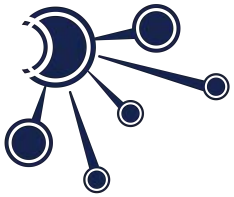


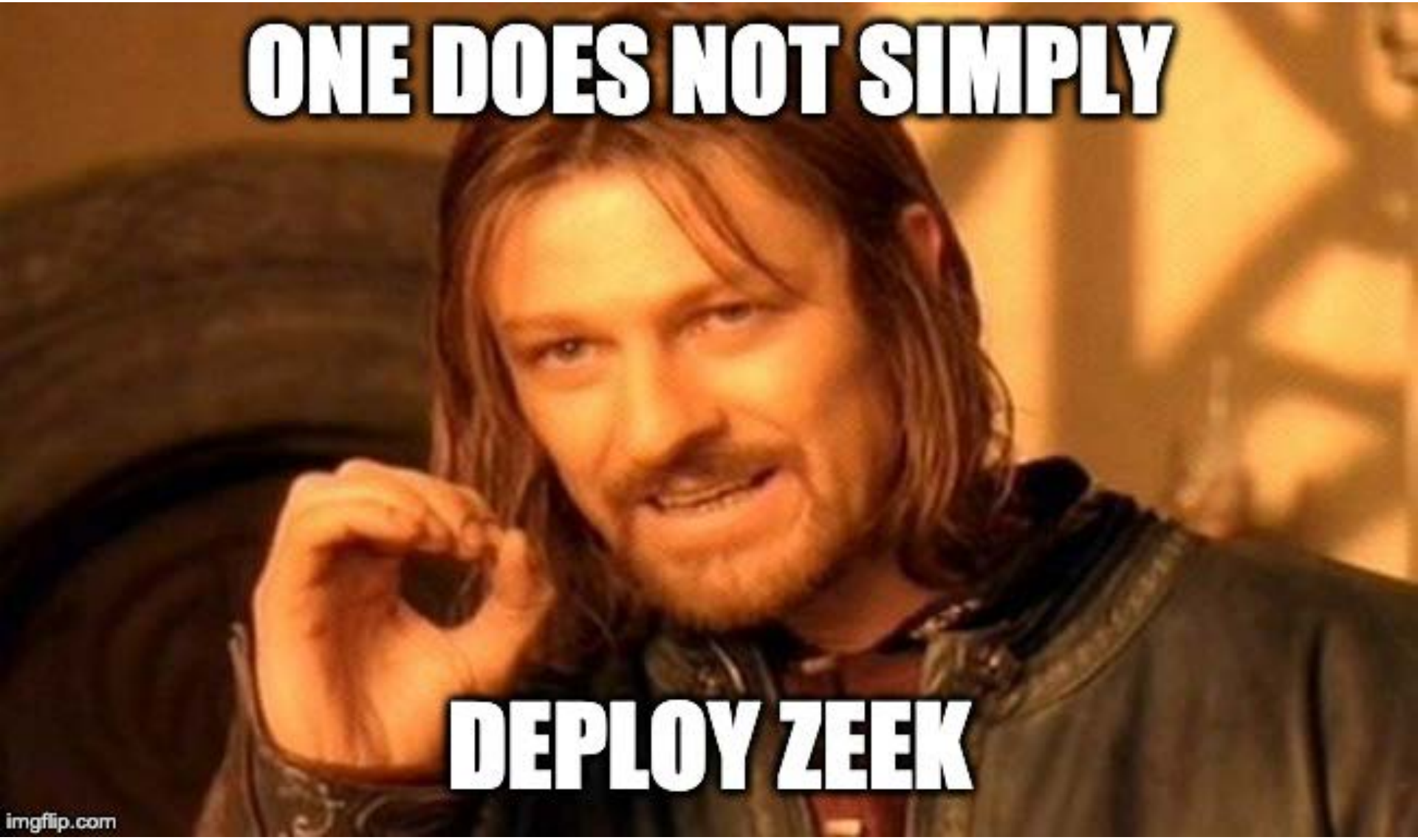
DYNAMITE
ANALYTICS

Oleg Sinitsin | Dynamite.AI

Dynamite-NSM

Open-source project for network traffic analysis with Zeek, Suricata, Flow Data and ELK


WHO NEEDS ANOTHER ELK?


