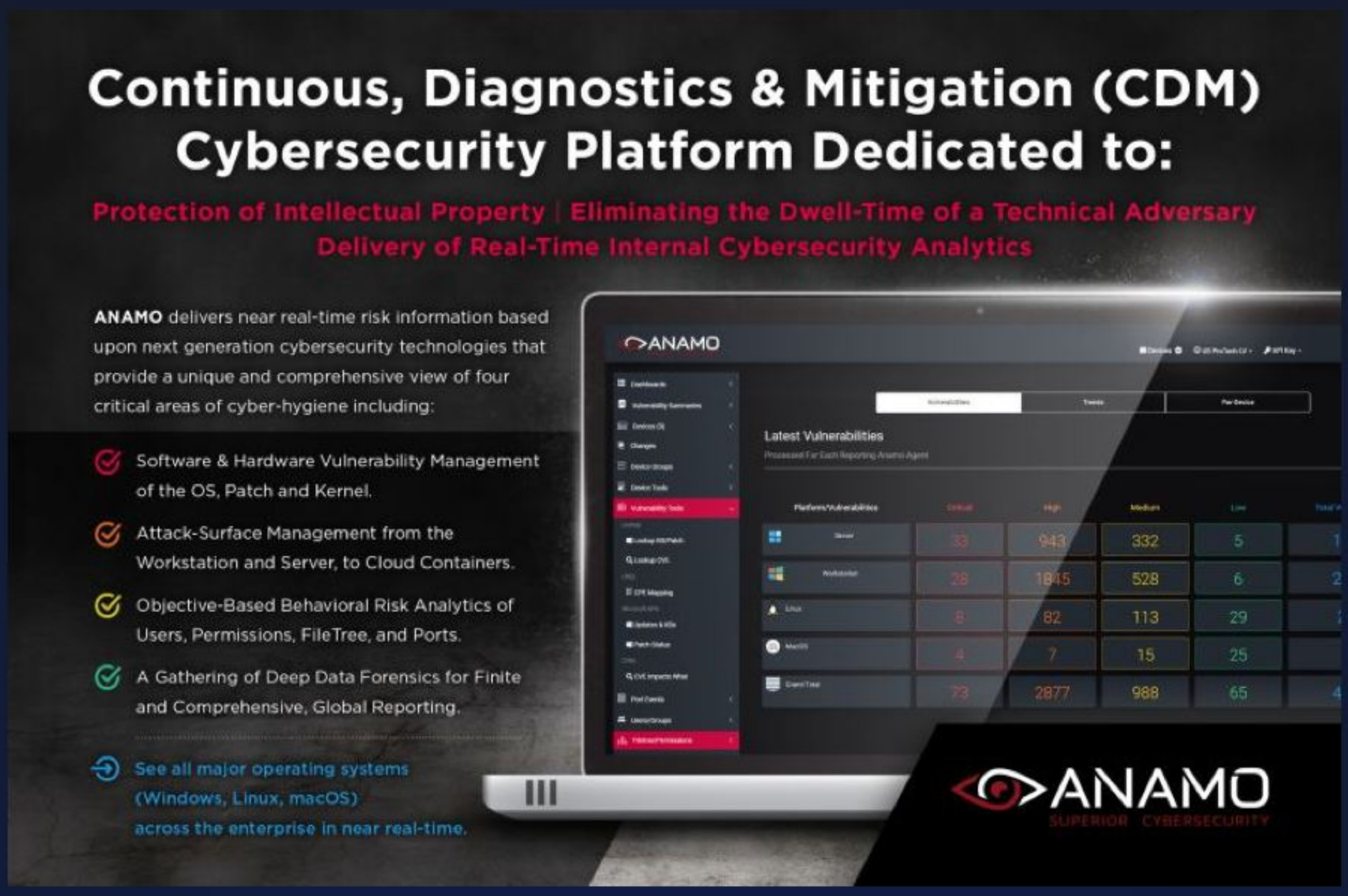
ANAMO

Powered by Nimbus-Key



The Cyber Shield Alliance:
Redefining Trust in Critical Infrastructure.
Anamo & Nimbus-Key® ID

US ProTech / Anamo
Jonathan Goesth, CEO

Nimbus-T Global
Jose Bolanos MD, CEO

The Cyber Shield Alliance: Redefining Trust in Critical Infrastructure. Anamo and Nimbus-Key® ID

1. The Imperative for Proactive Defense

In an era marked by state-sponsored cyberattacks and supply chain manipulation, static credentials have become untenable. The federal mandate for Zero Trust architecture (ZTA) compels agencies to eliminate implicit trust and rely on continuous validation of user, device, and context. **The Cyber Shield Alliance** — combining **Nimbus-Key® ID** and **Anamo's Continuous Diagnostics and Mitigation (CDM)**— delivers an identity framework designed for the most critical systems: governments, energy grids, and nuclear facilities.

