The Future of SOC: AI Powered by BARİKAT and Palo Alto Networks

Leading the Way in Modern Security Operations

Many organizations in the Middle East are rethinking the way they manage and run critical security operations centers (SOCs). As the region becomes a focal point for cyberattacks due to its geopolitical significance, abundant natural resources, and rapid adoption of digital technologies, the need for robust cybersecurity measures has never been more critical. Reports indicate that 55% of Middle Eastern companies prioritize mitigating digital and technology risks over the next year, exceeding the global average of 53%.[1]

The region's digital transformation continues as a strategic means of diversifying the economy and reducing dependence on raw materials. Enhancing cybersecurity and protecting critical infrastructure are key to ensuring the resilience of official digital initiatives.

Additionally, the proliferation of devices and an increasingly distributed IT environment create a wider attack surface, making organizations more vulnerable to cyberthreats. The global cybersecurity workforce gap was 4 million in 2023, with a significant shortage of skilled security professionals in the Middle East.[2] This shortage left businesses vulnerable to increasingly sophisticated cyberthreats. Transforming SOCs to be more agile, adaptive, and equipped with AI-powered capabilities is essential to stay ahead of these evolving threats.

Evolve to a Modern SOC Experience with BARİKAT and Palo Alto Networks

Rethink your SOC with the combined expertise of BARİKAT and Palo Alto Networks. Our partnership offers advisory, technical, and managed services based on the Palo Alto Networks Cortex® autonomous SecOps platform. Together, we provide the roadmap, skills, and AI-powered SOC your organization needs to stay ahead of evolving cyberthreats.

BARİKAT, a leader in cybersecurity, has a significant presence in Turkey and internationally. With over 600 corporate customers worldwide and partnerships with 40 vendors, BARİKAT stands for excellence in cybersecurity, leveraging deep technical expertise and a commitment to continuous improvement.

The key differentiator of BARİKAT is their ability to integrate Palo Alto Networks advanced technologies with their in-house developed solutions, creating a seamless and highly effective SOC experience. Clients demand tailored solutions for their specialized needs, and with hundreds of deployments, BARİKAT offers the depth of experience they need to ensure their security operations are optimized for maximum efficiency and effectiveness.

The BARİKAT engineering teams hold certifications across Palo Alto Networks Cortex product lines. The platform developed by BARİKAT's R&D unit builds on this by integrating Palo Alto Networks solutions and providing additional capabilities such as asset monitoring, SLA management, and attack surface monitoring.

BARİKAT, which is accredited by the Turkish Ministry of National Defense and NATO, ensures robust security solutions. BARİKAT Academy plays a crucial role in training both analysts and customer teams by offering continuous learning programs, workshops, and certifications to keep their skills up to date. This unique approach combines Palo Alto Networks advanced technologies and the in-house developed solutions from BARİKAT to create a seamless and highly effective SOC experience for both our customers.

[1] "Rising Threat Of Cyber Attacks In The Middle East," a&s Middle East, January 20, 2025.

[2] "ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap," ISC2, November 3, 2023.

[3] "Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities," World Economic Forum, January 13, 2025.

Stay Ahead of Evolving Threats with a Tailored SOC Strategy

As AI technology advances, it is used to both enhance cybersecurity defenses and create more sophisticated cyberattacks, making the threat landscape more complex. This makes having a clear and effective security strategy—tailored to the unique needs of the business—critical. BARİKAT emphasizes the importance of teamwork, integrating each customer's needs and challenges into our solutions. The process includes detailed assessments, tailored recommendations, and implementation, as well as continuous support to ensure our customers achieve their security goals. BARİKAT leverages Palo Alto Networks advanced security technologies and complements these with its own in-house developed software to address specific pain points.

> "The unprecedented level of sophistication in cyberthreats enabled by emerging technologies enhances the malicious actors' ability to operate scams and social engineering attacks, generate disinformation, and execute ransomware at a pace, scope, and scale never seen before. Nearly 47% of organizations cite adversarial advancements powered by GenAI as their primary concern."[3]
>
> **– World Economic Forum 2025**

Every engagement starts with a risk-based assessment of each client's current security posture, leveraging both in-house frameworks and established standards such as ISO/IEC 27001 and NIST. BARİKAT then develops a multiphase roadmap, incorporating Palo Alto Networks Cortex for detection, orchestration, and response.

