

HYPERTM

**HYDRA PERSISTENT
EVOLUTIONAL RANGE**

White Paper

The Challenge: Training That Ends When the Threat Does Not

Modern cyber conflict does not operate on exercise schedules. Adversaries maintain persistent access over weeks and months, adapting their tactics continuously in response to defensive measures, exploiting vulnerabilities in organizational behavior rather than just technology, and building institutional knowledge about their targets that compounds over time. The threat never resets.

Yet the dominant model for cyber readiness training remains fundamentally episodic: teams are assembled, a scenario is executed over a defined window, a report is written, and the environment is torn down. The adversary disappears. The intelligence they gathered disappears. The persistence they established disappears. Participants return to their units having exercised against a threat that bore little resemblance to the patient, adaptive operators they will face in actual conflict.

The result is a structural gap between training and reality. Defenders develop proficiency at incident response within scripted scenarios but lack experience managing sustained campaigns. Hunt teams conduct exercises against known threat profiles rather than genuinely persistent adversaries who have built real familiarity with the environment. Intelligence analysts work against synthetic data rather than organic adversarial behavior. And because each exercise begins from a clean state, no organization ever develops the institutional memory that real adversaries accumulate as a matter of course.

The DoW and federal cyber enterprise need a fundamentally different training model—one where the environment never resets, the adversary never disappears, and every training event builds on what came before. That is the operational problem HyPER was built to solve.

HyPER: The Living Cyber Battlespace

The Hydra Persistent Evolutional Range (HyPER) is our always-on, intelligence-driven cyber training environment designed to mirror the continuous, adaptive nature of real-world cyber conflict. Where traditional ranges create discrete training events, HyPER creates an operational ecosystem—a persistently contested digital battlespace where defensive operations never cease, adversarial campaigns unfold over weeks and months, and every team's actions influence the environment that every other team operates within.

HyPER is built on our HYDRA infrastructure platform, providing the underlying compute and orchestration layer, and integrates two proprietary capabilities that define its character. ShadowBreach, our adversary emulation platform, provides the adversarial forces—automated and human-guided threat actors that maintain persistent presence, build genuine targeting intelligence, and adapt their tactics based on observed defensive responses. ShadowSim, our traffic automation platform, populates the environment with realistic user behavior—emails, file activity, inter-system communications, and organizational workflows—creating the authentic operational noise within which both attackers and defenders must work.

The result is not a more sophisticated exercise. It is a different kind of training entirely—one where the terrain has history, the adversary has memory, and every participant's decisions carry consequences that persist beyond the day's session.

The Always-on Operational Model

HyPER operates continuously. Between major exercise events, the environment maintains sustained activity across three dimensions:

Defensive operations never cease. Blue teams, hunt teams, and security analysts operate against persistent adversarial presence between major exercises, conducting genuine threat hunting, refining detection capabilities, and testing new defensive tools against intelligent, adaptive

opposition. Security improvements made during one exercise cycle are validated—and potentially defeated—by adversaries that continue operating after the exercise concludes.

Adversarial campaigns continue across exercise boundaries. Red teams and ShadowBreach-driven automated adversaries maintain the access they established, continue lateral movement operations, and adapt their approaches based on the defensive countermeasures they observe. When the next exercise begins, the adversary does not restart from zero. They resume from wherever they were—with the persistence mechanisms they built and the organizational knowledge they accumulated still intact.

The intelligence picture evolves continuously. Because the environment never resets, both offensive and defensive teams accumulate operational knowledge over time—building genuine understanding of how adversaries behave in this specific environment, where defensive gaps persist despite repeated hardening efforts, and how organizational patterns create exploitable timing and access opportunities. Neither side operates from generic assumptions. Both sides develop the kind of target-specific intelligence that defines actual advanced persistent threat operations.

