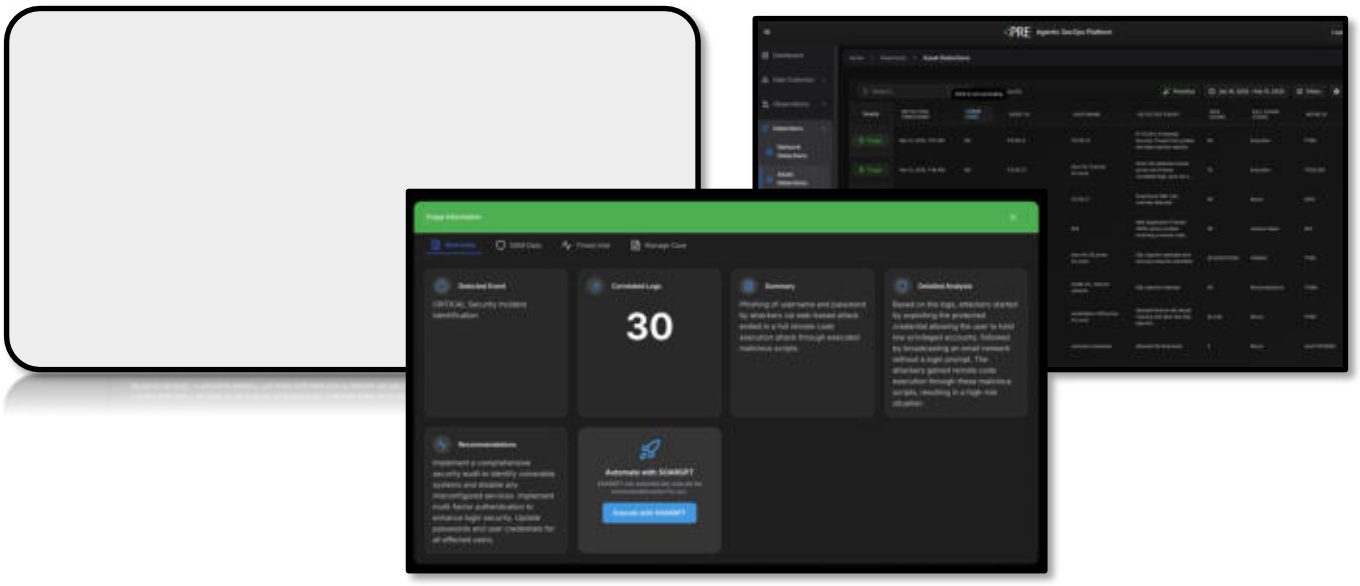
AI Native SecOps for Predictive & Proactive Cybersecurity

PRE Security presents our AI Native SecOps solution that revolutionizes modern cybersecurity operations with predictive, generative, and agentic AI technologies. PRE delivers comprehensive security workflow capabilities, solving many of the issues that have lingered with traditional “hand built” architectures – starting from ingesting data from any source to correlating it across all environments, providing advanced, generative detections and predictions, and automating response and preventative actions. Powered by our purpose-built large language models, PRE Security accelerates and enhances threat detection, incident response, and mitigation actions across all of your digital infrastructure. With PRE Security, your SecOps shifts left, from reactive to proactive, fortifying your defenses against the constantly evolving threat landscape.

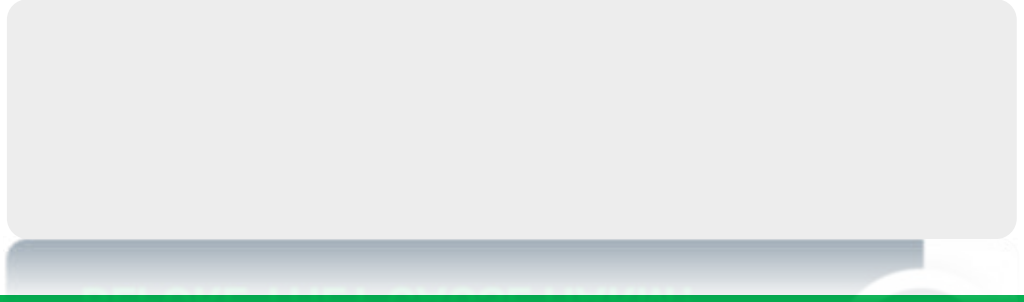


Enhance or replace your existing SIEM or XDR with PRE Security now!

