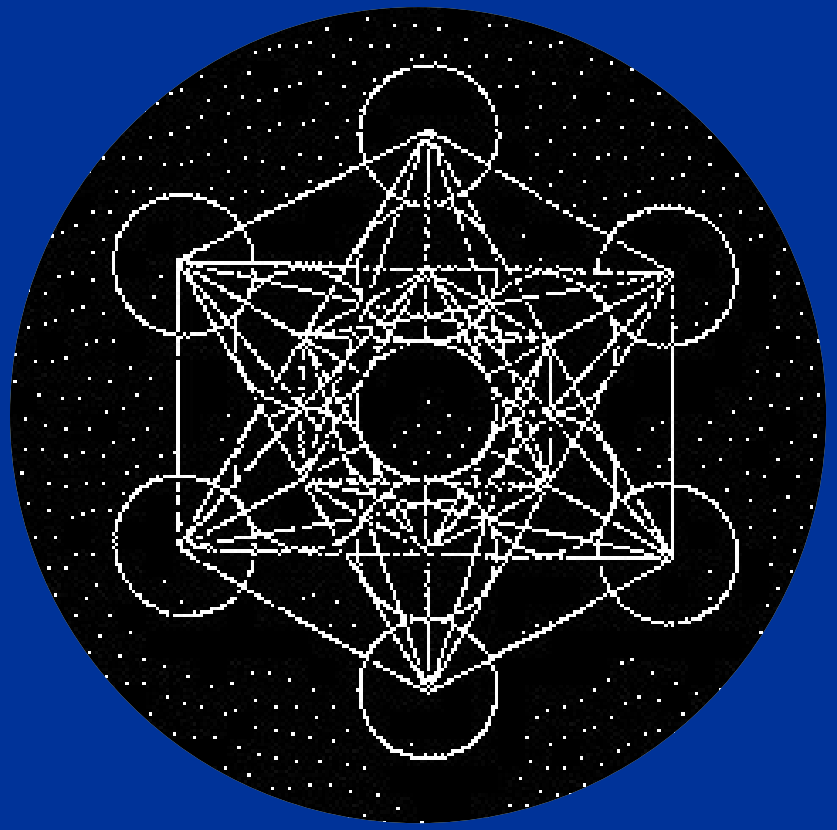
SOC Must Die

Engineering our way to Detection & Response Operations

Position Paper

Speaker

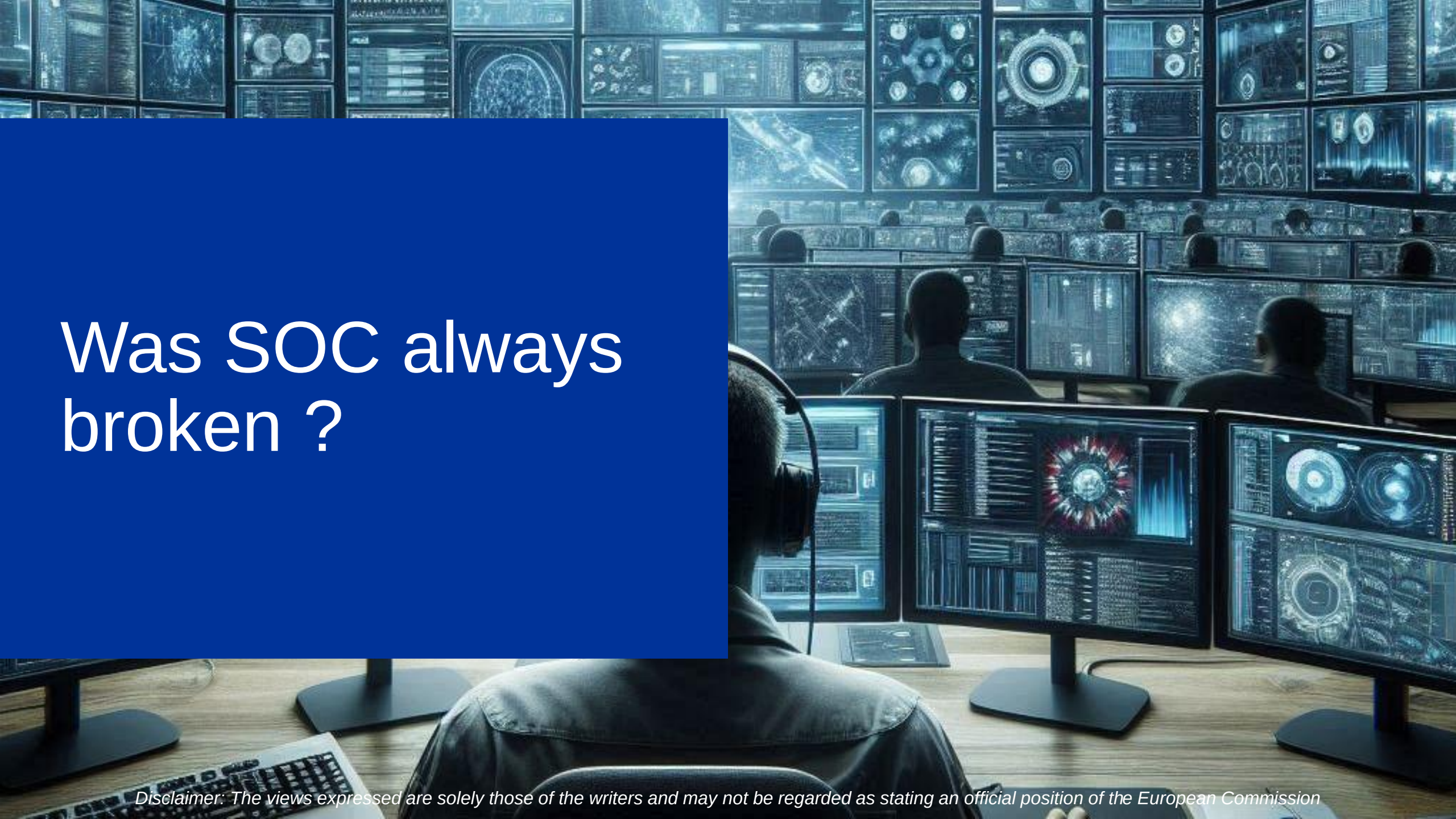


Amine Besson

- Independent international cyber operations contractor
- Been in way too many SOCs
- Focus on next-generation detection + response architectures, workflows, tools
- Research and Development at the European Commission for Detection Engineering (CSOC CATCH Team), Maintaining **OpenTide**
- **This talk is not a position of the EC, and is not representative of the EC CSOC viewpoints**
- **linkedin.com/in/behemoth**
- **github.com/behemothsecurity**

Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

Was SOC always broken ?



Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

What are we *really* doing ?

Detections… which detections ?

- High 70, 80, 90 % False Positives
- Mystical “well-tuned SIEM”
- Dubious detection rules management
- Invest a lot in SIEM when EDR/NDR is actually doing the heavy lifting
- Unknown Detection Coverage

Alerts ? Do you mean Incidents ?

- Slapping a SOAR on manual processes (autoclose !)
- Infamous “Check if Anomalous” Playbooks
- Feel-good triaging at the cost of efficiency
- One Alert = One Response

A long sunset for traditional analysis

Analyst Ecosystem

Old World

- Mostly Network IDSs
- Little to no endpoint data
- Simpler malwares
- Less actor awareness
- Direct legacy from NOCs
- Best effort, lots of craft

SIEM Obsession

- Grab the data, grab it fast!
- The Splunkers cult
- Analyst Toil really kicks off

?DR Explosion

- EDR, XDR, NDR, CDR…
- SIEM slowly gets abstracted into purpose driven tools
- Often proves more effective than SIEMs in raw TP numbers
- Obscurantism, less visibility into certain alerting mechanisms (AI Analyst, undocumented ML detections etc.), tough to correctly onboard

SOARs, Next Gen SIEMs

- Transform case management systems into workflows
- Modern data analysis systems, plug-and-play, unified schemas

Threat Informed Detection Engineering

- Current growth path for many teams
- Challenges ?DR by asking for more control over alerts and incidents
- Challenges SOAR by moving away from point-to-point alerts

Detection and Response Operations

- Less analysts and outsourcing
- Non-traditional structures
- Tech-centrism
- AI SOC will challenge more and more traditional analysis, and force to focus on detection/response content

Engineering Ecosystem

Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

Maybe… SOC is not the answer

Do we need to be so focused on triaging noise ?

