SELLER COUNSEL & TARGET CTO BRIEF • NON-INTRUSIVE DILIGENCE

15-Minute Read-Only Setup & Zero-Impact IP Guarantee

Auditable CloudFormation/Terraform IAM Scope, Zero Production Agents, Zero Source-Code Exfiltration & KMS Clean-Room Destruction

PRODUCTION AGENTS	TARGET CTO EFFORT	CLEAN-ROOM PURGE
0 Installed	**15 Minutes**	**<24 Hours**
0% CPU / Network Load	30-Second IAM Revocation	SHA-256 KMS Destruction Cert

QUANTSEC ADVISORY • SELLER ENGINEERING ASSURANCE & CLEAN-ROOM CUSTODY

TARGET CTO BRIEF

15-Minute Read-Only Onboarding & Zero-Impact IP Guarantee

Audience: Target CTO, VP Engineering, CISO & Seller Legal Counsel
Architecture: Out-of-Band Control-Plane API (Wiz Enterprise Partner)
Scope: AWS • Azure • GCP • VDR Clean Room
Revocation: Instant Single-Click Role Deletion

KERNEL / HOST AGENTS	LIVE TRAFFIC PROBES	TARGET ENGINEERING TIME	ARTIFACT CUSTODY
0 Agents	**0 Port Scans**	**15 Minutes**	**AWS KMS CMK**
Zero Workload Disruption	Safe for MedTech & FinTech	Auditable IaC Template	Signed Destruction Proof

1. ENGINEERING COMMITMENT TO TARGET TECHNICAL LEADERSHIP

BUILT BY PRINCIPAL ARCHITECTS

QuantSec Advisory was founded by Principal Security Architects who have sat on your side of the table during live product launches and enterprise audits. Traditional M&A IT diligence disrupts engineering sprints with 300-row spreadsheets, invasive agents, and reckless active scanners. Our **48-Hour Sprint** runs **100% out-of-band** against cloud provider control-plane APIs and clean-room VDR exports—requiring **15 minutes of DevOps setup**, imposing **0.0% CPU or network load on production workloads**, and never copying proprietary source code or customer PII/ePHI.

2. VERIFIABLE TECHNICAL GUARDRAILS: WHAT WE INSPECT VS. WHAT WE NEVER TOUCH

LINE-BY-LINE AUDITABLE IAM

✓ STRICTLY READ-ONLY METADATA INSPECTED

- ✓ **Cloud Control-Plane Configs:** AWS `SecurityAudit` / `ViewOnlyAccess`, Azure `Reader`, or GCP `Viewer` IAM policies via open-text CloudFormation/Terraform.
- ✓ **Agentless Snapshot Graph (Optional):** Out-of-band Wiz Partner API inspection for CVE/KEV package manifests without touching live compute nodes.
- ✓ **Offline OT & Network Artifacts:** Passive review of exported firewall ACLs, VLAN tables, CycloneDX SBOMs, and architecture diagrams inside our Clean Room.

✕ STRICTLY PROHIBITED & TECHNICALLY BLOCKED

- ✕ **Zero Write / Mutate Permissions:** Zero ability to modify IAM, security groups, workloads, routing tables, or production configurations.
- ✕ **Zero Customer Payload or Crown-Jewel Cloning:** IAM role explicitly excludes reading S3/Blob object contents, RDS/DynamoDB rows, or secret values (`kms:Decrypt` denied on app keys).
- ✕ **Zero Active Network Probing:** Zero Nmap/Nessus sweeps against fragile IoMT medical devices, lab OT analyzers, or payment HSMs.

3. END-TO-END 48-HOUR SPRINT LIFECYCLE & 30-SECOND REVOCATION

FULL TARGET CONTROL

WINDOW	TARGET ENGINEERING ACTION	QUANTSEC EXECUTION & SECURITY CONTROL
Step 1: Hour 0 (15 Minutes)	Review human-readable Terraform/CloudFormation template & deploy scoped cross-account Read-Only role.	ExternalID-pinned trust policy locked exclusively to QuantSec's dedicated Wiz Partner & single-tenant AWS Clean-Room enclave.
Step 2: Hours 2–36 (0 Minutes)	**None.** Your team stays 100% focused on product roadmap.	Out-of-band graph ingestion across IAM blast radius, network exposure, encryption metadata, AI-SPM configs, and VDR compliance artifacts.
Step 3: Hour 36 (Optional 30 Min)	Optional Principal-to-CTO context review call to validate compensating controls before readout.	Eliminates false positives so legitimate architectural decisions (e.g., isolated VPC proxies or VEX mitigations) are accurately credited in our IC memo.
Step 4: Hour 48+ (30 Seconds)	Delete the cross-account IAM stack in a single click or CLI command.	Immediate API revocation; QuantSec schedules cryptographic KMS CMK deletion across the deal Clean-Room VPC within 24 hours of engagement sign-off.

4. EPHEMERAL AWS CLEAN-ROOM & CRYPTOGRAPHIC DESTRUCTION CERTIFICATE

ZERO CONSULTANT LAPTOP STORAGE

Zero Local Endpoint Persistence: VDR uploads (architecture diagrams, SOC 2 reports, SBOMs, pen-test summaries) are ingested directly into an isolated, single-tenant AWS S3/VPC enclave encrypted under a **deal-specific AWS KMS Customer-Managed Key (CMK)**—never downloaded to local laptops. Within 24 hours of final readout, QuantSec revokes enclave access, schedules irreversible KMS key destruction, and issues a **SHA-256 Signed Certificate of Data & Key Destruction** to both Deal Sponsor and Seller Legal Counsel.

Questions from Target Engineering or Seller Counsel? Practice Lead **Ruben Benegas, MS, CISSP** (former Lead Product Cybersecurity Architect [Contract] at **Medtronic**; Principal Security Engineer at **U.S. Bank**; VP & Lead Security Engineer at **Wells Fargo**) is available for a 10-minute technical pre-check prior to role deployment • **ruben@quantsecadvisory.com** • **612-875-5531**