompts in, text out

Low blast radius.
Data leakage in prompts.

WAVE 02

2023 - 2024

RAG — Extended With Your Data

- Vector DBs, embeddings, retrieval
- LLMs see data they were never trained on
- Your corpora + the model

Sensitive data exposed.
Corpora poisoned.

WAVE 03

2024 - NOW

Agentic — Action, Not Just Answers

- Tools, MCP, orchestration
- LLMs call APIs, execute code, move money
- Model + data + your systems

Prompt → Action.
Blast radius = production.

WAVE 04

2026

Autonomous AI

- Finds zero-days independently
- Thousands of vulns across every major OS & browser

The model hunts on its own. — Anthropic Mythos, April 2026

"The model didn't just reach further. It started hunting on its own."

Your AI Footprint Is Public. Are You Looking at It?

Qualys ROCon 26 The Risk Operations Conference EMEA

~100,000

"Nearly 100,000 attack sessions targeted public LLM endpoints in a single campaign — with the explicit goal of mapping enterprise AI deployments before launching follow-on attacks."

— GreyNoise, January 2026



What's Exposed

- Public-facing LLM endpoints
- Model version fingerprints
- Open inference APIs
- Training data artifacts
- Shadow AI SaaS integrations

How Attackers See It

- Shodan & Censys scanning for ML ports
- Prompt injection probes at scale
- API enumeration via fuzzing
- Model extraction attempts
- Supply-chain dependency mapping

Why It Matters

- AI footprint = attack surface
- Most orgs don't know what's exposed
- Attackers map before they strike
- Recon is automated & continuous
- You can't protect what you can't see

New Fuel. Same Fire.

Qualys ROCon 26
The Risk Operations Conference
EMEA

PyPI → K8s → Backdoor

LiteLLM, a widely-used AI proxy package, was compromised on PyPI. Malicious code deployed a three-stage payload: credential harvesting, Kubernetes lateral movement, and a persistent backdoor for remote code execution.
The attack chain was traditional supply-chain poisoning — but the target was AI infrastructure middleware.

— LiteLLM supply-chain compromise, March 2026 (Trend Micro)

Before AI	Phase	After AI
Manual OSINT, Google dorking, LinkedIn scraping	**Reconnaissance**	AI-driven target profiling, automated social graph mapping, synthetic identity research
Generic phishing, bulk credential stuffing	**Initial Access**	Hyper-personalized spear phishing, deepfake voice/video, AI-crafted pretexting
Known CVEs, manual exploit adaptation	**Exploitation**	AI-generated exploit variants, polymorphic payloads, prompt injection chains
Static C2, scheduled tasks, manual exfil	**Persistence & Exfil**	Adaptive C2 with LLM-driven evasion, automated data classification & exfil prioritization

AI Risk is Outrunning Your Defenses

Qualys ROCon 26
The Risk Operations Conference
EMEA

Risk surface growing faster than inventory

New AI assets deploy daily — shadow AI, model endpoints, GPU workloads — while asset inventory updates quarterly. The gap widens every sprint.