Traditional SIEM and XDR SecOps architectures demand constant rule updates, manual tuning, and maintenance to keep pace with emerging threats. Even with regular updates, these systems are inherently static, often missing new attack patterns or falling behind rapidly evolving threats, especially from fast moving AI-driven adversaries.

PRE Security’s AI Native platform eliminates this problem by continuously learning from every interaction with your environment, evolving with the threat landscape. Our system builds a dynamic understanding of your organization’s unique vulnerabilities, risks, and threat patterns, ensuring detection and response capabilities improve over time – without needing manual design and input at every step.

- **Why It Matters**: With PRE Security’s purpose-built, continuously learning AI, your security operations grow more intelligent every day – keeping you ahead of the next attack vector without needing constant manual updates or rule adjustments.



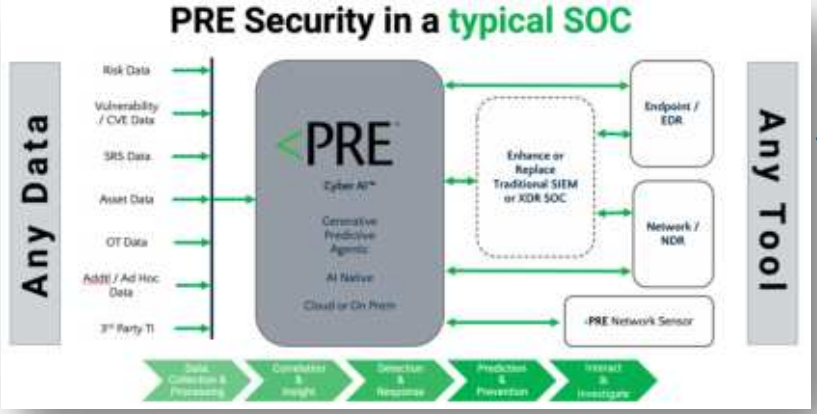
From the inventors of Open XDR

PRE Security Product Datasheet

Why PRE Security?

Traditional SIEM based SecOps architectures simply can't keep up with today's complex, rapidly increasing, and cleverly evolving threats. These outdated solutions are limited in scope and reactive by nature, resulting in delayed responses and missed threats. Furthermore, they are often built on expensive ingestion based pricing models that inhibit the ingestion of valuable data that can provide context in the short sighted need to control costs.
PRE Security redefines SecOps with its AI Native architecture reimagined to solve real SecOps challenges:

- < Generative AI: Creative, dynamic correlations, unexpected detections, Parserless™ ingestion and more.
- < Predictive AI: Why wait until you are breached to Detect & Respond when you can Predict & Prevent™?
- < Agentic AI: Automated, reasoned actions, responses and automations.



Multiple Use Cases:

< SIEM Replacement
modernize your old infrastructure w/ all new AI Native Secops from PRE Security.

< SIEM Enhancement
Pre-process logs to reduce your SIEM ingestion requirements, improve data normalization.

< Generative XDR + Predictions
Upgrade your XDR to generative detections and add Predictive Analytics with PRE.

Use Cases

Replacing Legacy SIEM Solutions

Scenario: A global enterprise wants to retire its Splunk or QRadar deployment due to operation challenges and desire to upgrade their abilities with an AI Native solution.