ONE DOES NOT SIMPLY
DEPLOY ZEEK
imgflip.com

Dynamite-NSM

Installed and managed with a Python command line utility

```
usage: dynamite.py [-h] [--interface NETWORK_INTERFACE]
                   [--agent-label AGENT_LABEL] [--ls-host LS_HOST]
                   [--ls-port LS_PORT] [--es-host ES_HOST] [--es-port ES_PORT]
                   [--debug]
                   command component

Install/Configure the Dynamite Network Monitor.

positional arguments:
  command               An action to perform [prepare|install|uninstall|start|
                        stop|restart|status|profile|update|point|chpasswd]
  component             The component to perform an action against
                        [agent|monitor|elasticsearch|logstash|kibana|suricata-
                        rules|mirrors|default-configs]
```

Dynamite-NSM

The Agent

Agents are scattered throughout your environment, and bind to a network interface (typically a mirrored port), after which traffic is forwarded to the monitor for enrichment and indexing.

Component	Description
Zeek [2.6.1]	Previously Bro, Zeek is a powerful network analysis framework that is differs from your typical IDS. It is capable of enumerating detailed information surrounding network connections and their underlying protocols.
Suricata [4.1.4]	Suricata is an Intrusion Detection System (IDS), powered by the latest open EmergingThreat rule-sets.
Oinkmaster [2.0]	A script to automate management of Suricata rule-sets, and keep rules up-to-date.
PF_RING [7.4.0]	A new type of network socket that dramatically improves the packet capture speed. It is used in conjunction with the Zeek to improve packet analysis.
Filebeat [7.2.0]	A powerful log forwarder, with a built in queue mechanisms, and a pressure sensitive protocol that works in conjunction with Logstash.