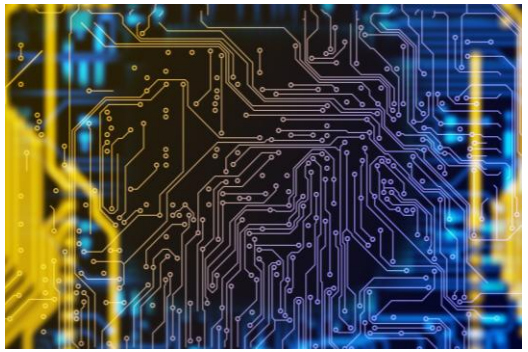
Why do we keep throwing tiered analysts at false positives ?

Automating downstream has shown to be… counterproductive

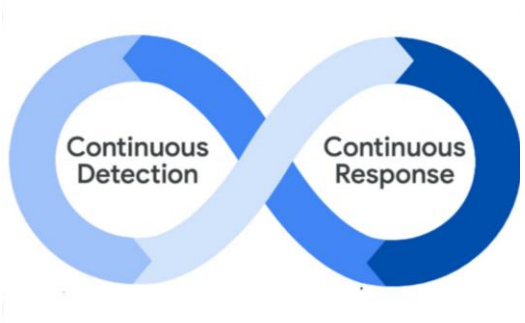
Analysis is *extracting* existing value. Could Engineering, which is *building* value, be front and center ?

Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

Towards Detection and Response Operations

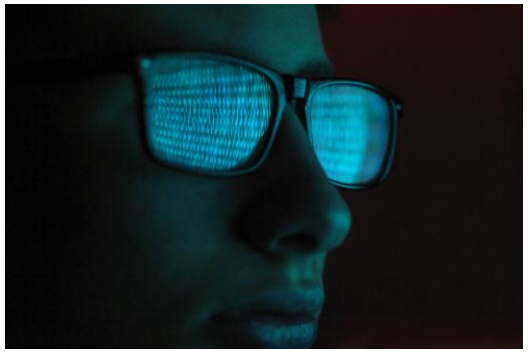


No more SOC. Engineering-first teams, dedicated profiles, skilled responders



Building with automation-first in mind, applying software engineering principles continuously