- Challenge: Ensuring consistent security monitoring and incident response across diverse and complex network environments and data silos built on traditional architectures and solutions.
- Solution: PRE Security's parserless, Universal Data Collector integrates seamlessly to ingest any and all data for context rich correlation and detection.
- Leveraging AI Native technologies allows unique solutions to long standing SecOps challenges and enabling new approaches including predictive analytics, natural language based interactions, and innovative response and prevention capabilities built in.

Enhancing Traditional SIEM based SOCs

Scenario: A large government entity cannot remove the SIEM but needs to address cost challenges with variable ingestion pricing.

- Challenge: Traditional SIEM architectures inhibit data ingestion due to pricing and storage schemes. Limiting ingestion also limits context, so users are in a catch 22 situation, forced by real world budget and administration challenges.
- Solution: PRE Security can sit in front of an existing SIEM deployment and pre-process data and perform analytics, then store only relevant security detection logs in the SIEM dramatically reducing cost and complexity while maintaining compliance and existing workflows.
- Another enhancement is sitting "on top of" an existing SIEM and taking the detections out and returning generative detections and predictions back into the SIEM.

Generative XDR and Predictions

Scenario: A global MSSP is still getting too many false positives and ineffective detections from their current XDR solution.

- Challenge: Attackers are also leveraging AI to rapidly iterate attack tactics and techniques, resulting in difficulty of detection using traditional pre-wired detections.
- Solution: PRE Security's generative XDR, powered by our CyberLLM™ detects based on training of frameworks like MITRE ATT&CK, CVE's and other cybersecurity information, but aren't limited to pre-defined recipes and can adapt and learn through discovery of multi-dimensional correlations.
- Adding Predictive Analytics to SecOps enables a whole new proactive approach helping to plug the holes before damage is even done, allowing prevention and preemption of attacks.

PRE Security Product Datasheet

Key Features and Benefits Summary:

FEATURE	BENEFIT
Ingest Anything - Universal Data Ingestion from any source. - Patent Pending Parserless Technology. - Support for unlimited data formats and data stores. - Upload additional environmental context via PDF, Excel, Word, etc. - Decouple log storage costs from analytics. - Fixed Asset based pricing.	- Provides complete visibility across all digital infrastructure. - Eliminates the need for custom parsers or complex integrations, reducing time and operational overhead. - Enables SOC teams to analyze critical data quickly, improving the quality and speed of response. - Reduces cost and complexity of maintaining custom parsers and integrations. - Enables rapid onboarding of new data sources. - Reduce costs without ingestion based pricing. Store logs cheaply.
Correlate Everything - Automatic data correlation across any data sources - Multi-dimensional alerts with data enrichment - Upload organizational-specific content to use as additional context - Easily add additional threat feeds and security-related information	- Provides context-rich, multi-dimensional alerts combining data from any number of sources. - Enables SOC teams to focus on the most critical threats rather than dealing with irrelevant alerts and false positives. - Reduces alert fatigue by filtering out low-priority incidents and focusing on highest-risk threats. - Gives security analyst the insights they need at their fingertips to make faster, more informed decisions.
Interact & Investigate in Natural Language - Allows SOC teams to interact with security data in Natural Language queries powered by SOCGPT™. - Provides immediate, context-rich responses for investigations. - Leverages AI to rapidly identify hard-to-identify patterns of anomalous activities and behaviors.	- Shortens investigation times by enabling analysts to ask simple questions and retrieve complex insights instantly. - Improves accessibility for less experience security analysts who may not be as familiar with tradition query language or complex logs. - Enhances decision-making ability by delivering critical context along with each query result. - Streamlines overall incident response process by allowing analysts to take immediate action without switching tools or interfaces. - Improves overall efficiency, allowing SOC teams to identify and handle the more severe incidents in less time.
Generative XDR Detections - The PRE Security purpose-built CyberLLM™ dynamically detects known and emerging threats. - Adaptive Threat Detection that evolves with new attack vectors.	- Continuously adapts and evolves with threat data, providing real-time detection of novel threats. - Eliminates reliance on static rules and signatures. - Dramatically improves detection accuracy and reduces false positives. - Ensures faster Mean Time to Detection (MTTD) and Mean Time to Response (MTTR) reducing window of exposure.
Predictive Analytics - Proprietary Predict & Prevent™ capabilities analyze both historical and real-time data to predict future .threats and vulnerabilities before they can be exploited. - Proactively reduce risk and improve security posture. - Transparent, Consensus Predictions.	- Enables organizations to act proactively instead of reactively. - Reduces exposure to zero-day vulnerabilities by predicting specific attack patterns. - Helps prioritize threats based on their likelihood of occurring. - Reduces the risk of breaches by enabling organizations to deploy mitigative efforts in advance. - Lowers overall attack surface by identifying and addressing weaknesses before attackers can target them.
Prescriptive Response & Prevention Action - Automated workflows provide real-time prescriptive guidance for threat response. - Integrated AI automation for threat mitigation. - Response Actions by Prompt and Automation.	- Minimizes damage by automating responses such as isolating compromised systems upon detection, preventing lateral movement within the network. - Drastically reduces response times by decreasing the times for manual processes typical for incident response. - Reduces operational load on SOC teams by automating repetitive tasks. - Ensures a more consistent and reliable response to incidents.

