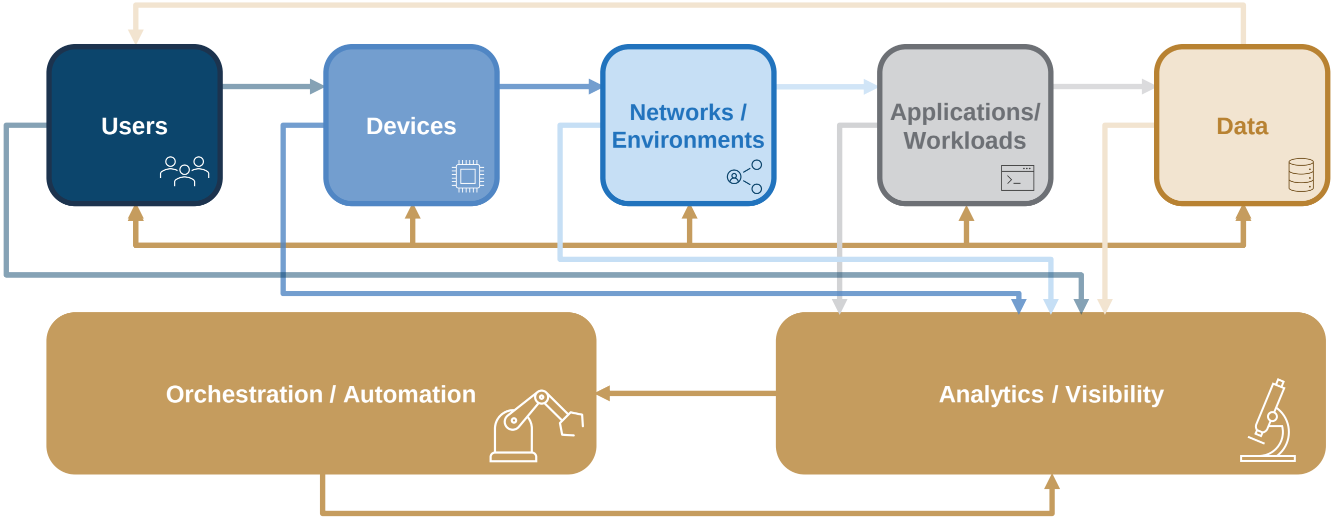
SUMMIT ZERO TRUST

FULL-SPECTRUM CYBER OPERATIONS

Disrupting Threats and Safeguarding Critical Missions



Our Approach: Our cyber security professionals help national security leaders implement zero trust principles across targeted technology domains by establishing trust for users, devices, and applications, enforcing least-privilege access, continuously monitoring trustworthiness, and rapidly responding to security incidents.

Uninterrupted Mission Assurance

We ensure mission continuity and cyber resilience by proactively identifying and mitigating cyber threats. Our advanced threat detection, vulnerability assessments, continuous monitoring, and AI-enhanced threat hunting capabilities rapidly detect, respond to, and neutralize cyber threats before they can disrupt mission-critical systems and operations. Regularly conducted cyber wargames and simulated attack exercises further enhance readiness, providing decision-makers with actionable insights to secure operations against emerging threats.

Verified Security for OT and ICS

Herren deploys Zero Trust architectures tailored explicitly to mission-critical operational technology (OT) and industrial control systems (ICS). Our team applies rigorous micro-segmentation, continuous verification protocols, real-time anomaly detection, and proactive threat modeling to secure critical infrastructure against cyber intrusions. Our SUMMIT ZERO TRUST™ approach ensures that sensitive OT and ICS systems remain protected, preserving operational integrity and mitigating risk in high-stakes defense environments.

Embedded Cybersecurity for Platforms and Weapon Systems

Our cyber professionals also integrate comprehensive cybersecurity throughout the lifecycle of defense platforms and weapon systems. Our secure engineering practices include robust DevSecOps methodologies, early-stage risk assessments, penetration testing, and secure software development standards. These practices ensure that cybersecurity is integral to system design and maintained through deployment, providing warfighters with reliable, resilient platforms capable of withstanding sophisticated cyber threats.

Accelerated RMF Accreditation

We streamline the Risk Management Framework (RMF) assessment and accreditation processes by applying automation and analytic-driven validation techniques. Our methodology significantly accelerates Authority to Operate (ATO) approvals, reducing manual tasks through intelligent evidence collection, security control validation, and automated documentation. This approach expedites compliance timelines, ensuring that defense systems are securely and efficiently authorized for deployment, without compromising security or regulatory standards.

About Herren. For more than 35 years, national security leaders have trusted Herren to address their most complex challenges, safeguarding critical missions and maximizing the value of every taxpayer dollar. *To learn more, visit HerrenAssociates.com*