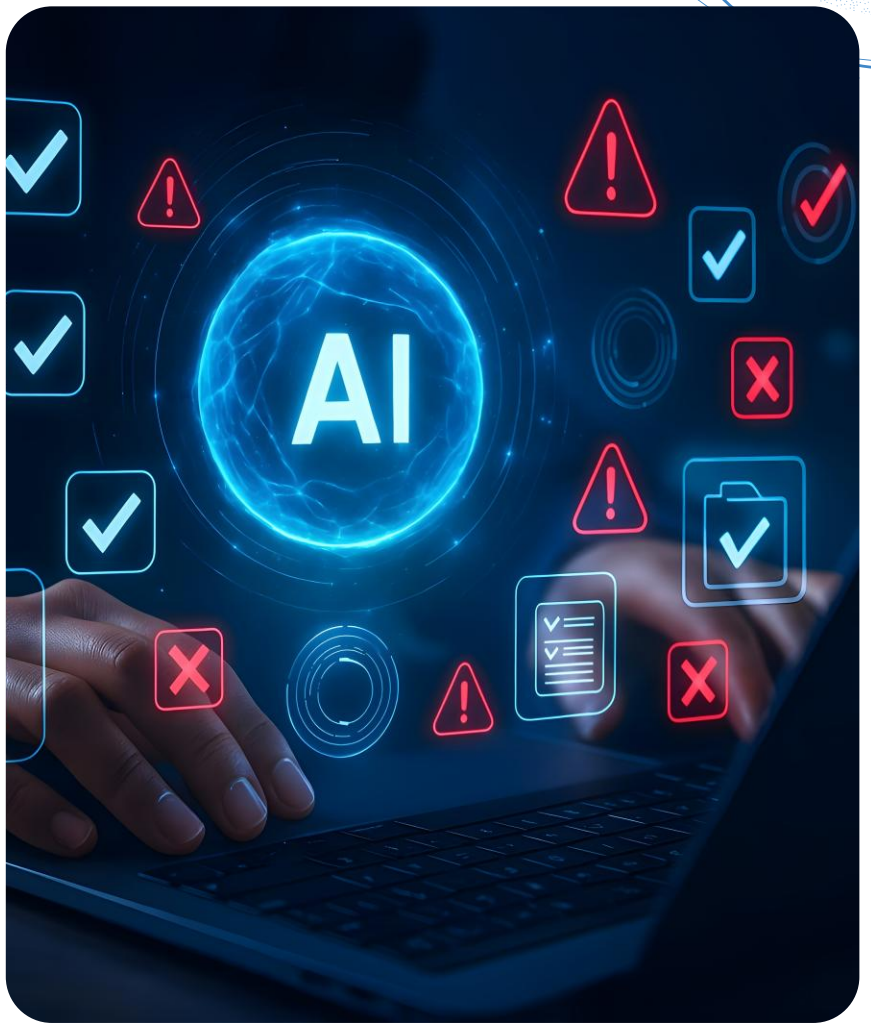
Adversaries are now Agentic

Attackers use AI agents to automate the kill chain at machine speed . You are fighting an adaptive hunter with a manual, ticket-based playbook.

Exploit window has disappeared

Anthropic's Mythos autonomously discovered thousands of zero-day vulnerabilities across every major OS and browser — flaws hidden for decades. The exploit window didn't collapse. It disappeared.

"The risk operations playbook hasn't changed. The threat environment has."



Automate or Fall Behind.

Qualys ROCon 26 The Risk Operations Conference EMEA

From

Siloed Tools
Dashboard-Driven
Weekly Scans
Manual Actions
Risk View



To

Event-Driven
Automation
Agentic AI
Continuous
Real-time
risk actions

Automate or Fall Behind.

Qualys ROCon 26
The Risk Operations Conference
EMEA



Closed loop, intent-driven, agentic.

We're Already Agentic.

When AI finds thousands of zero-days overnight, you need agents that prioritize, validate, and remediate at machine speed.

Qualys ROCon 26 The Risk Operations Conference EMEA

ROCky is the AI-powered Cyber Risk Assistant that orchestrates the agent marketplace — intent in, action out, with full auditability.

Find Risk.
Discover & Prioritize

IN PROD



Agent Sid
Hackers Eye View of your risk

- Continuous external perimeter monitoring
- Toxic-combo & exposure detection
- MTTD: weeks → hours



Agent Nyra
Threat-Based Prioritization

- The <1% of threats that matter
- Attacker-aligned, not scan-aligned

Prove Risk.
Validate

IN PROD



Agent Val
Safe Exploit Validation with Proof

- Closes the validation gap
- Confirms exploitability at machine speed
- No more guessing at real risk – test before and prove after fixing risk.

Fix Risk.
Remediate & Reduce

IN PROD



Agent Sara
Your Patch Tuesday Sidekick

- Maps threat intel to impacted assets
- Prioritizes high-risk CVEs
- Auto-creates remediation jobs

"Same playbook. Same agents. AI is just the next surface."

Same Methodology. New Attack Surface.