Nimbus-Key® ID - Cyberattacks begin where trust is weakest: the login. Over 80% of breaches stem from compromised credentials, exposing the fatal flaws of passwords and static 2FA / MFA. **Nimbus-Key® ID** introduces a next-generation solution with **True User Verification™** and **DE-MFA® (Dynamically Encrypted Multi-Factor Authentication**)— a system that issues biometric-bound, encrypted login keys refreshed every five minutes. These ephemeral credentials are immune to phishing, theft, and even quantum decryption due to their short lifespan. In alliance with Anamo's real-time risk orchestration, every login becomes a dynamic trust decision. This isn't just authentication—it's a living defense layer that closes the most common cyberattack vector.

Anamo CDM - The first commercially available **Continuous Diagnostics and Mitigation (CDM) platform** built to modernize federal and enterprise cybersecurity cybersecurity by detecting an internal technical adversary or unauthorized user in one-pivot on any system.. Developed to align directly with CISA and DHS CDM standards, this patent-pending SaaS solution ingests and analyzes a wide range of telemetry — from user and group behavior, device posture, ports, permission changes, software vulnerabilities (CVEs), and historical forensics — **Anamo** delivers real-time dashboards and prioritized remediation recommendations without manual setup or data entry. Unlike legacy siloed tools (EPP, EDR, SIEM, ASM), Anamo consolidates their capabilities into a unified, always on interface that identifies "hard-to-detect" risks and "technical adversaries" in near real time.

What truly sets Anamo apart is its dynamic risk engine — delivering comparative **HashID Analytics**, the system not only detects zero-day exploits and anomalous behavior, but also automatically triggers adaptive response actions such as notifications, adaptive authentication, and end-point isolation—all through an accessible, intuitive interface that requires no specialized expertise. Offered in tiered editions (Fundamentals, Professional, Enterprise) and backed by free trials and NFR licensing, Anamo provides a scalable, affordable path to advanced CDM— empowering organizations to move from reactive alerts to proactive, Intelligence-driven defense.

2. The One-Two Punch in Cyber Defense

In the battle against modern cyber threats, most systems fail at the point of entry—login. **Nimbus-Key ID** delivers the first blow with True User Verification™ , leveraging KYC/AI/ Biometric validation of user, device UUID, and DE-MFA (Dynamically Encrypted Multi-Factor Authentication). Each login generates a one-time, quantum-resilient credential that expires within minutes, ensuring that stolen credentials are useless before they can be exploited (nimbus-t.com).

Anamo follows through with the knockout punch: **a real-time risk orchestration engine** that continuously evaluates the trustworthiness of every device, user behavior, port activity, and known vulnerability (CVEs) across the network (anamo.io). Together, these systems form an airtight, multilayered shield. A valid biometric alone isn't enough without verified device context. And a clean device can't bypass Nimbus's zero-trust, identity-bound encryption. It's not just multifactor—it's multi-dimensional. This integration turns identity into a live, risk-aware perimeter, rendering brute force, phishing, and credential stuffing obsolete. No loopholes. No shortcuts. Just verified identity and real-time risk intelligence working in perfect coordination to shut the door on attackers.

3. Command and Control: Anamo's Always-On Cyber Intelligence Core

Anamo is more than a CDM platform—it's a real-time cybersecurity command center engineered for mission-critical environments. Built to serve the operational needs of both U.S. federal agencies and enterprise networks, Anamo delivers 24/7/365 threat detection and active mitigation through intelligent dashboards that prioritize risk, guide resource allocation, and trigger immediate remediation. **Over 300 organizations**, including federal agencies, have made CDM a cornerstone of their cyber defense—and Anamo is leading the charge with its next-generation architecture.

