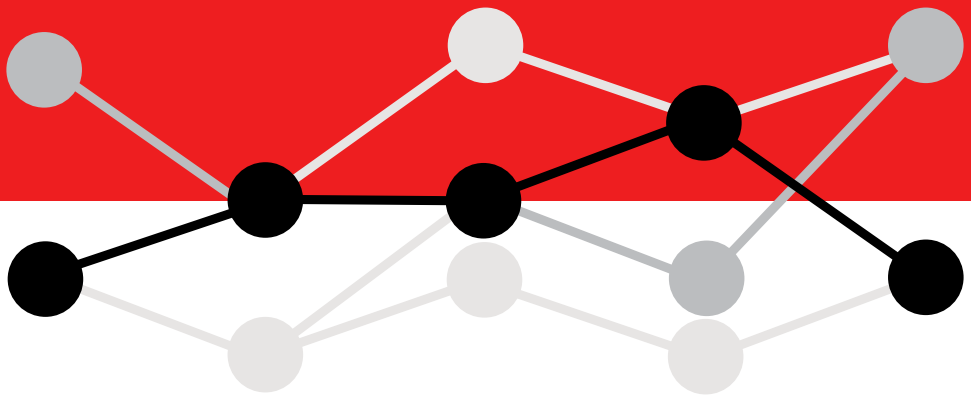
ENSIGN®

by **Reservoir** Labs



Multi-Domain Analytics

Solution Brief

ENSIGN® is the codename for an innovative machine learning technology offering multi-domain analytics with High Performance Computing scalability. ENSIGN accepts large, structured, multi-dimensional datasets, such as spreadsheets or logs, and decomposes them, independently or jointly, into identifiable, discrete patterns of behavior. These patterns provide a roadmap for data comprehension and can be used to drive both investigative and automated security activities.

By promoting ENSIGN at RSA, we are seeking to connect with forward-looking customers and vendors interested in exposure to a leading-edge technology in artificial intelligence and machine learning that is not yet incorporated into any commercially available end-user solution.

ENSIGN solves a critical problem in the application of machine learning to cyber and enterprise security - it provides deep insight into unlabeled data without the need for heroic feature engineering. The approach builds on advanced, well-founded techniques from the field of spectral hypergraph analytics. These techniques have been extended and made computationally tractable using Reservoir's patented data structures and supporting proprietary algorithmic advances. Combined with supporting tools, these advances enable a broad range of potential use cases, scalable and streaming operation, and the ability to leverage a variety of computing configurations.

ENSIGN Features

Linux Platform Software

Desktop, Server, Cluster, or Cloud

Up to Billion-scale Datasets

Integrates with Python Packages

Proof-of-Concept Evaluation

Professional Services

Custom Development

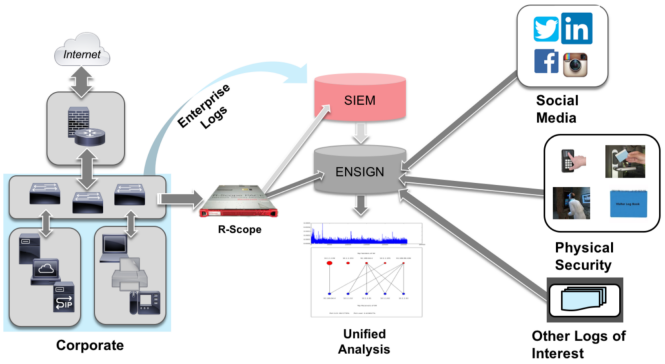
End-user License or OEM

Reservoir Labs

ENSIGN® in Action

Multi-Domain Data Comprehension

With joint decompositions, security administrators and insider threat specialists can discover patterns spanning multiple data sources - network, host, physical, and social. Using ENSIGN, they gain deep insight into data that helps identify risks and bottlenecks and that supports informed decisions about policy and resourcing.

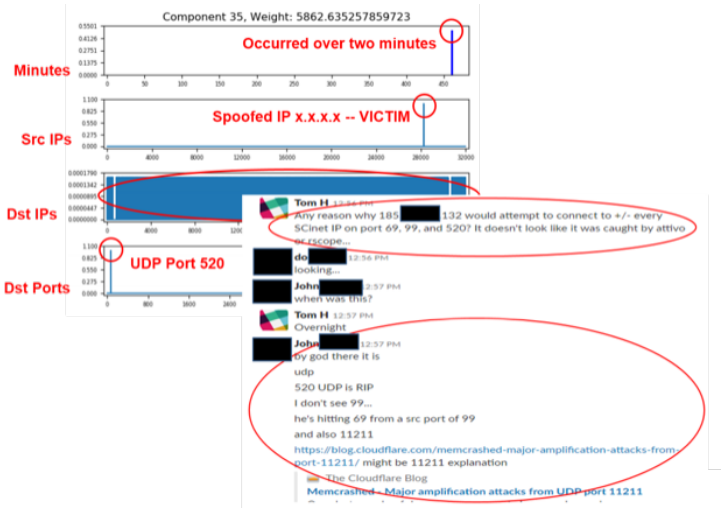


Threat Hunting

Used by small, dedicated teams in a SOC operating outside day-to-day operations, patterns discovered by ENSIGN kickstart focused investigations. These patterns already connect key dots that make clear who the relevant actors are. Skilled teams then hunt making directed, efficient use of knowledge stores and big-graph platforms to validate hypotheses.

Network Monitoring and Baselining

Mixing periodic and streaming decompositions, ENSIGN is used as part of day-to-day operations to discover "what has changed." Operations personnel catch emergent patterns indicative of discovery, collection, exfiltration, and malware execution. They understand how today's traffic differs from yesterday's.



Is ENSIGN Right for You?

Organizations with large-volume data who would benefit from understanding its dominant patterns; analysts who frequently see data where the structure is understood, but not the content

Advanced threat hunting teams interested in evaluating a unique, pattern-focused machine learning approach

Teams with the expertise and interest to develop their own scripted workflows for data analytics

Security solution providers with end-user platforms seeking to add value by integrating (OEM) deeper analytics or more sophisticated drivers of big-data or big-graph query capabilities