Once aligned on the strategic plan and implementation timeline, BARİKAT executes against the priorities identified in the jointly developed roadmap and implements a tailored SOC transformation solution.

By combining Palo Alto Networks Cortex with the BARİKAT tailored managed services, we deliver stronger threat detection, faster response, and greater visibility across complex environments. The platform developed by BARİKAT's R&D unit builds on this by adding asset monitoring, SLA tracking, and proactive attack surface management, helping organizations reduce risk, maintain compliance, and stay ahead of evolving threats. Through seamless integration of the Cortex platform, external attack surface management (EASM), operational technology (OT) sensors, and custom APIs in the BARİKAT AI-driven SOC, our joint solution provides a complete, intelligent security approach tailored to each organization's unique needs.

BARİKAT leverages the powerful AI-enabled automation capabilities of the Palo Alto Networks Cortex platform to handle time-consuming, resource-intensive SOC tasks and processes. The platform knits data together from across the entire IT environment—including cloud, network, devices, and applications—to provide a comprehensive view of an organization's security estate.

Business Benefits

- **Enhances the security posture:** Strengthen your security stance and reduce the risk of cyberthreats.
- **Improves operational efficiency:** Focus on core business activities with confidence, knowing your cybersecurity needs are met.
- **Enhances threat detection and response:** Using real-life threat simulations, ensure earlier and more accurate detection and response.
- **Achieves a sustainable security transformation:** Define an organization-centric roadmap for continuous improvement and adaptation to evolving threats, as well as ensure long-term benefits and resilience against cyberthreats.

[3] "Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities," World Economic Forum, January 13, 2025.

Access Top-Tier Expertise for Advanced SOC Management

Today's teams need to be equipped with the necessary expertise to manage and evolve their SOCs effectively. The rapid pace of cybersecurity advancements demands continuous skill development. BARİKAT, in partnership with Palo Alto Networks, plays a key role in providing continuous training to both analysts and customer teams.

Through BARİKAT Academy, a range of learning programs, workshops, and certifications are offered to teams to keep analysts' skills up to date with the latest cybersecurity advancements. These training initiatives focus on real-world threat scenarios, providing analysts with hands-on experience that they can apply when adopting proven implementations and use cases to meet each organization's specific needs.

> "Since 2024, the cyber skills gap has increased by 8%, with two in three organizations lacking essential talent and skills to meet their security requirements; only 14% of organizations are confident that they have the people and skills they need today."[4]
>
> – World Economic Forum 2025

BARİKAT also offers temporary workforce replacement with level-one and level-two analysts to ensure the security posture has no gaps. Çati (a shared services arm of BARİKAT) provides development and ongoing certification opportunities (e.g., Palo Alto Networks Certified Network Security Engineer [PCNSE]). This comprehensive approach ensures that organizations have access to highly skilled professionals who are well versed in the latest cybersecurity technologies and practices. BARİKAT maintains a high staff retention rate, with many analysts specializing in OT security, cloud security, and advanced threat hunting, which in turn, enriches its SOC expertise.

An upcoming expansion to the Netherlands is another investment in the ability for BARİKAT to provide a "follow-the-sun" approach—enabling 24/7 coverage and shared expertise across regions—to help mitigate local talent shortages.

Business Benefits

- **Effectively manage cybersecurity operations:** Address skills gaps to ensure security operations run smoothly and effectively.
- **Commit to continuous learning and development:** Benefit from the latest advancements in cybersecurity through ongoing education initiatives.
- **Reduce analyst workload:** Use Cortex XSOAR® playbooks and automated responses to enable your smaller teams to manage larger environments effectively.
- **Grow a skilled professional pipeline:** Build a pipeline of skilled professionals by partnering with Palo Alto Networks and local universities for joint training programs and internships.