What sets Anamo apart is its deep integration of multiple best-in-class capabilities into a single, unified platform:

- SIEM for real-time incident detection,
- EDR for endpoint response,
- ASM to uncover exposed attack vectors,
- Vul-Scan for continuous CVE monitoring,
- EPP for perimeter protection, and
- Behavior Awareness (BA) to detect insider threats and anomalous actions.

This fusion enables Anamo to move beyond isolated alerts and into orchestrated, automated defense. **It doesn't just see the threat—it understands it, prioritizes it, and acts on it with surgical precision.** In a cyber landscape where seconds matter, Anamo gives infrastructure leaders the real-time intelligence control they need to stay aheaad of IoA's, IoC's and ZDE's.

4. Defending America's Power Grid from Pre-Positioned Cyber Warfare

The FBI has issued a stark warning: Chinese state-sponsored actors, including the **Volt Typhoon group,** have successfully embedded themselves within U.S. critical infrastructure—particularly power grids—quietly pre-positioning access for future sabotage. These intrusions are not speculative—they're operational. Attackers aren't simply collecting intelligence; they're preparing to "wreak havoc and cause real-world harm" by taking down electric power, water, transportation, and communication systems during future geopolitical conflicts. Unlike conventional cybercrime, these operations focus on long-term persistence, stealth, and coordinated disruption—aimed at causing physical damage, economic chaos, and mass panic.

This new threat landscape demands a response that is both predictive and preemptive—and that's where the combined power of **Anamo and Nimbus-Key® ID** becomes indispensable. Anamo's CDM platform monitors grid systems in real time, correlating endpoint activity, device behavior, and CVEs to detect subtle signs of intrusion long before action is taken. It doesn't just alert—it acts, executing autonomous mitigation like session revocation or endpoint quarantine. Paired with Nimbus's DE-MFA® —which binds each login to a biometric-verified identity and a device-specific key that expires every five minutes—the combined system renders credential reuse and lateral movement functionally impossible. In a world where hostile actors are already inside the wire, this **one-two punch of dynamic authentication and intelligent orchestration is not just superior—it's essential.** Without it, the grid remains a silent target; with it, every access point becomes a shielded gate guarded by real-time trust.

5. Nuclear-Grade Identity Assurance: Securing the Core of National Infrastructure

The energy sector—and nuclear facilities in particular—stand at the epicenter of a rapidly intensifying cyber battleground. A **recent Resecurity report highlights a surge in attacks targeting nuclear and energy networks by hacktivist groups** and nation-state actors linked to China, Iran, North Korea, and Russia, exploiting the convergence of IT/OT networks and IIoT deployments to penetrate critical control systems. These campaigns, designed for espionage and potential sabotage, elevate the stakes: a single breach could compromise reactor operations, safety controls, or even emergency response mechanisms. Regulatory bodies like NERC and DOE have responded with updated cybersecurity mandates, yet the scale of the threat demands solutions that far exceed compliance checklists .

The **Cyber Shield Alliance** dives deep into this challenge with uncompromising, nuclear-grade identity assurance. Every access request is tied to True User Verification™, a biometric handshake that confirms the human behind the credential.

Access takes place only on verified, secure devices, using DE-MFA's quantum-resistant, ephemeral keys that expire in minutes. Crucially, risk thresholds adapt to mission criticality: low-stakes functions require standard verification; high-stakes operations like reactor management or safety systems trigger multimodal proof and elevated scrutiny, all logged in real-time for audit and forensic review. By locking down identity at the deepest layers—human, device, device health, context, and time-bound tokens—the alliance constructs a cyber moat around nuclear infrastructure. In a world of stealthy adversaries and rapidly evolving threats, this isn't extra security—it's the golden standard for protecting what matters most.

6. Quantum-Resilience Meets CDM: Fortifying the Future Before It Arrives

As quantum computing accelerates toward mainstream deployment, the cryptographic foundations of today's digital infrastructure are at risk of becoming obsolete. Algorithms that once took centuries to break may soon be cracked in minutes. For critical sectors—government, defense, energy, and nuclear—the implications are existential. Adversaries are already conducting "harvest now, decrypt later" attacks, stockpiling **Hash ID data** with the intent to unlock it when quantum decryption becomes viable. This threat makes post-quantum cybersecurity not optional—but urgent. These constant types of attacks must be met with a continuous diagnostics and mitigation program and Anamo is a patented (pending) commercial-grade SaaS Cybersecurity platform that's ready to deploy today.