Continuous improvements to detection coverage, CTI in the loop



Detection & Response Engineers to move towards autonomic operations

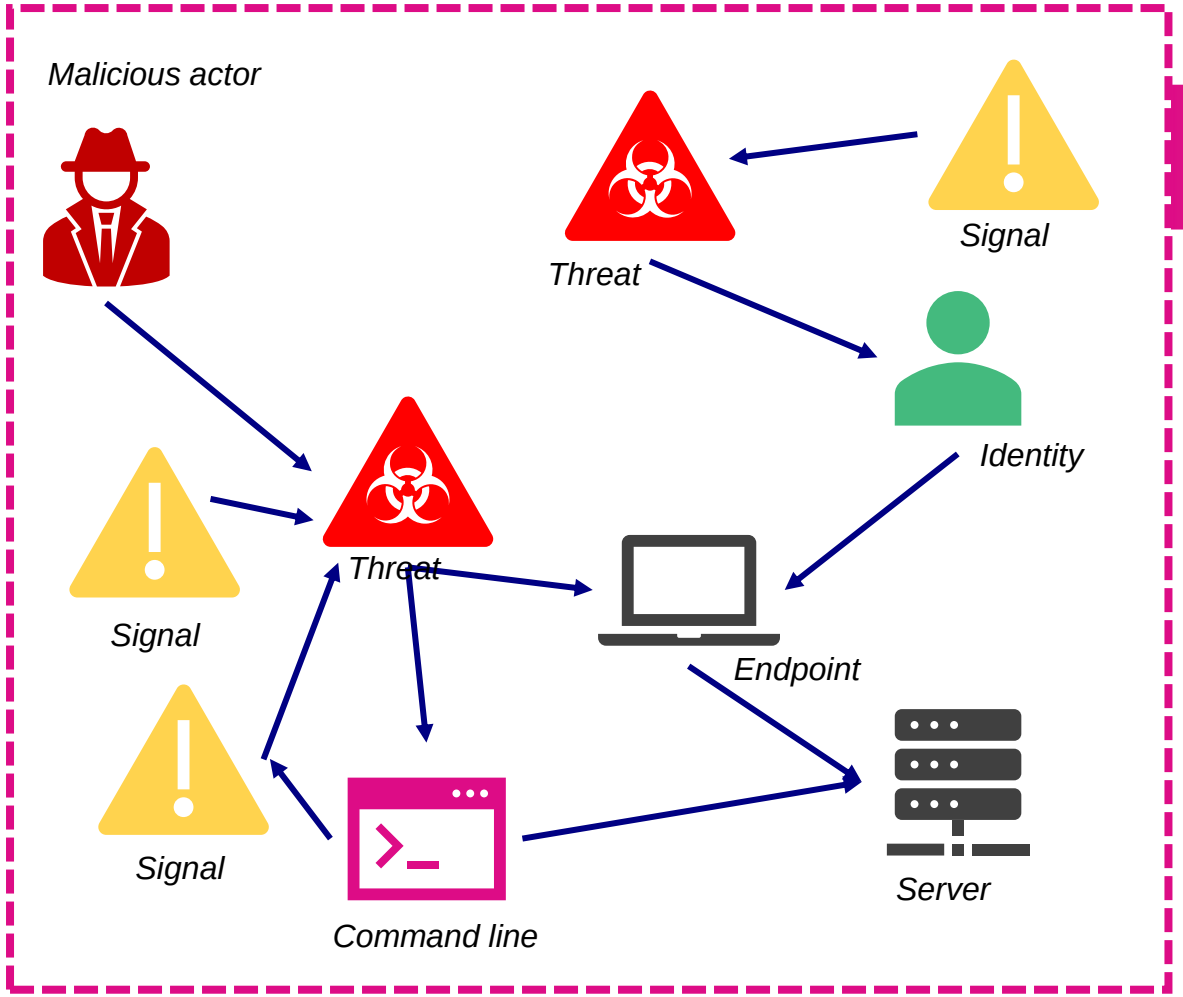
Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