The Qualys Enterprise TruRisk Platform — now extended to AI

Qualys ROCon 26 The Risk Operations Conference EMEA

01

Discovery & Ownership

The First Rule

- Full AI stack: GPU, software, agents, MCP, RAG
- Any runtime: self-hosted, cloud, or SaaS LLMs (Bedrock, Databricks, etc.)
- Code-to-runtime context & CMDB correlation
- Ownership mapping via Qualys tags

02

Assessment

AI-Native Posture & DAST

- Automated prompt injection testing (DAST)
- AI-SPM, weights integrity & system prompt validation
- RAG data classification & provenance
- OWASP Top 10 for LLMs

03

AI Attack Path

Toxic Path Discovery

- Shadow AI on endpoints accessing prod data
- Network-exposed agents, LLMs & RAGs
- Prompt-to-crown-jewels via MCP/RAG
- Risk-scored attack graphs

04

Remediation & Controls

Commanding the Path

- Guardrail & system prompt hardening
- Vulnerability patching & misconfig fixes
- Revoke over-privileged entitlements
- Require human-in-the-loop for high-risk actions

05

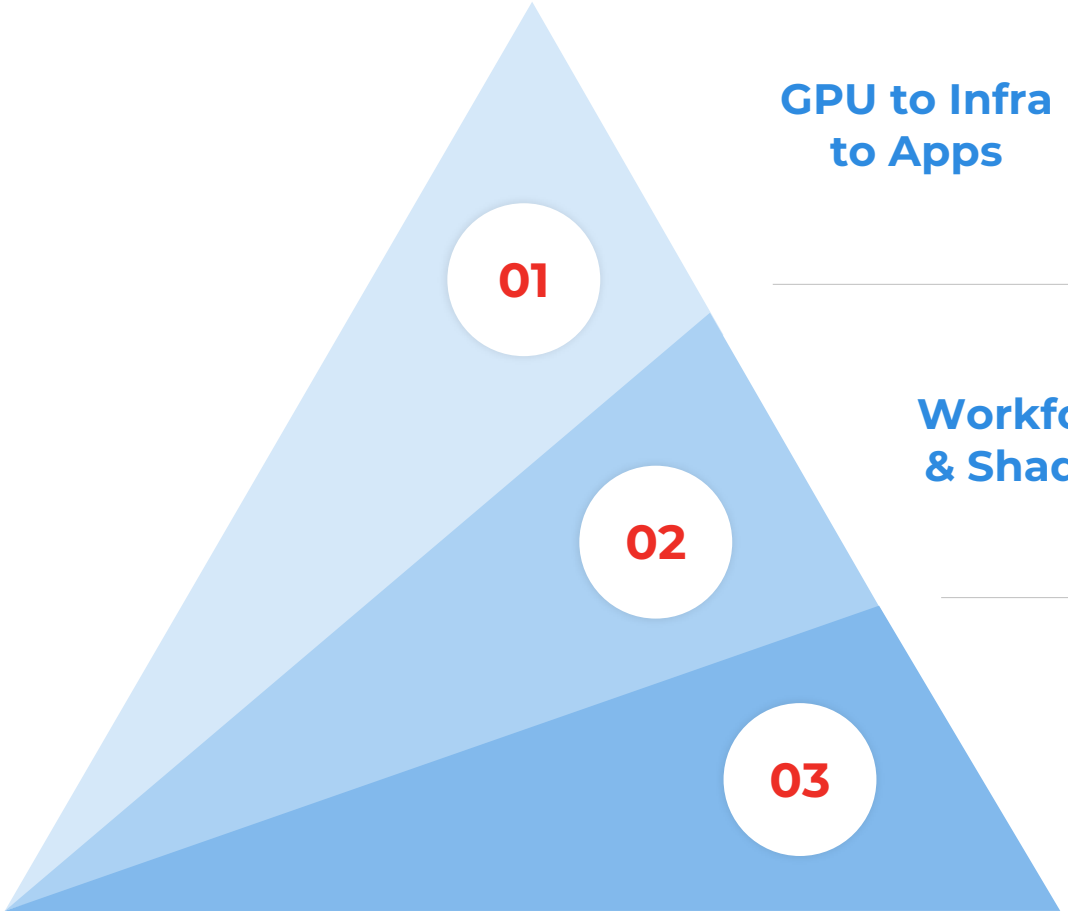
Compliance

Governance & AI-BOM

- Automated AI-BOM generation
- Custom Governance Policies
- EU AI Act & MITRE ATLAS mapping
- Continuous audit-ready reporting

One Platform. The Full AI Risk Surface.