Nimbus-Key ID answers this challenge with **DE-MFA** (Dynamically Encrypted Multi-Factor Authentication)—a breakthrough approach that issues cryptographic login credentials every five minutes, uniquely tied to a verified user's biometrics and device fingerprint. These ephemeral keys expire before any brute-force or quantum algorithm could even begin the decryption process. Meanwhile, Anamo strengthens this posture with a decentralized trust model that distributes identity and access decisions across a dynamic, continuously monitored risk layer. This eliminates the vulnerability of centralized key stores or single points of failure. Together, they form a self-refreshing, quantum-resilient identity ecosystem that not only withstands current threats but anticipates future adversaries. It's not just security for today—it's infrastructure built to outlive the next generation of cyber weapons.

7. Supply Chain and Third-Party Control: Sealing the Back Door Before It's Used

In today's hyperconnected ecosystem, the digital supply chain is one of the most exploited vectors for cyber intrusion. From **SolarWinds to MOVEit, high-profile breaches** have shown that attackers no longer storm the front gate—they slip in quietly through third-party vendors, partners, and unmanaged access points.

These external connections often lack the hardened security controls applied to internal systems, creating dangerous blind spots across mission-critical infrastructure. The result: breaches that bypass core defenses, inject malware into operational workflows, and propagate through networks with little resistance.

The Cyber Shield Alliance eliminates this vulnerability with i**dentity-bound, risk-aware access control for every external actor**—from contractors and IT vendors to field technicians and equipment suppliers. Nimbus-Key ID ensures that each user, regardless of their employer or domain, is issued **a globally unique, biometric-verified digital identity token**. No shared logins. No pass-through credentials. This ID is cryptographically bound to their device and expires within minutes. Simultaneously, Anamo's orchestration engine evaluates real-time risk factors—patch status, device health, geolocation, behavioral anomalies—before allowing any access. If anything is out of alignment, access is blocked or escalated. This dual-lock system ensures that even trusted third parties must continuously prove their trustworthiness. In an age where one rogue laptop can bring down a national grid, this alliance offers supply chain access that is not only federated, but fully fortified.

8. Compliance at Scale: Turning Burden into Strategic Advantage

For government agencies and critical infrastructure operators, regulatory compliance isn't just a checkbox—it's a mandate with national security implications. Standards such as **FedRAMP, FISMA, NERC CIP, and NRC 10 CFR 73.54** require demonstrable control over access, continuous monitoring, incident response, and forensic traceability. Yet meeting these standards across a sprawling, hybrid environment with internal staff, third-party vendors, and legacy systems can become overwhelming—especially when managed manually. Delayed reporting, incomplete logs, and fragmented audit trails not only put compliance at risk but expose organizations to operational shutdowns, legal penalties, and reputational damage.

The **Cyber Shield Alliance** addresses this challenge head-on with a **compliance-first architecture** that is purpose-built for scale. Every biometric login, device trust evaluation, session approval, and DE-MFA token issuance is logged immutably—creating a granular, tamper-proof audit trail. **Anamo's real-time DRIFT detection i**dentifies changes in privilege, configuration, or risk posture and immediately triggers revocation or escalation workflows. These events are automatically compiled into audit-ready dashboards, complete with timestamps, risk scoring, and remediation actions— aligned with federal regulatory control frameworks such as CMMC 2.0, NIST 800, energy, and nuclear sectors. Instead of treating compliance as an afterthought, the Alliance makes it a living, breathing process that evolves with the threat landscape. By automating compliance with Anamo's proprietary GRC App and embedding it into the core of identity and access management, agencies can shift from reactive fire drills to proactive governance—reducing overhead, streamlining Inspections, and hardening trust with regulators and stakeholders alike.

9. Seamless Cross-Domain Orchestration: Unifying Identity Across Legacy, Cloud, and Critical Systems.

One of the most persistent challenges in securing critical infrastructure is the **fragmentation of identity systems.** From cloud-based SaaS applications and mobile endpoints to legacy on-prem databases and industrial control systems (ICS), organizations often juggle dozens of disparate identity and access management (IAM) frameworks—each with its own protocols, policies, and limitations. This complexity not only slows down deployment and increases risk but also creates inconsistent user experiences that frustrate teams and open doors to misconfigurations and security gaps.

