Reservoir Labs

ENSIGN™

Discovery of Deep Patterns at Enterprise Scale

ENSIGN is turning the field of cyber analytics on its head with an approach to advanced threat detection rooted in pattern discovery rather than incident detection.

NO UPFRONT CLASSIFICATION of normal versus abnormal network traffic

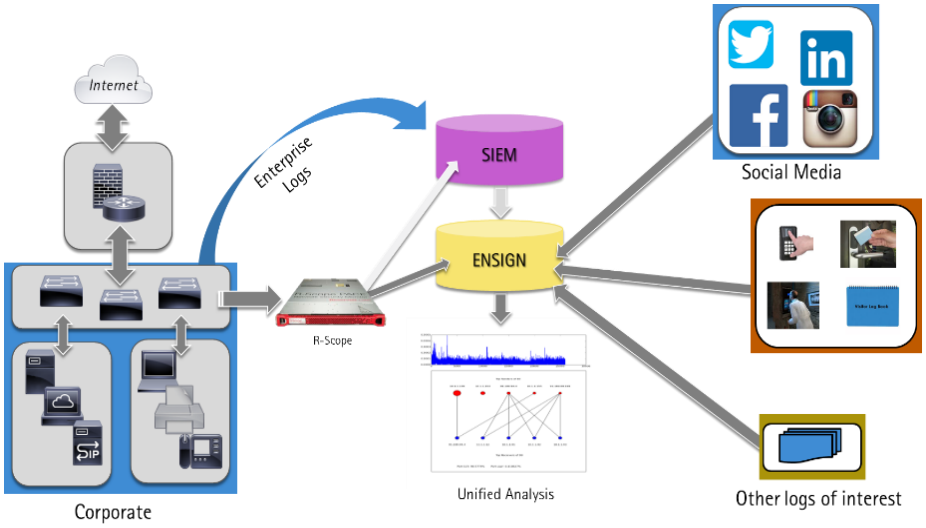
SIMULTANEOUSLY ANALYZE MULTIPLE METADATA ATTRIBUTES for a comprehensive view

INTEGRATE DIVERSE STRUCTURED AND UNSTRUCTURED DATA for optimal situational awareness

REVEAL OBFUSCATED ATTACKS by extracting behaviors that span long periods of time

Observe

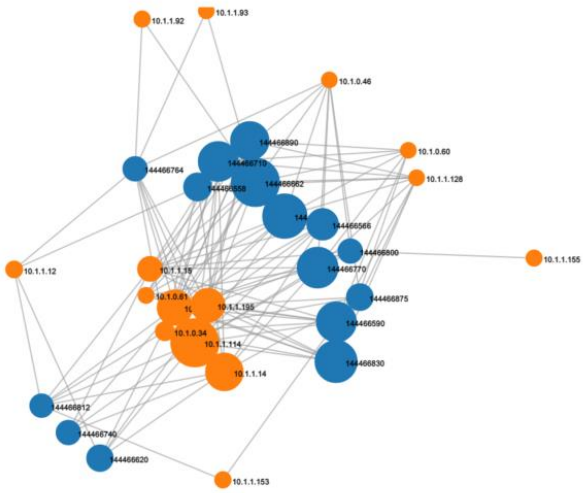
Scrutinize all of your data simultaneously



2017

Identify

Find patterns you didn't know existed



Most analytic approaches suffer from the practical difficulties of needing upfront specification of "normal" versus "abnormal" behavior. ENSIGN needs no baseline and adapts to constantly changing and adapting nature of enterprise input, uncovering patterns such as:

- Distributed port scans evolving to machine takeover
- Distributed denial of service attacks
- DNS-based data exfiltration/insider threat
- SSH password guessing
- Network policy violations
- Exploitation of application-specific port vulnerabilities
- Vulnerable IoT devices
- Broken or misconfigured network services
- Selective, persistent use of cryptographic methods
- And more "unknown, unknowns"

Disrupt

Leave them nowhere to hide

The ability to see the unforeseen patterns in your cyber environment makes ENSIGN an unparalleled hunting tool. ENSIGN replaces tedious incident-to-incident forensic analysis with automated discovery.

Knowledge is Power.

ENSIGN™ is available as a Toolbox and as a Service.