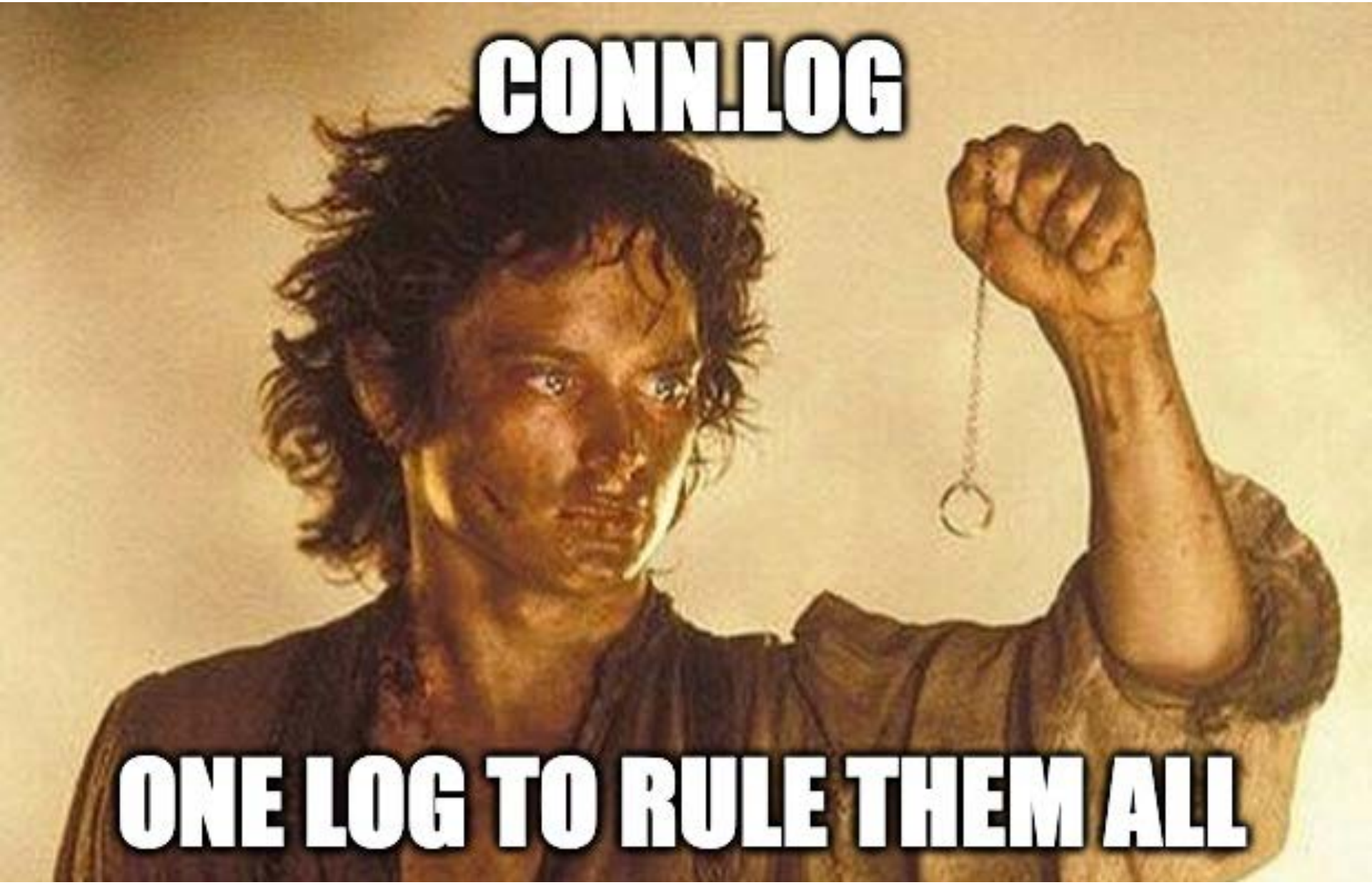
Dynamite-NSM

The Monitor

Your monitor is responsible for parsing, enriching, indexing, and visualizing analyzed traffic sent from multiple agents or NetFlow exporters.

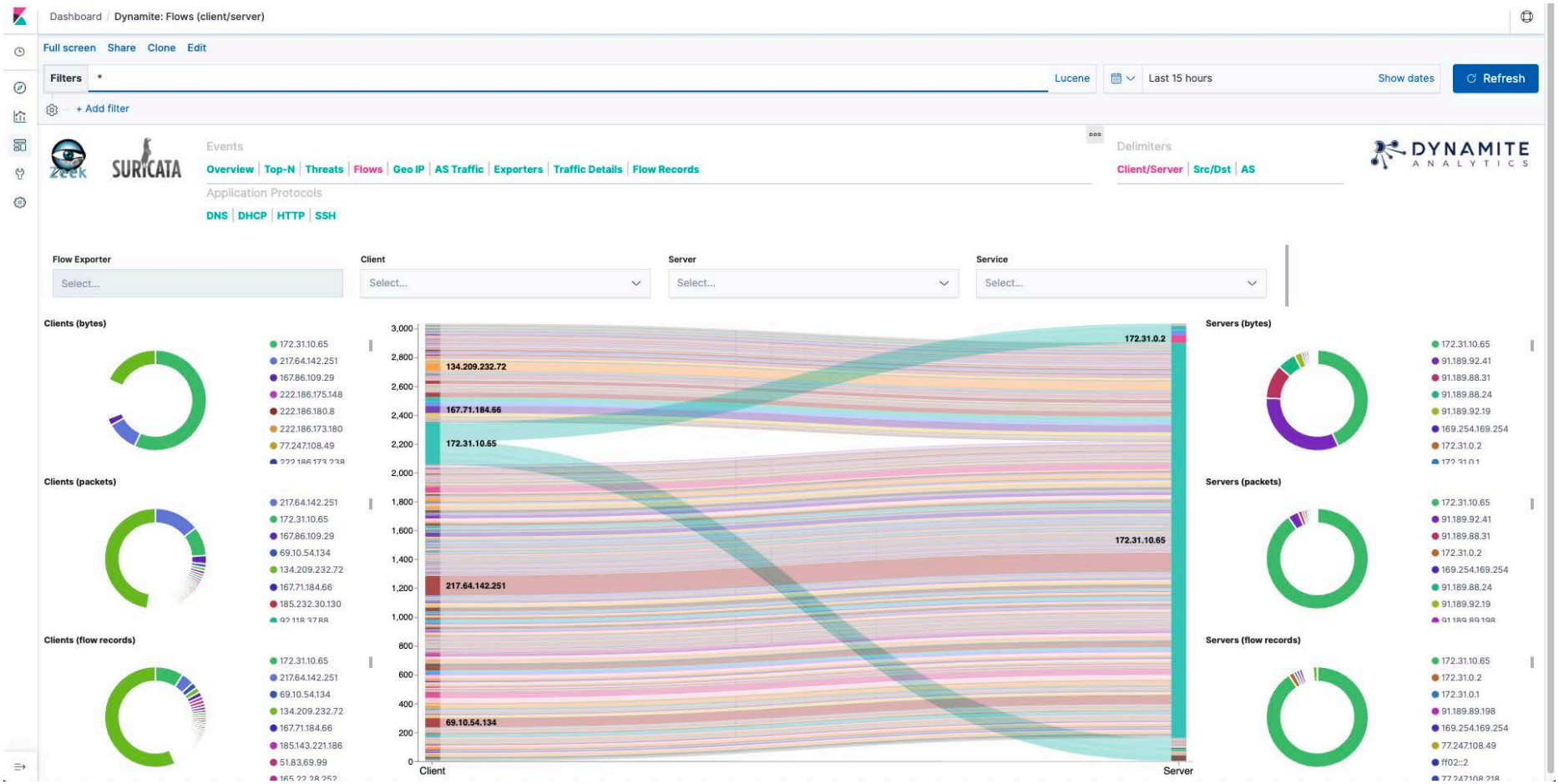
Component	Description
Logstash [7.2.0]	A server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it.
Elasticsearch [7.2.0]	A distributed, RESTful search and analytics engine.
Kibana [7.2.0]	A web-app that allows you to visualize your Elasticsearch data
ElastiFlow™ [3.5.0]	Provides network flow (**and now Zeek!**) data collection and visualization.
Synesis [1.1.0]	Provides Suricata data normalization and visualization.