Anamo solves this problem with powerful **identity orchestration** capabilities designed to operate across heterogeneous environments. Its architecture supports seamless integration with **SAML, OIDC, LDAP, Kerberos, and proprietary IAM protocols**, allowing it to unify authentication flows across the full digital estate—from next-gen cloud apps to hardened ICS stacks (strata.io, ibm.com). This orchestration enables centralized policy enforcement, risk evaluation, and adaptive authentication across every domain. Whether it's a remote contractor accessing a control panel at a power station or an administrator logging into a government analytics dashboard, the authentication experience is unified, secure, and context-aware.

Deployment becomes agile and scalable—start with a pilot in one region or division, then expand laterally across agencies, grids, or plants. No forklift upgrades. No disruption. The Alliance turns complex, siloed identity systems into a **single, intelligent security fabric**, reducing friction while elevating security posture at every layer.

10. The Future of Critical Infrastructure Security: Building the Intelligent Perimeter for a Post-Perimeter World

As cyber threats grow more advanced, persistent, and state-sponsored, securing critical infrastructure is no longer about guarding the network perimeter—it's about securing identity, context, and intent at every digital interaction. T**he Cyber Shield Alliance between Nimbus-Key ID and Anamo** represents the blueprint for this new era. It unites the core pillars of next-generation cybersecurity: verified human identity, real-time device health monitoring, dynamically encrypted login credentials resistant to quantum attack, and intelligent risk orchestration that adapts with every session. This is not a patchwork of tools—it's a fully integrated, dynamic defense platform engineered for critical environments where downtime is not an option, and breach consequences are catastrophic.

What makes this alliance truly transformative is its readiness for the future. It's built to evolve—**with native support for AI-powered threat hunting, 10T and I110T device onboarding**, and **autonomous access controls** that self-adjust based on real-time context. It prepares infrastructure not just for today's ransomware and insider threats, but for tomorrow's AI-driven supply chain attacks, synthetic identity fraud, and quantum-enabled decryption efforts. As government agencies and operators modernize legacy systems under tightening regulatory mandates, the **Cyber Shield Alliance** delivers a scalable, interoperable, and forward-compatible platform that doesn't just meet compliance—it redefines it. This is more than a cybersecurity solution; it's a strategic security framework for a hyper-connected, adversary-rich world. It is the gold standard for identity-centric, intelligence-driven defense—and it will define the next decade of critical infrastructure security. Others won't just want to follow—they'll need to.

References

1.Anamo is a CDM cybersecurity platform providing Continuous Diagnostics and Mitigation https://anamo.io/
2. Nimbus-Key® ID with True User Verification and DE-MFA® https://nimbus-t.com
3. What is Identity Orchestration? https://www.strata.io/resources/whitepapers/what-is-identity-orchestration/?utm_source=chatgpt.com
4. NSA Releases Recommendations for Maturing Identity, Credential and Access Management
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3328152/nsa-releases-recommendations-for-maturing-identity-credential-and-access-manage/
5. M-22-09: Federal zero trust architecture strategy – White House memorandum
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
6. Chinese Government Poses "Broad and Unrelenting" Threat to US Critical Infrastructure, FBI Director Says. https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says
7. Resecurity warns of increased cyber threats to energy and nuclear facilities from hacktivists and nation-states. https://industrialcyber.co/utilities-energy-power-water-waste/resecurity-warns-of-increased-cyber-threats-to-energy-and-nuclear-facilities-from-hacktivists-and-nation-states/