Customer Success Story:

"Since implementing PRE Security's platform, we've seen a 45% reduction in response times across our SOC team and a 60% improvement in detecting threats before they impact our network. The ability to predict threats has allowed us to fortify our defenses proactively and reduce our overall risk posture"

< CISO, Global Financial Institution

PRE Security Product Datasheet

Flexible Deployment Options / Predictible, Fixed Pricing Model

PRE Security can be easily deployed in various environments tailored to your operational needs:

- **Cloud-Based (SaaS):** Fully managed in the cloud for simplified deployment and scalability.
- **On-Premises:** Virtual appliances installed on your hardware servers for complete in-house control.
- **Hybrid:** Leverage your existing cloud providers such as AWS or Azure or in combination with on-premises deployment.

Unlike industry norm ingestion based or variable pricing schemes, PRE Security offers fixed contract pricing based on IPs

- **Starter Pack of up to 10k assets**
- **Additional assets in incremental bands of 10-100k assets:** Simplify asset counts by sizing into bands of IP counts.

Software Features:

- Parserless™ Data Ingestion
- Universal Data Collector / Exporter (patented Log2NLP™ & NLP2Log™ process)
- SearchGPT™ to talk with your data using natural language
- Data Fabric Filtering, Normalization, and Enrichment
- Multi-Dimensional Generative Data Correlation
- Generative XDR, Contextual Natural Language Alerts powered by the CyberLLM
- Risk and Priority evaluation with Auto Triage Agentic Actions
- Predictive Analytics
- Natural Language Threat Hunting (SOCGPT™)
- Network and Anomaly Detections (Next-Gen SIEM / XDR)
- Threat Intelligence including Predictive Intelligence
- Agentic AI Automations and SOARGPT™
- Built-in Breach & Attack Simulator with BreachGPT™
- And much more.

Technical Specifications

Component	vCPUs	RAM	Storage	GPU
Cyber LLM™ Server Virtual Appliance	24+	128GB+	200GB+	40GB nVidia (16GB+ VRAM)*
Predict Server Virtual Appliance	8	64GB	200GB	
Network Sensor Virtual Appliance	8	1GB	100GB	

*Minimum config is 1x GPU, large is 4x 80GB GPU. Nvidia A100 with NVIDIA driver is preferred. AMD, Intel, and Apple GPU's also supported.

Call to Action

Ready to take your cybersecurity to the next era?

Book a personalized demo of PRE Security today or start a free trial to experience faster detection, enhanced analysis, predictions, and seamless mitigation of threats.

For further inquiries or partnerships, contact us at: info@presecurity.ai