Replacing Legacy SIEM Architectures with AI Native SecOps

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 These outdated solutions are limited in scope and reactive by nature, resulting in delayed responses and missed threats.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 and response

Traditional SIEM based SecOps are:
Rigid, Precarious, Expensive

Ingestion, Parsers, Integrations, Queries, SOAR – everything in the legacy SecOps workflow is hand built, hard wired, and complex – and therefore also fragile, buggy, and limited to only what it is programmed to do – nothing more.

AI Native SecOps is:
Creative, Flexible, Inspired

AI Native SecOps learns as you go, breaking down walls and silos and providing real time, dynamic insight and response, unexpected and multi-dimensional correlation, and unforeseen detections, predictions, and actions.

The Old "Splunk" Way	The New AI Native Way
Unpredictable, Costly Ingestion Based Pricing - Increase in logs results in unexpected surges in costs. - This pricing inhibits ingesting all available sources, resulting in reduced context and therefore increased false positives. - Storage forcibly tied to SIEM product.	**Fixed, Predictable Pricing and Cost Reduction** - Lower your costs while making it predictable, budgetable. - Storage decoupled from Analytics to control, reduce costs. - Use low cost S3 storage or even local NAS – you control storage methodology, location, and cost.
Ingest Only Sources with Pre-built Integrations and Parsers - Error prone and complex to manage. - At vendor discretion and priority timeline. - Limits context from disparate and varied data sources.	**Parserless™ Ingestion of Everything** - Any data in – no pre-built integrations required! - Even ingest offline data in pdf, xls, or txt, for example. - Eliminate data silos, add context, reduce false positives.
Limited Normalization and Enrichment - SOC Analysts have to hand construct precise query instructions. - Response from SIEMs can be slow, iterative, and limited in scope by precise variables included, and fraught with error.	**Generative and Predictive Enrichment** - Leverage patented Log2NLP for natural language visibility - Predictive threat intelligence and extensive enrichment. - Ability to filter and reduce logs using data fabric techniques.
Handwritten Queries - SOC Analysts have to hand construct precise query instructions in jargony code structure prone to error. - Response from SIEM is slow, iterative, and limited in scope by precise variables included. - Garbage in, garbage out. Small data in, Small answers out.	**Inspired Generative Answers** - Constantly, automatically correlated detections that are generatively prepared for SOC teams to review. - Analysts can interact with data in natural language, interacting with and interrogating data in real time. - Provides immediate, context-rich responses with inspired answers to questions that haven't even been asked yet.

splunk> splunk> PRE PRE PRE™

Disrupting SecOps with AI Native

Lower Costs: Eliminate Ingestion-based pricing and expensive storage in in the SIEM by decoupling log storage.
Expand Capabilities: Generative observations result in expanded detections and predictions, new possibilities.
Re-imagined Workflows: Make the move from hand built, pre-wired systems, to fully AI Native Secops workflows.

Turn the old "Splunk" way upside down with PRE Security.

Replacing Legacy SIEM Architectures with AI Native SecOps

Software Features:

- Parserless™ Data Ingestion
- Universal Data Collector / Exporter (Log2NLP™ & NLP2Log™)
- Data Fabric Filtering, Normalization, and Enrichment
- Multi-Dimensional Generative Data Correlation
- Generative, Contextual Natural Language Alerts
- 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.

Customer Success Story:

"PRE Security is the platform we thought we'd have to build ourselves before we found out it already existed. Only through an AI Native approach will we be able to move from a reactive to a proactive stance and keep ahead of the growth in attacks going forward. We had no chance of keeping up with our old SIEM system. And we saved money to boot by switching to PRE! Highly recommended."

< CISO, Hospitality Company

Flexible Deployment Options

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.

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