

Cyber Fusion Centre — A NextGen, AI-Powered SOC for New World Threats



Enterprises across banking, healthcare, retail and technology are under pressure to detect and stop AI-driven attacks while security teams stay stretched thin, tool stacks stay fragmented, and compliance expectations keep climbing. Doing all of this at once, with a patchwork of vendors, is exceptionally hard.

This is where Persistent's Cyber Fusion Centre-led Managed SOC practice partners with Palo Alto Networks — a NextWave Platinum MSSP partner relationship built on the Cortex platform — to give enterprises one accountable partner instead of a patchwork of vendors.

Why This Offering — Solving Enterprise Security Operations Needs

The Persistent–Palo Alto joint offering exists to solve a real and immediate problem: enterprises juggle detection, response and modernization as separate initiatives, and struggle to operationalize any of them fast enough to stay ahead of threats.

Persistent brings differentiated strengths to close this gap.



Native AI Platform, Not an Add-On

with full context across endpoints, network, identity and cloud in one unified incident queue — driving a 70% reduction in false positives and 30% savings in total cost of ownership.



Sector-Tuned Detection Content

through PiSOC, Persistent's pre-built library tuned for sectors like banking (SWIFT fraud) and healthcare (PHI/EHR), spanning 300+ detection rules, 25+ automation playbooks and 35+ threat-hunting playbooks.



Premium Threat Intel & UEBA at No Extra Cost

through Unit 42 threat feeds and AI-driven behavior analytics built into the platform, so clients skip unreliable open feeds and separate UEBA tooling.



Outcome-Based SLAs, Not Effort-Based Billing

measured against Mean Time to Response under 15 minutes, Escalation under 30 minutes and a False Positive Rate under 25%, backed by one-click AI response actions.

In short, this offering gives enterprises one partner for AI-driven detection, response and modernization — the combination most staffing-only MSSPs cannot offer alone.

Key Use Cases — Real-World Scenarios

This Offering Solves

This Managed SOC offering addresses enterprise security needs across detection, response, modernization and compliance, including:



When Alerts Outpace Analysts

A stretched SOC team drowns in thousands of daily alerts from a fragmented stack, while sophisticated attackers slip through the noise. Persistent's Cyber Fusion Centre, built on Cortex XSIAM and XSOAR, converges detection, triage and response into one AI-native workflow — Full-Stack MSSP-aaS or Hybrid MSSP (BYOS) — run through Persistent's own PiCSM ITSM and PiSOC use-case library.



A SIEM That Can't Keep Up

A legacy QRadar deployment strains under data volume and still can't correlate across domains fast enough to stop a fast-moving intrusion. Persistent's "Beyond QRadar" offering migrates the environment to Cortex XSIAM's AI-driven detection and correlation — Persistent has already completed a production migration for an existing QRadar-on-Cloud (QROC) customer.



One Console Instead of Ten Tools

An analyst juggles separate consoles for SIEM, XDR, threat intel and automation, losing precious minutes stitching the story together during an active incident. Cortex XSIAM delivers AI-driven detection, analytics and correlation while Cortex XSOAR handles orchestration and response, backed by Unit 42 threat intelligence, in a single console.



Modernizing Without Starting Over

A regulated institution wants AI-driven detection and response but can't justify ripping out a SIEM it just finished paying for. The SOAR-Led SOC on Your SIEM model (BYOS + XSOAR) layers automation and response on top of the existing SIEM, paired with Persistent's Governance, Risk & Compliance practice, so modernization doesn't introduce new audit risk.



When an Incident Needs Forensics, Not Just Containment

A ransomware incident is spreading fast, and the team must preserve forensic evidence while containing the damage in real time. Unit 42's Digital Forensics and Incident Response (DFIR) team owns and manages the engagement — evidence preservation, root-cause analysis and recovery — available as a paid add-on to the core Managed SOC, with Persistent coordinating the response end-to-end.

Better Together — Palo Alto, Persistent and the Customer

Where the risk shows up in security operations, who responds, and how the partnership pays off over time.

Where This Shows Up, and Who Responds

The Scenario An alert fires at 2 a.m. flagging unusual lateral movement across a hybrid environment — legacy tools can't correlate the signal across endpoint, network and identity fast enough.	The Scenario A legacy QRadar SIEM can't keep pace with data volume or correlate across domains quickly enough to catch a fast-moving intrusion.	The Scenario A regulated institution needs AI-driven detection and response without abandoning a SIEM investment it can't yet retire.	The Scenario A ransomware incident is spreading fast, and the team must preserve forensic evidence while containing the damage in real time.
Palo Alto Cortex XSIAM ingests and correlates telemetry from endpoint, network, identity and cloud in real time, with AI stitching the story together automatically.	Palo Alto Cortex XSIAM replaces static correlation rules with AI-driven detection built to ingest at scale.	Palo Alto Cortex XSOAR layers automation and orchestration on top of the client's existing SIEM (BYOS).	Palo Alto Unit 42's Digital Forensics and Incident Response (DFIR) team owns and manages the engagement — evidence preservation, root-cause analysis and recovery.
Persistent Runs the 24/7 Cyber Fusion Centre that triages, investigates and closes the incident against agreed SLA targets.	Persistent Has already executed a production QRadar-to-XSIAM migration for an existing QRadar-on-Cloud customer, and runs the cutover with minimal disruption.	Persistent Pairs the rollout with its Governance, Risk & Compliance practice so modernization is evidenced, not just implemented.	Persistent Coordinates the engagement end-to-end, feeding Unit 42's findings back into the Cyber Fusion Centre so containment and long-term detection stay in sync.

