Reservoir Labs

ENSIGN™

R-Scope® Analytics

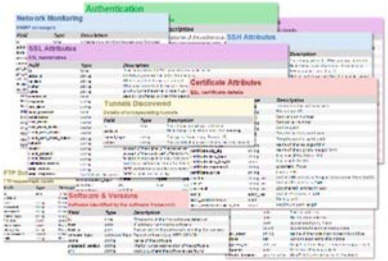
Finding Deep Patterns in Network Flows at Enterprise Scale

ENSIGN is poised to turn the field of cyber analytics on its head with an approach to advanced threat detection enabled by R-Scope that is rooted in pattern discovery rather than incident detection. Funded by the Department of Defense to deliver mathematically sound unsupervised discovery for large-scale multi-dimensional data and now adapted to the cyber domain, ENSIGN reduces vast logs of information into a set of true, unbiased, visually concise stories about what is actually happening on a network. Demonstrated at the 2017 ACM/IEEE Supercomputing Conference, these stories reveal activity and threat intent that would otherwise go unnoticed by methods limited to signature-based discovery alone.

Observe Your Network

R-Scope provides unparalleled fast, scalable metadata collection. This enables ENSIGN to leverage this vast and deep data stream to recover coherent, recognizable patterns of activity.

R-Scope metadata collection enables depth of analysis that was previously impossible.


Authentication
Network Monitoring
SSL Attributes
SSH Attributes
Certificate Attributes
Tunnels Discovered
Software & Versions

A network data stream is the sum of overlapping activities. Reconstructing those activities begins with collecting the totality of what is actually taking place on the network, including:

- Message source and destination hosts with port
- Message attributes including type, size, and more
- Protocol and connection state information
- Query strings
- Attachment attributes
- Time and duration

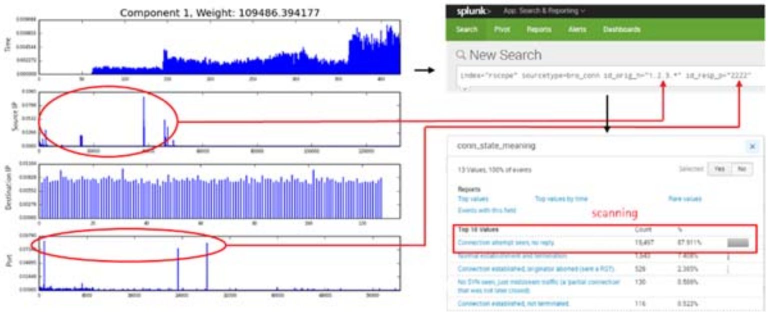
2018

Observe – Identify – Disrupt

Identify Activity

In most cases, the story underpinning the existence of a pattern is self-evident – an occurrence of expected, easily recognizable, benign activity. In other cases, however, patterns emerge among one or more dimensions (regular time intervals, a common target, a common request type) that indicate a deeper, more malicious intent.

The ability to find the unforeseen patterns gives a threat actor nowhere to hide.



index="rscope" sourcetype=bro_conn id_orig_h="1.2.3.*" id_resp_p="2222"

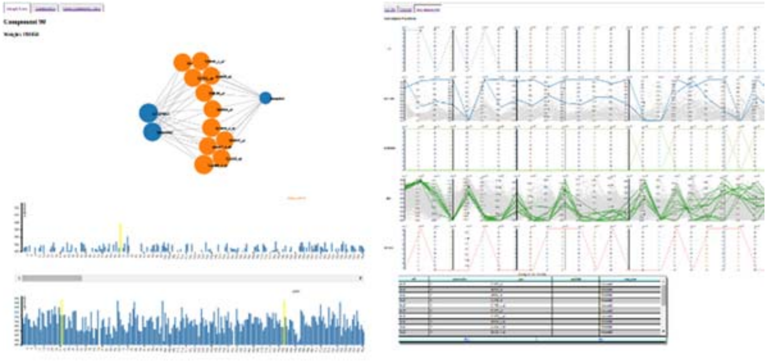
Top 10 Values	Count	%
Connection attempt seen, no reply	15,457	87.911%
Normal establishment and termination	1,343	7.408%
Connection established, originator aborted (sent a RST)	526	2.385%
No SYN seen, just midstream traffic (a partial connection that was not later closed)	130	0.588%
Connection established, not terminated	116	0.522%

From unsupervised discovery, the challenge is reduced to attaching meaning to the patterns that comprise the data stream. This task is assisted by a variety of unique visualizations combined with both automated and interactive classification and exploration tools.

Disrupt Bad Actors

ENSIGN isolates patterns of activity that can then be explored through Splunk®. Which port scan connections got through? Is this really data exfiltration? Who is making suspicious use of encryption?

The combination of R-Scope, ENSIGN, and Splunk make for the ultimate hunting tool.



ENSIGN has uncovered and visualized activity patterns including:

- Distributed port scans evolving to machine takeover
- Distributed denial of service attacks
- DNS-based data exfiltration/insider threat
- SSH password guessing (apart from scanning)
- Exploitation of application-specific port vulnerabilities
- Scans for printers or IoT devices
- Selective, persistent use of cryptographic methods

Ahead of the Curve

Get access to tomorrow's analytics today.

R-Scope is the most capable network sensor on the market today. It collects today the information necessary to drive tomorrow's advanced machine learning-based analytics. Easy-to-use, R-Scope is available with support and services packages from Reservoir Labs. Learn more at www.reservoir.com/r-scope.