Qualys ROCon 26
The Risk Operations Conference
EMEA



GPU to Infra to Apps

From silicon to the serving layer — discover, assess, and secure every AI workload component

Workforce AI & Shadow AI

Visibility into every AI tool your people use — sanctioned or not, SaaS or local

Code to Cloud

Shift-left scanning for AI dependencies, model supply chain, and deployment configs

XDR excluded — TotalAI is pre-boom posture management, not runtime detection. We secure the surface before the attack, not during.

"AI risk operations — continuous, automated, end to end."

The Qualys Advantage

AI-native approach, powered by unmatched infrastructure reach

Qualys ROCon 26 The Risk Operations Conference EMEA

200M+
Deployed Agents

Unmatched endpoint reach for AI asset discovery

01



02

Cloud Native Connectors

AWS, Azure, GCP — where AI workloads live

04

10k+
Enterprise Customers

Trusted relationships across Fortune 500

03

NDR+ Shadow AI Services

Multi-layered visibility across NDR, Flow Logs, and Endpoint DNS to eliminate unmanaged blind spots

Strategy: Fail fast, adapt, test market – move from LLM-only to full AI infrastructure coverage

What's Shipping. What's Next?

Qualys ROCon 26
The Risk Operations Conference
EMEA

Today

AI asset discovery, LLM scanning, shadow AI visibility, OWASP & EU AI Act compliance