Digital Forensics and Incident Response (DFIR) is delivered by Palo Alto's Unit 42 team as a paid add-on to the core Managed SOC engagement, coordinated by Persistent.

One Partner, Every Stage — From First Assessment to Ongoing Operations

Pre-implementation

Palo Alto

Risk-scoring and environment discovery show exactly what's running today across endpoint, network, identity and cloud.

Persistent

The SOC health check and maturity assessment turn that data into a scoped roadmap, sized to real risk.

Customer value

A right-sized business case, not a guess.

Implementation

Palo Alto

XSIAM and XSOAR deploy in monitor mode first, so nothing breaks before it is understood.

Persistent

Palo Alto-certified engineers who have run this rollout before handle configuration, integration and change management.

Customer value

Faster time to value — the client is not paying to learn on its own environment.

Post-implementation

Palo Alto

The platform keeps monitoring, detecting and enforcing policy as threats and usage evolve.

Persistent

Runs day-to-day Cyber Fusion Centre operations, tunes detections continuously, and keeps compliance evidence current.

Customer value

Continuous protection and audit-readiness, without growing the client's own security headcount.

The Persistent Difference — Why Leading Enterprises Choose Us

Beyond any single vendor certification, here is the depth institutions are actually buying when they choose Persistent for Managed SOC:



Platinum Partner at Scale

NextWave Partner Program, Platinum tier, MSSP & Resell agreement across the US, UK and India — delivered by dedicated Palo Alto-certified teams holding 35+ technical certifications across XSIAM and XSOAR, plus 10+ sales certifications.



Proven Migration Expertise

Deep competency in QRadar-to-XSIAM migrations, including a completed production migration for an existing QRadar-on-Cloud (QRoC) customer — a shipped engagement, not just a slide claim.



IP & Accelerators Built for SOC Speed

PiCSM (Persistent's integrated ITSM) and the PiSOC use-case library carry 300+ pre-built detection rules, 25+ automation playbooks and 35+ threat-hunting playbooks, enabling up to 2x faster transition and 5x faster fine-tuning versus a from-scratch build.



A Dedicated Cybersecurity Organization

Persistent was named a Leader in ISG Provider Lens™ 2025 for Cybersecurity Services, backed by 35+ years of security-practice experience and a partner ecosystem of 60+ alliances across 7 strategic partnerships.



One Accountable Partner Instead of Many Vendors

Where point solutions leave institutions managing a dozen vendor relationships, Persistent's Cyber Fusion Centre puts platform, content and 24/7 practitioner-led operations under one team and one SLA.

Outcomes and Business Benefits — What Customers Gain

With this combined offering, enterprises unlock tangible, board-level value.



Stronger Security Posture

Native AI context across endpoint, network, identity and cloud drives up to a 60% reduction in false positives, sharpening signal for faster analyst response.



Higher Platform Utilization

Clients report up to an 80% increase in SOC utilization once Cortex XSIAM and XSOAR are fully operationalized against their environment.



Faster Detection & Response

Converged detection and automated response across the Cyber Fusion Centre drive up to a 50% reduction in Mean Time to Respond (MTTR).



Reduced Operational Load

Persistent's practitioner-led managed services cut platform cost by up to 30% and reduce internal team dependency, improving SLA adherence.



A SOC Built to Mature Over Time

Phase-wise roadmaps and SOC maturity assessments help institutions advance detection and response capability without disrupting core operations.

Figures reflect Persistent's Cyber Fusion Centre delivery benchmarks across MSSP engagements.

Your Next Step in Managed SOC

If your organization is ready to:

- Consolidate a fragmented security stack onto one AI-native platform
- Reduce fraud, breach and third-party risk exposure
- Modernize a legacy QRadar or SIEM environment without disrupting operations
- Adopt AI-driven detection and response with confidence, at enterprise scale
- Stand up secure, day-one operations for a carve-out or divestiture
- Move from reactive monitoring to outcome-based, 24/7 SOC operations

Then Persistent's Cyber Fusion Centre-led Managed SOC, powered by Palo Alto Networks, is your ideal partner framework.

Let's build your AI-driven Cyber Fusion Centre together.

USA

Persistent Systems, Inc.
2055 Laurelwood Road, Suite 210
Santa Clara, CA 95054
Tel: +1 (408) 216 7010
Email: info@persistent.com

India

Persistent Systems Limited
Bhageerath, 402
Senapati Bapat Road
Pune 411016
Tel: +91 (20) 6703 0000

About Persistent

Persistent Systems (BSE: 533179 and NSE: PERSISTENT) is a global services and solutions company delivering AI-led, platform-driven Digital Engineering and Enterprise Modernization to businesses across industries. With over 26,500 employees located in 18 countries, the Company is committed to innovation and client success. Persistent offers a comprehensive suite of services, including software engineering, product development, data and analytics, CX transformation, cloud computing, and intelligent automation. The Company is part of the MSCI India Index and is included in key indices of the National Stock Exchange of India, including the Nifty Midcap 50, Nifty IT, and Nifty MidCap Liquid 15, as well as several on the BSE such as the S&P BSE 100 and S&P BSE SENSEX Next 50. Persistent is also a constituent of the Dow Jones Sustainability World Index. The Company has achieved carbon neutrality, reinforcing its commitment to sustainability and responsible business practices. Persistent has also been named one of America's Greatest Workplaces for Inclusion & Diversity 2025 by Newsweek and Plant A Insights Group. As a participant of the United Nations Global Compact, the Company is committed to aligning strategies and operations with universal principles on human rights, labor, environment, and anti-corruption, as well as take actions that advance societal goals. With 468% growth in brand value since 2020, Persistent is the fastest-growing IT services brand in 'Brand Finance India 100' 2025 Report.