USE CASE: Sustained APT Campaign — Training That Mirrors the Actual Threat

A DoW cyber protection team is preparing for operations against nation-state adversaries known for long-duration, low-and-slow campaigns that establish persistence over months before executing their objectives. Traditional exercise formats give them experience managing individual incidents, but no experience sustaining vigilance against a patient, adaptive threat across extended timeframes. In HyPER, the CPT engages against an adversary—guided by our red team operators and sustained by ShadowBreach automation—that has been operating in the environment for weeks before the exercise officially begins. The team inherits an environment where the adversary has already established persistence, is conducting active reconnaissance, and is adapting tactics based on observed defensive activity. The team must identify

existing compromises, contain ongoing campaigns, and hunt for persistence mechanisms they did not witness being established—exactly the operational reality they will face against actual advanced persistent threats.

Customer Benefit: Participants develop genuine experience managing sustained adversarial pressure rather than responding to scripted incidents. Hunt teams build real proficiency at identifying persistent compromise in complex environments. Intelligence analysts develop authentic analytical skills working against an adversary whose behavioral patterns emerged organically rather than from a scenario script. The result is cyber readiness that reflects the actual character of advanced threat operations.

Core Capabilities

Intelligent Warfare Scenario Development

HyPER replaces scripted exercise scenarios with what we call Intelligent Warfare—a scenario development methodology where adversary behavior is driven by genuine operational conditions and adaptive decision-making rather than predetermined scripts. The scenario does not follow a plan. It follows the environment.

Adversarial teams develop targeting packages based on actual observed network behavior, organizational activity patterns, and the authentic telemetry generated by ShadowSim's user simulation. Defensive teams refine detection logic against genuine, adaptive adversarial activity rather than known indicator sets. Exercise controllers introduce injects and adaptations grounded in real-time operational assessment—what is actually happening in the environment—not what was planned six weeks before execution.

Critically, HyPER's inject framework extends beyond the cyber domain. White Cell operators can introduce kinetic-world events that directly affect the digital environment—a simulated undersea cable cut that degrades external connectivity, a power plant outage that forces failover to backup systems, an ISP disruption that isolates a network segment,

or a physical facility compromise that changes the access landscape mid-exercise. These cross-domain injects force participants to operate under the kind of cascading, multi-domain pressure that characterizes real-world crisis conditions, where cyber defenders rarely have the luxury of responding to threats in isolation from the physical infrastructure their networks depend on.

The result is a training environment that cannot be gamed through memorization. Neither side knows what the other side will do, because neither side's actions are scripted—they emerge from genuine intelligence assessment and operational decision-making under realistic pressure.

Multi-phase campaigns spanning weeks and months create operational continuity that episodic exercises cannot replicate. Nation-state APT playbooks, ransomware operator behavior, supply chain compromise campaigns, and insider threat scenarios all unfold across realistic timelines with authentic escalation patterns and decision points. Participants must manage campaigns strategically—allocating resources, managing fatigue, maintaining intelligence collection, and making decisions whose consequences persist beyond any single exercise session.

Intelligent Automated Opposition Forces

HyPER's operational environment is sustained by two automation platforms working in concert across separate but interdependent dimensions of the contested battlespace. ShadowBreach owns the threat. ShadowSim owns the noise. The interaction between them is what makes the environment genuinely hard to operate in—for both attackers and defenders—in a way that no single-platform range can replicate.

ShadowBreach is HyPER's adversarial engine. It maintains continuous threat actor presence through automated campaign operations that run around the clock, sustained between major exercises without human operator intervention. ShadowBreach-driven adversaries do not pause when a training event concludes—they maintain the footholds they established, continue lateral movement operations,

probe for new access pathways, and adapt their tradecraft based on the defensive responses they observe.

ShadowBreach's tactics, techniques, and procedures are mapped to the MITRE ATT&CK framework, providing a common taxonomy that enables consistent reporting, gap analysis, and after-action assessment. Its operational value, however, lies beyond technique execution. It lies in technique adaptation. When defenders implement new detection logic, ShadowBreach modifies its approach. When a persistence mechanism is discovered and removed, it seeks alternative pathways. When movement patterns trigger alerts, it adjusts timing and method. The adversary evolves as the defender evolves—creating the authentic, continuous arms race that defines real cyber conflict and that scripted scenarios, by design, cannot deliver.