WE GOT LOGS
NOW WHAT?


CONN.LOG
ONE LOG TO RULE THEM ALL

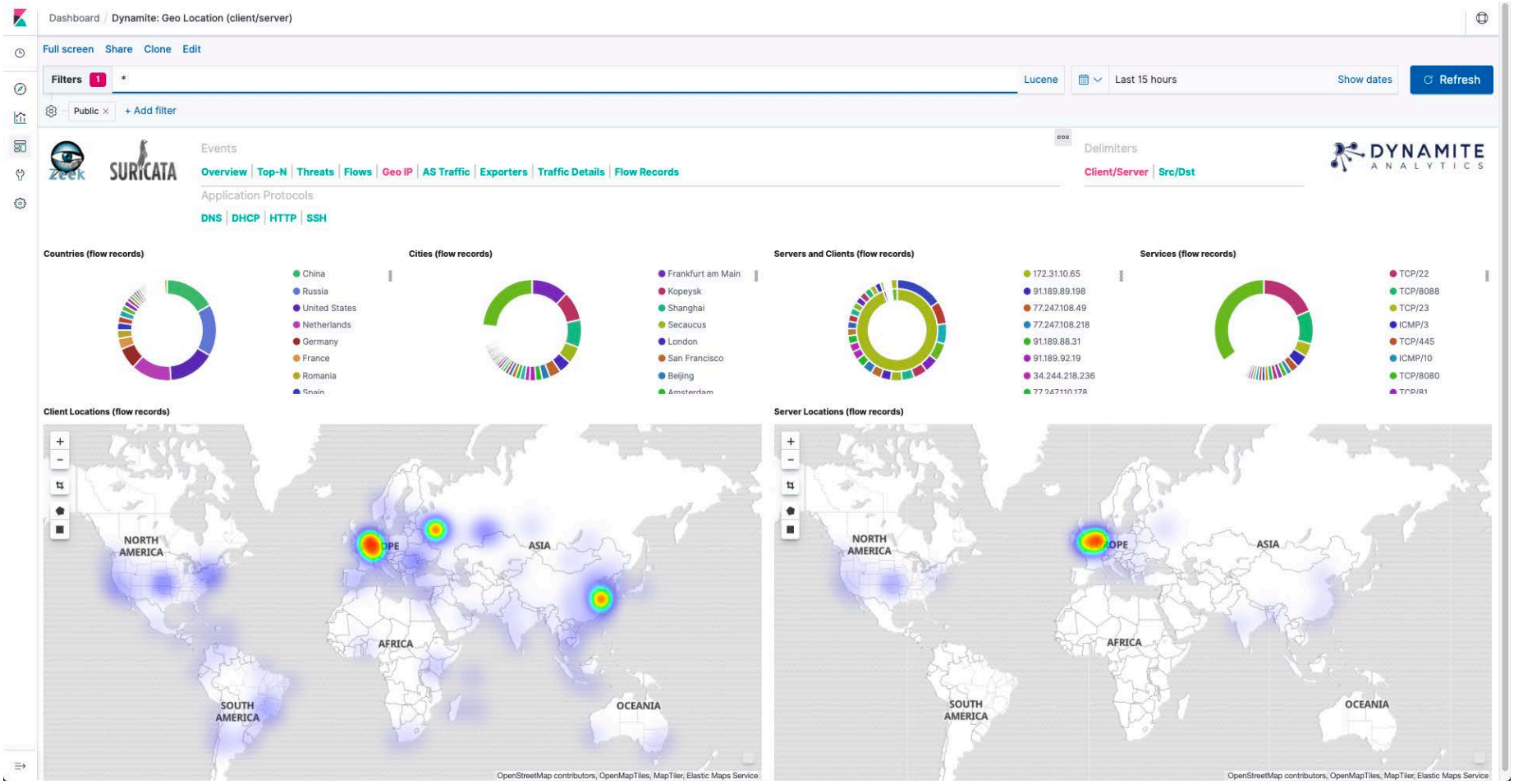
Dynamite-NSM

Traffic Flows



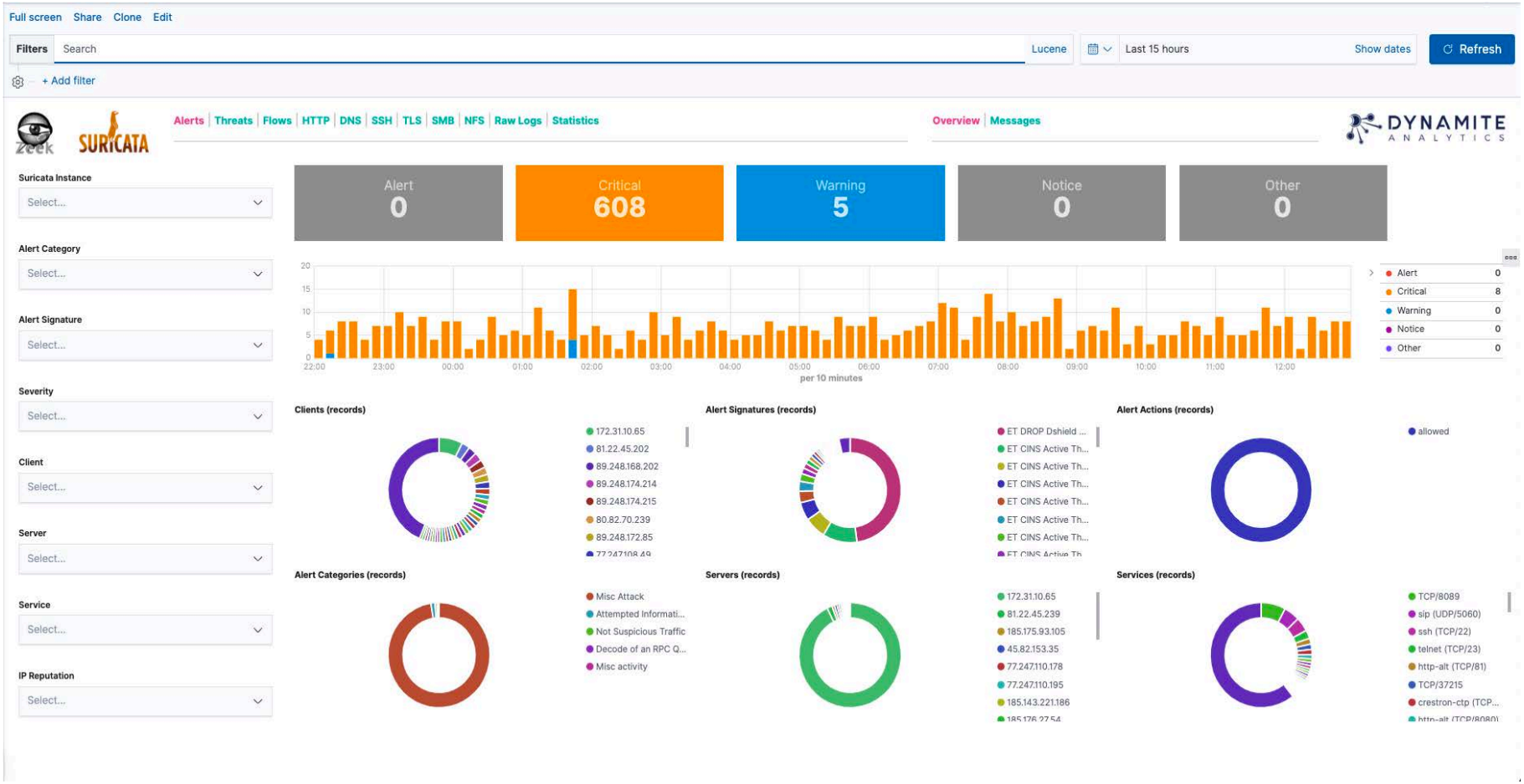
Dynamite-NSM

GeoIP Enrichment



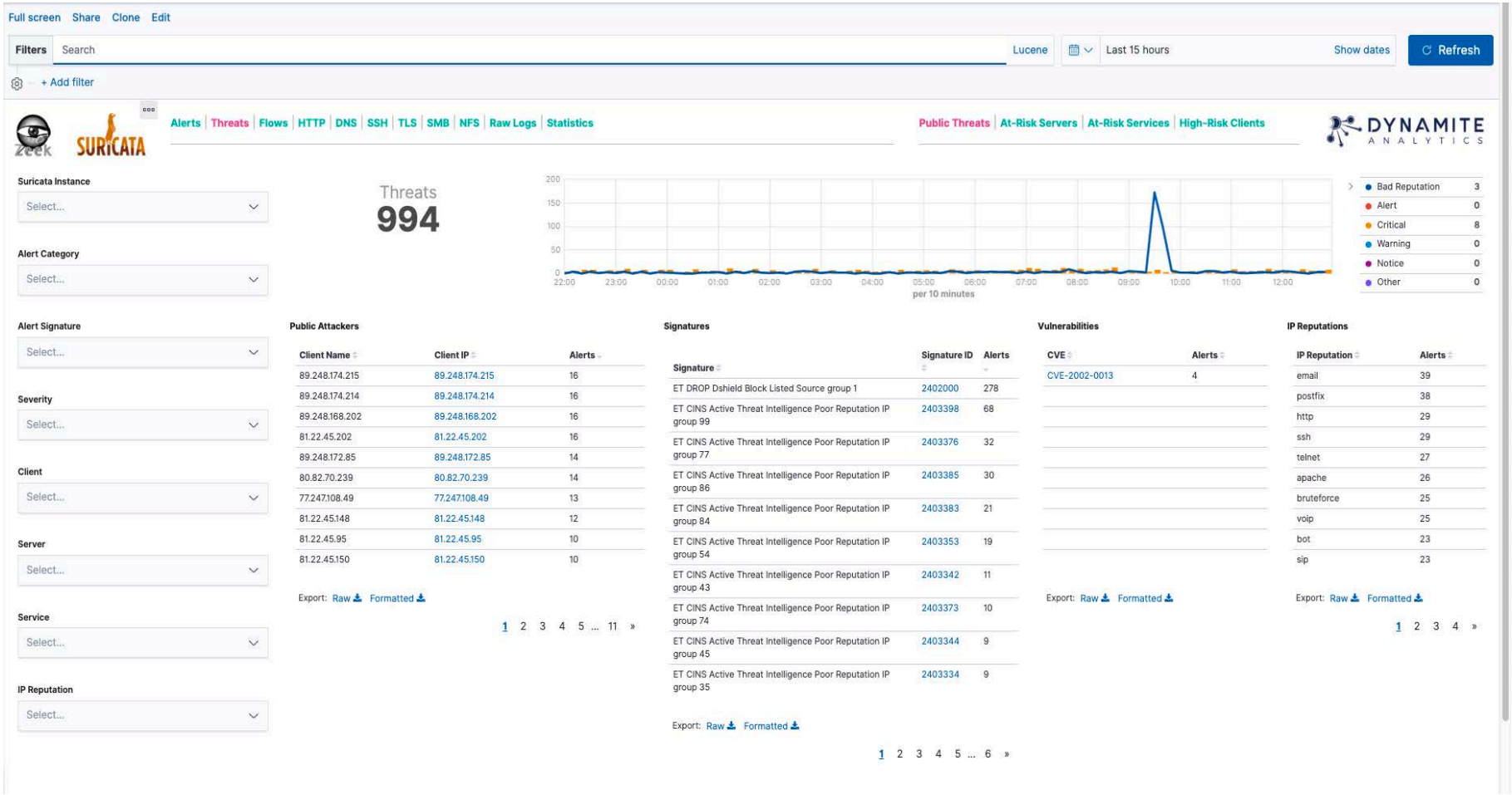