Next Quarter

Agent & RAG discovery, agentic DAST, MCP assessment, external AI discovery

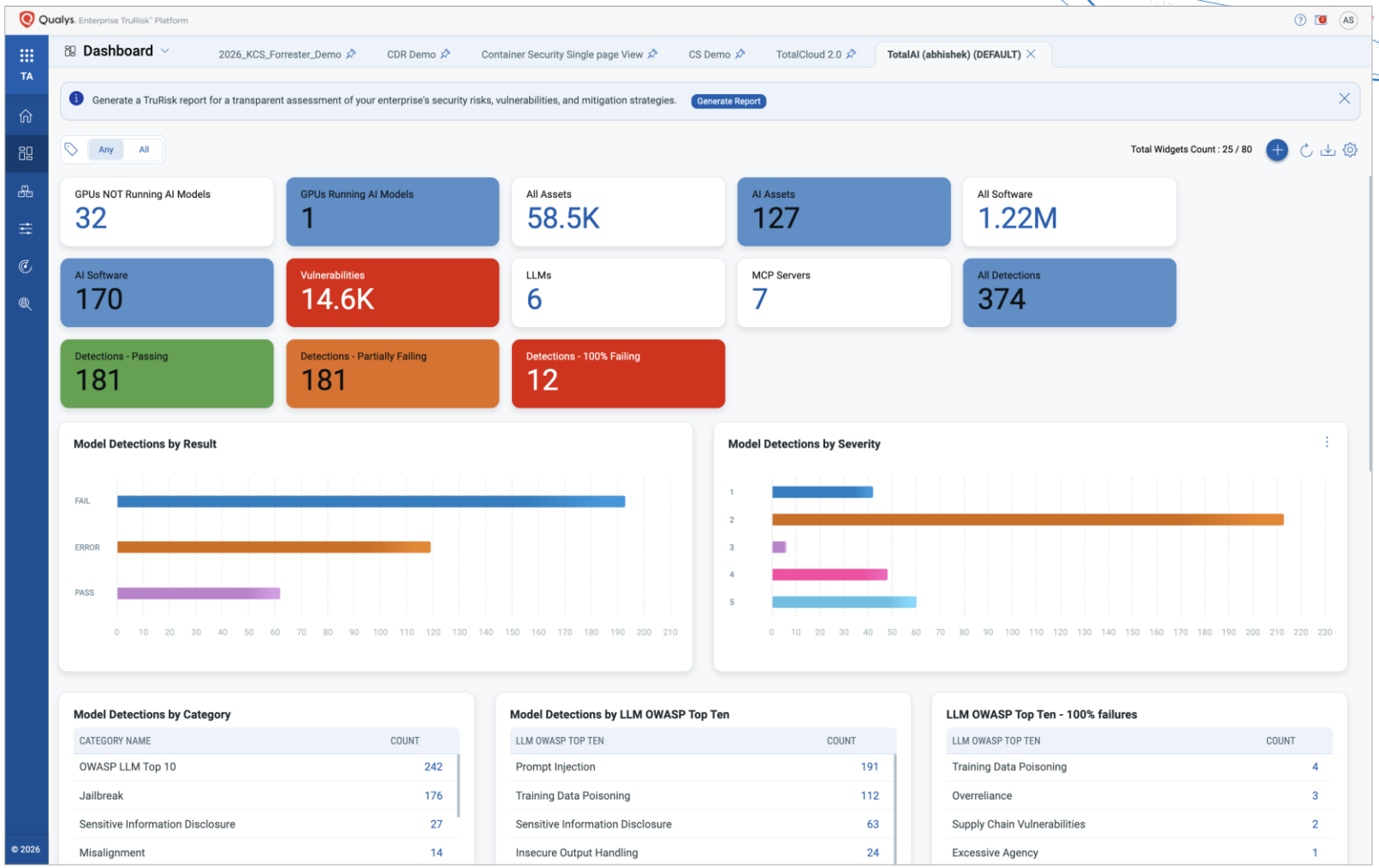
This Year

Blast radius analysis, identity mapping, automated red-teaming, unified AI-BOM

2027+

Full AI attack path analysis, privilege drift detection, continuous AI threat posture

"What you'll see next is what our engineers have been cooking — not a roadmap."



Qualys ROCon 26
The Risk Operations Conference
EMEA

"Let me show you this in ROCky."

QUALYS TOTALAI

Live Demo

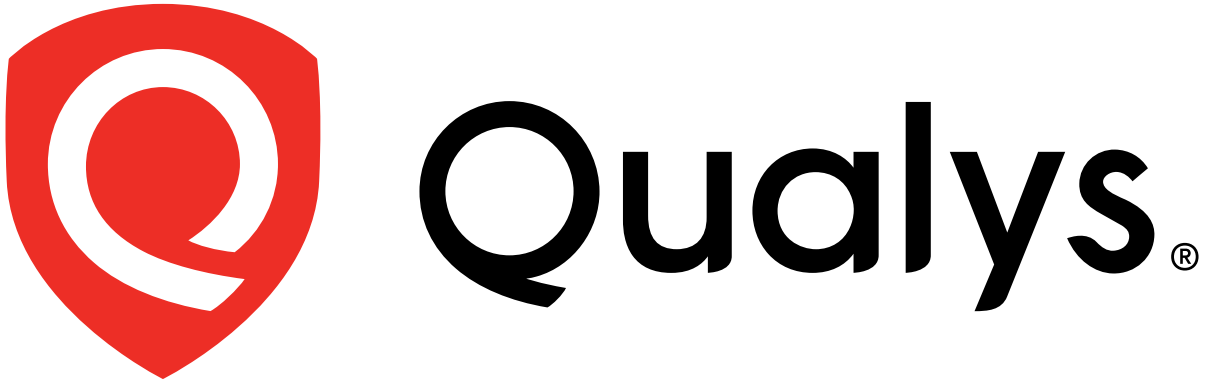
Qualys ROCon 26
The Risk Operations Conference
EMEA



Qualys ROCon 26
The Risk Operations Conference
EMEA

Thank You!




Qualys®

Qualys

ROCon 26

The Risk Operations Conference

EMEA