ShadowSim operates across the same environment but controls an entirely different layer: the human activity of the simulated organization. Across the same network where ShadowBreach is conducting its operations, ShadowSim's simulated users are sending emails, transferring files, accessing applications, collaborating across systems, and generating the full spectrum of digital behavior that characterizes a functioning enterprise. This is not cosmetic realism. It is the core analytical challenge HyPER is designed to impose. In real cyber operations, defenders do not identify threats against a quiet background—they identify them within the constant operational noise of an organization going about its business. ShadowSim creates that noise at scale. Defenders must distinguish a ShadowBreach lateral movement campaign from normal inter-department file activity. Hunt teams must find anomalous communication patterns embedded within a dense baseline of legitimate email traffic. The ability to work within that complexity—not around it—is a skill that only develops through sustained practice in a realistic environment.

Human red team operators integrate with ShadowBreach automation during major exercise events, providing the strategic judgment and contextual decision-making that automation alone cannot replicate. Target selection, escalation timing,

operational security decisions under defensive pressure, and the subtle tradecraft that distinguishes sophisticated threat actors from automated tooling all benefit from human expertise. This hybrid model delivers adversarial operations that combine the persistence and scale of automation with the authenticity and adaptability of experienced operators.

USE CASE: Continuous Hunt Operations — Building Genuine Threat Hunting Proficiency

A federal agency's hunt team has completed multiple tabletop and exercise-based training events, but leadership questions whether the team has developed genuine proficiency or simply familiarity with scripted adversary behaviors. They need a training environment where the threat is real enough that team performance cannot be predicted in advance. In HyPER, the hunt team operates continuously against ShadowBreach-driven adversaries that have been building persistence across the environment for weeks. The adversary has developed genuine familiarity with the environment's architecture, established multiple redundant persistence mechanisms, and adapted its behavior based on observed defensive activity—including the team's previous hunting operations. The team does not know what the adversary has already established. They must find it.

Customer Benefit: Hunt team members develop genuine analytical proficiency working against an adversary whose behavioral signatures emerged from authentic operational activity rather than exercise design. Because ShadowBreach adapts to observed defensive countermeasures, teams cannot rely on previously successful hunting methodologies—they must continuously refine their approaches. Over successive training cycles in the persistent environment, leadership gains a realistic picture of actual team capability rather than exercise performance.

Intelligence Competition and Attribution Development

Real cyber conflict is an intelligence competition as much as a technical one. Adversaries build targeting intelligence over months. Defenders develop threat understanding through sustained observation. Counter-intelligence operations create information asymmetries that shape tactical decisions. HyPER replicates all of this through the organic intelligence dynamics that emerge when persistent adversarial and defensive operations unfold in a shared, continuously active environment.

Offensive teams develop comprehensive targeting packages through sustained reconnaissance—building detailed profiles of defensive tool configurations, organizational behavior patterns generated by ShadowSim, and personnel access patterns over time. Defensive teams analyze adversarial behavior continuously, developing genuine threat intelligence from observed activity in the environment. Counter-intelligence operations allow teams to deliberately shape what their opponents observe, introducing deception into the intelligence picture and forcing both sides to validate the reliability of their collected data.

Attribution challenges emerge organically rather than from exercise design. As multiple threat actors—automated and human—operate simultaneously in the environment, defensive analysts must correlate activities across time periods, distinguish between different adversary groups with overlapping infrastructure, and develop attribution assessments based on accumulated behavioral evidence. This mirrors the actual analytical complexity of cyber threat intelligence work in a way that no scripted exercise can replicate.

White Cell Operations, Exercise Control, and White Card Injection

HyPER's White Cell provides the operational oversight layer that sustains the persistent environment across continuous operations. Unlike traditional exercise control functions that operate only during defined exercise windows, HyPER's White Cell maintains 24/7 visibility across the contested battlespace—monitoring adversarial

campaign progression, guiding scenario evolution based on real-time operational assessment, and ensuring that the persistent environment maintains operational fidelity over extended timeframes.

Persistent, autonomous operations are HyPER's default state—but not every training requirement is served by letting the environment run free. Specific exercise objectives, certification requirements, and targeted skill development needs often require a defined event to occur, a particular condition to exist, or a precise training trigger to fire at the right moment. HyPER's white card injection capability gives White Cell operators real-time authority to direct the automation layer toward a specific outcome without pausing the environment or breaking its operational continuity.