Dynamite-NSM

Signature Alerting

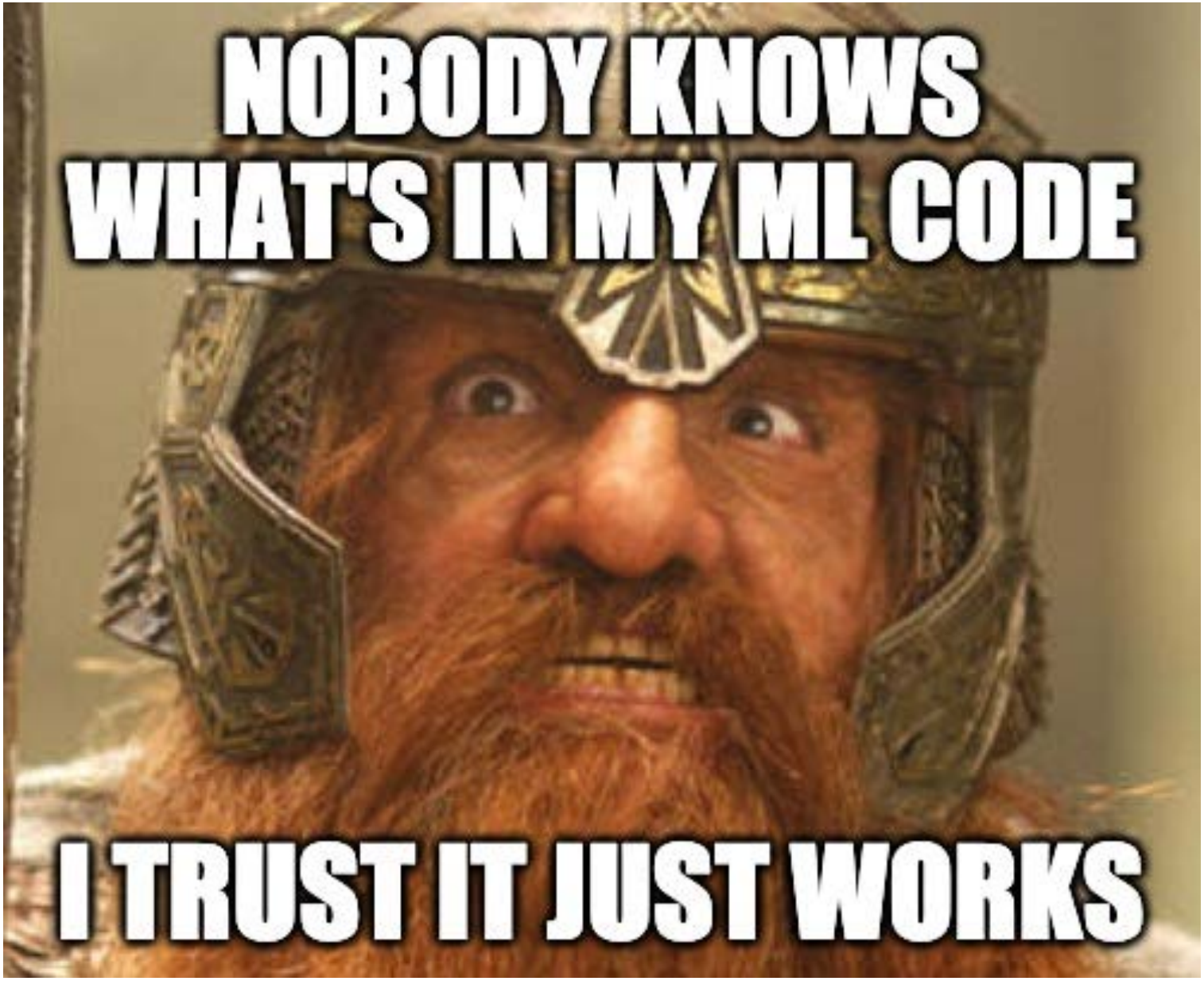


Dynamite-NSM

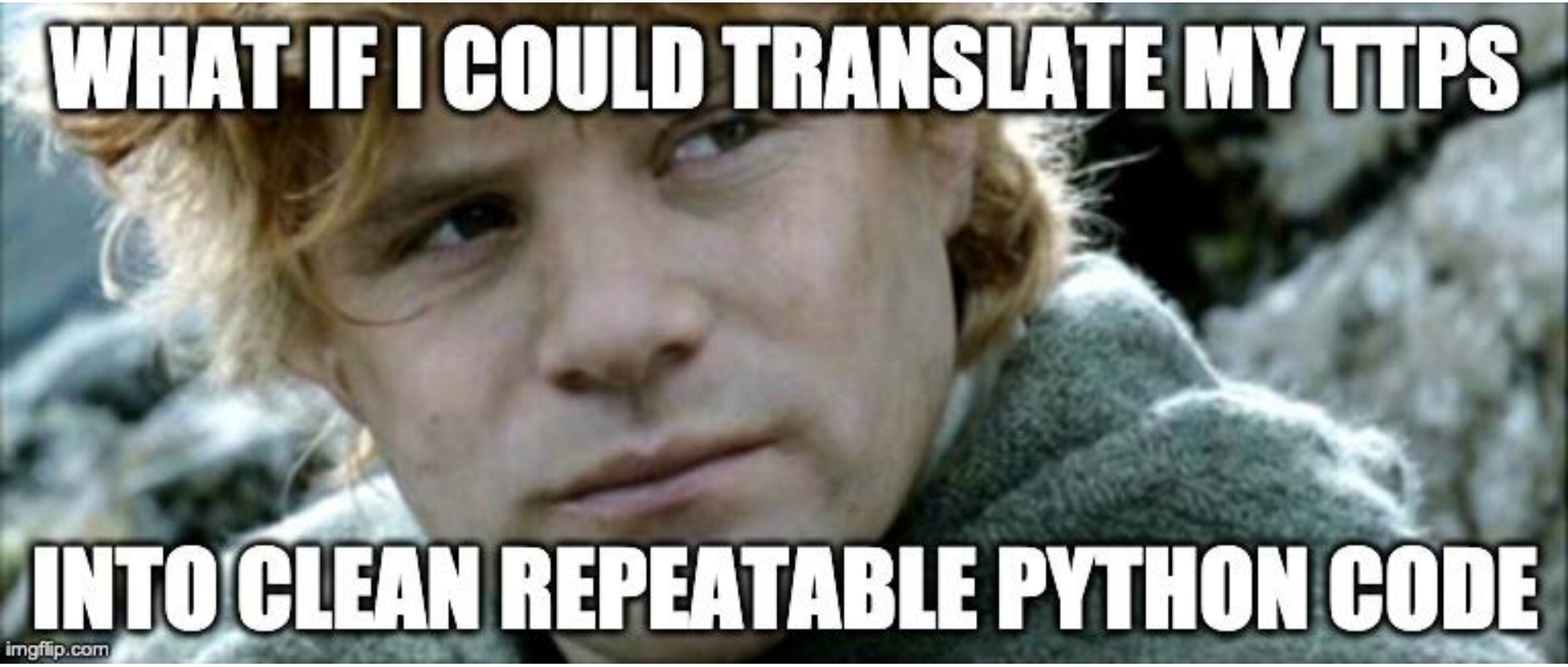
Threat Deep-Dive




WHERE IS MY SOC PLAYBOOK?


NOBODY KNOWS
WHAT'S IN MY ML CODE
I TRUST IT JUST WORKS


MITRE ATT&CK MAY BE THE BEST THING
SINCE THE LORD OF THE RINGS


WHAT IF I COULD TRANSLATE MY TTPS
INTO CLEAN REPEATABLE PYTHON CODE
imgflip.com


ENCRYPTED PACKETS DON'T LIE
THEY ARE JUST HARD TO UNDERSTAND


HUMAN MIND REMAINS
THE BEST ANALYTICAL TOOL

Oleg Sinitsin

oleg@dynamite.ai

https://github.com/DynamiteAI/dynamite-nsm

We are always looking for good people…

Oleg Sinitsin

oleg@dynamite.ai

https://github.com/DynamiteAI/dynamite-nsm

We are always looking for good people…