[4] "Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities."

AI-Powered Threat Detection for Stronger SOC Security

> "There is a paradox between the recognition of AI-driven cybersecurity risks and the rapid implementation of AI without the necessary security safeguards to ensure cyber resilience. While 66% of organizations expect AI to have a major impact on cybersecurity in 2025, only 37% report having processes in place to assess the security of AI tools before deployment."[5]
>
> – World Economic Forum 2025

AI-powered security operations are essential because they provide advanced threat detection, response, and management capabilities, ensuring your organization is protected against the latest cyberthreats. The integration of AI-driven security operations enhances efficiency and effectiveness.

BARİKAT leverages the Palo Alto Networks Cortex platform and combines innovative solutions to offer a modern SOC that uses AI-driven security operations. This integration allows for real-time threat analysis, automated responses, and continuous monitoring. These software modules verify the effectiveness of playbooks and correlation scenarios, ensuring optimal performance.

The value of the partnership comes from the combination of the Palo Alto Networks product portfolio and BARİKAT SOC to offer end-to-end security in a single, AI-enabled platform. It uniquely provides advanced orchestration and automation (Cortex XSOAR), extended detection and response (Cortex XDR®), proactive attack surface management (Cortex Xpanse®), and AI-powered SOC (Cortex XSIAM®) within one unified platform.

Additionally, the BARİKAT custom-developed software complements the Palo Alto Networks product portfolio, providing additional capabilities such as attack surface monitoring and asset management. Standardized processes around threat intelligence ingestion, correlation, and incident escalation within a single AI-powered platform ensure consistent and rapid detection across client environments.

BARİKAT AI-driven security tools enhance the efficiency and effectiveness of each organization's SOC. Together, we deliver solutions that are capable of identifying and mitigating threats faster than traditional methods to ensure proactive security measures. By leveraging Palo Alto Networks next-generation SOC analytics, BARİKAT can identify hidden patterns and tactics, techniques, and procedures (TTPs) used by advanced adversaries, enhancing preemptive defense.

Business Benefits

- **Reduce response times:** Experience faster response times, ensuring timely action against potential threats. Organizations frequently report better mean-time-to-detect (MTTD) metrics after adopting AI-powered solutions from BARİKAT.
- **Enhance accuracy when identifying threats:** Get more effective security measures.
- **Increase predictability in detection and triage:** Ensure consistent and reliable detection and triage processes with automation.
- **Minimize the impact of cyber incidents:** Maintain business continuity by reducing downtime and operational disruption.
- **Drive continuous improvement:** Adapt to evolving threats with resilient future solutions.

[5] "Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities."

About BARİKAT

As a regional cybersecurity leader, BARİKAT is committed to securing the digital future through focused expertise and innovation. Trusted by hundreds of organizations, we deliver end-to-end security services across managed security, threat detection, and consulting. Our exclusive focus on cybersecurity empowers businesses to build resilient digital infrastructures. Learn more at www.barikat.com.tr.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

Value of the BARİKAT and Palo Alto Networks Partnership

- **An innovation-led partnership:** Ongoing collaboration with Palo Alto Networks, focusing on joint innovation to enhance cybersecurity solutions.
- **Proven expertise:** Engineering team certifications from BARİKAT and hands-on experience across the Palo Alto Networks Cortex product lines, including PCNSE certification.
- **Recognized excellence:** BARİKAT has received numerous industry awards and recognitions, including local recognition for the best managed security service providers (MSSPs) and specialized OT security services. Notable credentials include:
  - Accreditation by the Turkish Ministry of National Defense and NATO.
  - R&D center accreditations from the Turkish Ministry of Industry and Technology.
  - Holder of the E-Turquality logo.
- **Comprehensive security solutions:**
  - Operates SOCs in Turkey and the Gulf Cooperation Council (GCC), with plans to expand to the Netherlands (EU).
  - Proven experience in OT-enabled security to support critical infrastructures where both IT and industrial environments need protection.
  - SOC teams that undergo rigorous, ongoing training with actual threat simulations, ensuring deep hands-on experience.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com