White cards are precision injects delivered directly through ShadowBreach, ShadowSim, or both simultaneously. Through ShadowBreach, controllers can trigger a spearphishing campaign against a defined user group to test detection and response procedures, initiate a credential harvesting sequence timed to coincide with a shift change and reduced watch posture, or launch a multi-stage intrusion chain designed to expose a known gap in a team's detection coverage. Through ShadowSim, controllers can introduce anomalous user behavior—a simulated insider suddenly accessing systems outside their established pattern, an unusual volume of data transfers from a specific workstation, or off-hours login activity from an account with elevated privileges—creating the exact conditions needed to exercise a hunt team, validate a detection rule, or test an incident escalation procedure. White cards can also be applied in combination, with ShadowBreach executing an external intrusion while ShadowSim simultaneously surfaces insider behavior anomalies, replicating the multi-vector complexity that stress-tests both technical detection and analyst decision-making.

The defining characteristic of white card injects is that they execute within the persistent environment rather than replacing it. When the inject concludes, the environment does not reset. The foothold established, the anomalous traffic generated, the detection gap exposed—all of it persists and compounds within the continuously evolving

operational picture. Exercise designers gain the precision of a purpose-built training scenario without surrendering the authentic operational context that gives HyPER its training value.

Performance analytics across continuous operations provide assessment fidelity that episodic exercises cannot match. Rather than measuring team performance within a discrete exercise window, HyPER tracks capability development over months—identifying how teams improve under sustained adversarial pressure, where skill gaps persist despite repeated training opportunities, and how organizational processes evolve over time. White card events are logged within this longitudinal record, giving evaluators a complete picture of both organic performance and response to directed training conditions.

ShadowSim: Realistic Operational Environment

The contested terrain in HyPER is not a generic network range populated with placeholder traffic. It is a living operational environment driven by ShadowSim, our traffic automation platform, which generates realistic user behavior across the simulated organization—emails, file transfers, inter-system communications, web activity, collaboration workflows, and the full spectrum of digital activity that characterizes a functioning enterprise. This authentic operational noise is not cosmetic. It is structurally essential to the training value HyPER delivers.

The analytical challenge that defines real cyber operations is not identifying malicious activity in isolation—it is identifying malicious activity within the constant background of legitimate organizational behavior. ShadowSim creates that challenge. Defenders must distinguish between a ShadowBreach-driven lateral movement campaign and normal file sharing between departments. Hunt teams must identify anomalous communication patterns within a dense, realistic baseline of legitimate email and collaboration traffic. The ability to make those distinctions, under operational pressure, is a skill that can only be developed against a realistic environment—not a quiet range.

ShadowSim's behavioral profiles evolve over time, creating dynamic baselines that prevent both attackers and defenders from operating on static assumptions. User behavior shifts as the simulated organization grows, adopts new technologies, and modifies its workflows. Attackers must continuously update their understanding of what normal looks like in order to blend into it effectively. Defenders must continuously recalibrate their anomaly detection as the baseline shifts. This evolutionary dynamic ensures that the training environment never becomes a known quantity that can be gamed through familiarity.

Agency-specific network architectures and realistic enterprise topologies, including SCADA and ICS environments for critical infrastructure scenarios, can be replicated within HyPER, with ShadowSim populating them with operationally appropriate user behavior profiles. The result is a training environment that mirrors not just the technical architecture of the organization being simulated, but the human activity patterns that create both the operational context and the analytical challenge that real cyber defenders navigate every day.

The Market: Who Needs Persistent Operational Training

DoW Cyber Mission Forces

The Cyber Mission Force was built to conduct persistent operations against sophisticated adversaries. Its training environment should reflect that operational reality. Cyber Protection Teams, Combat Mission Teams, and National Mission Teams all require sustained engagement against adaptive, persistent opposition—not periodic exercises against scripted scenarios. HyPER provides the operational environment where CMF elements can develop and validate the capabilities they need for the missions they are actually assigned.

