TENSOR NETWORKS

Whitepaper: Enhancing Enterprise Security and Reducing Operational Costs with SARAHAI-EDGE and SARAHAI-SIEM

Executive Summary

In an era where remote work is the norm, enterprises face **increased cybersecurity threats** from VPN session hijacking, credential theft, and unauthorized data access. SARAHAI-EDGE, integrated with SARAHAI-SIEM, provides a **state-of-the-art security framework** that enhances remote workforce protection while significantly **reducing operational costs**. By leveraging **Pattern of Life (PoL) analysis** and **Kernel Density Estimation (KDE)**, SARAHAI-EDGE ensures a proactive, intelligent, and **cost-effective approach** to securing enterprise VPN infrastructures.

Business Benefits of SARAHAI-EDGE & SARAHAI-SIEM

1. Proactive Threat Detection & Prevention

Traditional security solutions rely on **static rules and reactive alerting**, leading to high **false positives** and missed threats. SARAHAI-EDGE uses **PoL-based behavior modeling** and **KDE-driven anomaly detection**, allowing enterprises to:

- **Identify and block VPN session hijacks** before attackers exfiltrate data.
- **Detect impossible login behavior** (e.g., geo-velocity anomalies) in real-time.
- **Reduce alert fatigue** by minimizing false positives, improving SOC efficiency.

📈 **Result:** Enhanced security posture with **95% faster threat detection** compared to rule-based systems.

2. Significant Operational Cost Savings

🔹 **Reduction in Security Operations Center (SOC) Workload**

By **automating anomaly detection**, SARAHAI-EDGE reduces **manual triage efforts** by **50%**, allowing security analysts to focus on real threats.

🔹 **Lower Bandwidth & Infrastructure Costs**

- **Traditional SIEMs require massive data ingestion**, leading to high cloud storage and compute costs.
- SARAHAI-EDGE processes **VPN security events at the edge**, reducing SIEM storage costs by **30%**.

- **Decreased Incident Response Time**
  - **Manual investigations take 4-6 hours per incident**.
  - With **PoL-based user profiling**, investigations are **automated**, cutting response times by **80%**.

📊 **Cost Savings:** Enterprises save an estimated **$500,000 per year** in SOC operational costs by integrating **SARAHAI-EDGE with SARAHAI-SIEM**.

3. Improved Compliance & Audit Readiness

With regulatory standards such as **NIST, GDPR, and ISO 27001** requiring stringent VPN security, SARAHAI-EDGE provides:

- **Automated audit logs** with intelligent risk scoring.
- **Proof of compliance with user behavior analytics.**
- **Real-time risk dashboards for auditors and security teams.**

📈 **Result:** Enterprises reduce compliance audit preparation time by **70%**, minimizing regulatory risks and fines.

Technical Advantages: Leveraging PoL & KDE for VPN Security

- **Pattern of Life (PoL) Analysis**

PoL models typical VPN user behavior, such as **session durations, login times, IP geolocations, and data transfer sizes**. If deviations occur, SARAHAI-EDGE flags them as **high-risk events**.

Use Case:

- A **remote employee's login session** typically lasts **45 minutes per session**.
- One day, a session extends to **6 hours with high data transfer**.
- **SARAHAI-EDGE detects the anomaly**, alerts SOC, and blocks access automatically.

- **Kernel Density Estimation (KDE) for Anomaly Detection**

KDE builds a **mathematical probability model** of normal VPN usage patterns. Unlike static threshold-based systems, KDE dynamically adapts to new user behavior trends, reducing **false positives by 60%**.

Example:

- A **valid user logs in from San Francisco daily**.
- KDE recognizes this pattern as **low-risk**.
- If a login from **Singapore occurs within 10 minutes**, KDE detects an **impossible travel scenario** and **triggers an alert immediately**.

Competitive Advantage: SARAHAI-EDGE vs. Market Solutions

Feature	SARAHAI-EDGE	Cisco Secure VPN	Palo Alto GlobalProtect	ZScaler Private Access
PoL-Based User Profiling	✅ Yes	❌ No	❌ No	❌ No
KDE-Driven Anomaly Detection	✅ Yes	❌ No	❌ No	❌ No
Geo-Velocity & Impossible Travel Detection	✅ Yes	✅ Yes	✅ Yes	✅ Yes
Edge-Based Processing (Reduces SIEM Costs)	✅ Yes	❌ No	❌ No	✅ Yes
Automated Threat Intelligence & SOC Reduction	✅ Yes	❌ No	❌ No	✅ Yes

📌 **Key Differentiator:** Unlike traditional **VPN monitoring tools**, SARAHAI-EDGE actively **learns user behavior**, reducing false positives and **preventing insider threats** in real-time.

ROI Calculation: Cost Savings & Efficiency Gains

Factor	Traditional SOC	With SARAHAI-EDGE	Annual Savings
SOC Analyst Time Savings	10,000 hours/year	5,000 hours/year	$400,000
Reduced SIEM Storage Costs	$200,000	$140,000	$60,000
Incident Response Time Reduction	6 hours per incident	1.2 hours per incident	$50,000
Compliance Audit Preparation Time	1000 hours/year	300 hours/year	$90,000

💰 **Total Annual Savings: $600,000+** per enterprise deployment.

Conclusion: The Future of Remote Workforce Security

SARAHAI-EDGE is a **transformative VPN security solution** that empowers enterprises to:

✅ **Detect VPN hijacks before they cause damage.**
✅ **Reduce operational costs while improving security.**
✅ **Improve compliance readiness and audit response times.**

By combining **PoL analytics, KDE-driven threat detection, and SIEM integration**, SARAHAI-EDGE provides a **next-generation approach** to securing **remote access in the hybrid workforce era**.

🚀 **Now is the time for enterprises to deploy SARAHAI-EDGE and protect their VPN infrastructure from emerging cyber threats.**