ANAMO

Powered by Nimbus-Key

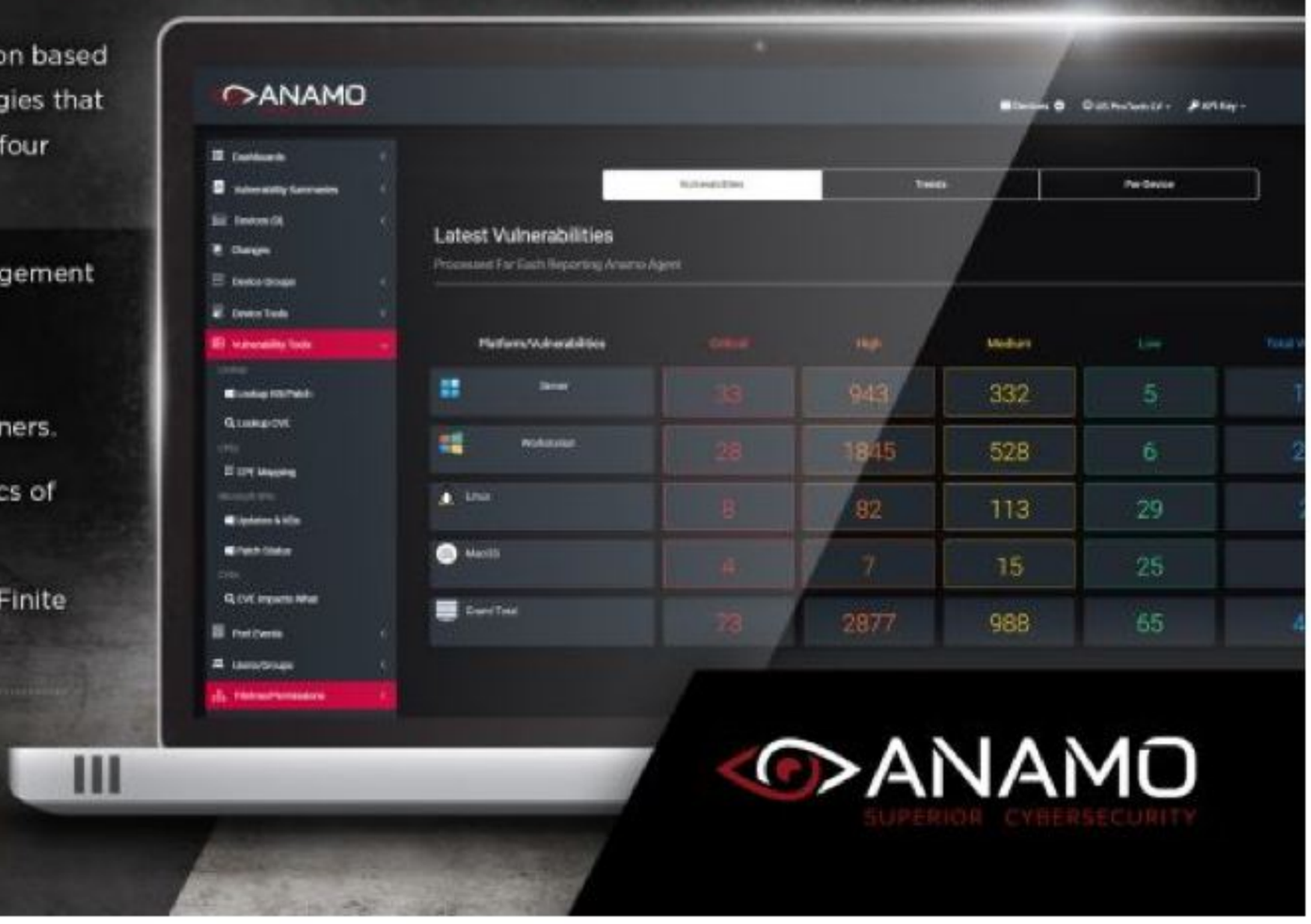
Continuous, Diagnostics & Mitigation (CDM) Cybersecurity Platform Dedicated to:

Protection of Intellectual Property | Eliminating the Dwell-Time of a Technical Adversary
Delivery of Real-Time Internal Cybersecurity Analytics

ANAMO delivers near real-time risk information based upon next generation cybersecurity technologies that provide a unique and comprehensive view of four critical areas of cyber-hygiene including:

- Software & Hardware Vulnerability Management of the OS, Patch and Kernel.
- Attack-Surface Management from the Workstation and Server, to Cloud Containers.
- Objective-Based Behavioral Risk Analytics of Users, Permissions, FileTree, and Ports.
- A Gathering of Deep Data Forensics for Finite and Comprehensive, Global Reporting.

See all major operating systems (Windows, Linux, macOS) across the enterprise in near real-time.



Powered by Nimbus-Key®

Contact: US Protec / Anamo:
Jonathan Goetsch, CEO
jonathan@usprotech.com

Contact: Nimbus-T Global:
Jose Bolanos MD, CEO
jose@nimbus-t.com