Other Federal Agencies

DHS, FBI, and the broader federal cyber enterprise face persistent threats that operate across organizational boundaries and exploit interagency coordination gaps. HyPER's cross-agency exercise capabilities and realistic information sharing scenarios provide federal agencies with training environments that reflect the authentic complexity of inter-organizational incident response—including the jurisdictional sensitivities, information sharing limitations, and competing priorities that shape real federal cyber operations. These are agencies we already serve, and HyPER addresses training gaps that no existing solution closes.

Intelligence Community

Forward intelligence operations and expeditionary processing demand training environments where intelligence competition is a genuine operational activity rather than an exercise construct. HyPER's persistent model—with adversaries that develop authentic institutional knowledge of the environment over time and defenders building real threat understanding through sustained observation—provides IC elements with the analytical depth and operational complexity that scripted exercises structurally cannot deliver.

Partner Nations and FMS Programs

Building genuine cyber defense capability in partner nations requires more than delivering training content—it requires providing the operational environment to develop and sustain that capability. HyPER's persistent model, paired with HYDRA's deployable infrastructure, allows FMS programs to deliver not just episodic training but a living operational environment that partner nation forces can use continuously to develop and maintain readiness. Our established relationships in INDOPACOM, SOUTHCOM, and with NATO partners position HyPER as a natural complement to existing theater security cooperation engagements.

The Underlying Demand Signal

Across all of these segments, the demand driver is the same: the national security cyber enterprise has accepted that episodic training does not produce the persistent readiness that persistent threats demand. The question is no longer whether continuous operational training environments are needed. The question is who can actually build and operate one. HyPER answers that question with production-grade infrastructure, proven operational methodology, and a team that has been building and running cyber ranges for DoW and federal customers for over 15 years.

Why HyPER: The Operator Advantage

HyPER is not a product developed by a training company that decided to add persistent operations features. It is the operational evolution of capability that we have been building and refining in direct support of DoW and federal cyber missions for over a decade and a half. That distinction matters.

Our cyber operators don't just build training environments—they operate in them. Our red team operators have executed real-world adversary emulation against DoW and federal customers, giving them the authentic attacker perspective that makes ShadowBreach's adversarial behavior genuinely realistic rather than technically functional. Our defensive operators have stood watch in contested environments under operational pressure, giving them the practitioner knowledge that informs how HyPER's defensive training scenarios develop genuine skill rather than scripted proficiency. The tradecraft built into HyPER's design comes from practitioners who have operated under the same conditions they are now building training environments to replicate.

Our platform ecosystem—HYDRA, ShadowBreach, and ShadowSim—is not a collection of third-party tools integrated for training purposes. These are proprietary capabilities that we developed to solve real operational problems, that we operate in support of actual DoW missions, and that we continuously improve based on operational experience. HyPER brings these capabilities together into a coherent

persistent training environment that no competitor can replicate with commercial-off-the-shelf components.

Our customer relationships reflect the trust that operational delivery creates. DoW, DHS, FBI, and international partners have relied on our experts not just for technology but for operational outcomes—exercises conducted, capabilities built, missions supported. HyPER extends that operational partnership into a persistent model, providing customers not just with a training capability but with a sustained readiness development relationship built on the same operational credibility that defines every engagement.

The Path Forward

The cyber threat environment has permanently outpaced episodic training. Adversaries operate continuously, adapt persistently, and build institutional knowledge about their targets over time. Training environments that reset between events cannot develop the sustained readiness that sustained threats demand.

HyPER closes that gap. It provides the persistent, adaptive, intelligence-driven training environment that the DoW and federal cyber enterprise need—a living battlespace where every training cycle builds on the last, every defensive improvement is tested against an adversary that continues to operate, and genuine operational experience accumulates over time rather than evaporating when the exercise window closes.

We have the infrastructure, the operational methodology, and the practitioner expertise to deliver it. Our team has built and operated cyber ranges for DoW and federal customers for over fifteen years. We have developed the tools that power HyPER through real operational experience. And we have the operational relationships with the customers who need this capability most.

The demand signal is clear. The capability exists. We're the team that can deliver it.

Explore more cyber capabilities and products at markonsolutions.com/full-spectrum-cyber.