The future is not *just* AI SOC

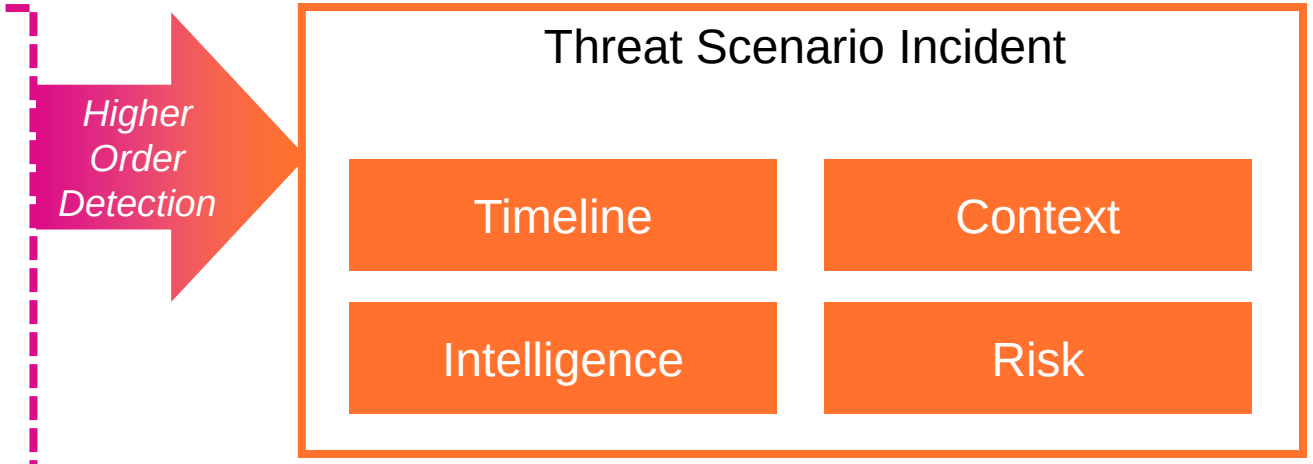
It always starts with Detections

- **If you want to reinvent your Response posture, you must first take control of your Detection posture.**
- Triaging noise is expensive and meaningless and makes SOC unscalable. Throwing an agent into it downstream may help, but to really improve you need to first fix the upstream.
- Balancing precision and recall is challenging but can be progressively improved.
- Vendor detections are a *starting* point, not the endgame…
- Signal-to-noise ratios is a problem amplified by single-order detections… and creating surgical, higher order ones takes engineering minds.

We need a better detection architecture



Dynamic Entity and Threat Signal Graph

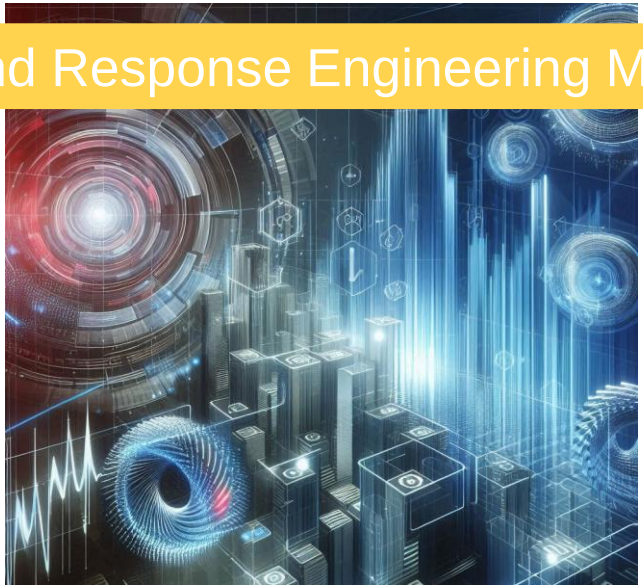


- **Most SOCs are still doing 1:1 alert to incident to response architectures… making AI SOC very much a garbage in, garbage out system.**
- We are still missing the vocabulary and tools to fully reinvent what detections should be
- Today, we can perform entity focused strategies : Risk Based Analytics, Entity Grouping…
- Vendors are slowly creeping towards understanding these problematics and potentially delivering solutions

Engineering Response from the start

Detection and Response Engineering Maturity

Alerts are signals, not incidents. Entity extraction and grouping



Continuous (risk) scoring approaches, dynamic thresholds

Composite Detections to create clear Threat timelines

Adopting Detection Engineering: Introducing OpenTide

Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

1 minute pitch

What ?

- A framework to help Detection Engineering team working in consistent way around technical standards and workflow
- Intelligence-to-Detection Pipeline
- Everything as-code
- The start of what we call DetectionOps

Why ?

- Detection-as-Code is still too much of an internal kitchen job
- No structured way to track detection coverage
- Ingesting and processing Detection Engineering inputs is tough and painful

Who ?

- Used, Open Sourced and maintained by the EU Commission CSOC, CATCH Team (Detection Engineering Team)
- Other large SOCs adopting detection-as-code and more
- SOC Prime
- EUPL 1.2

Core Concepts

Threat + Detection Modelling

- Structures how intelligence and other input should be processed
- Creates an ever growing knowledge graph to support decision making
- Clarity to detection posture and prioritization
- As-code, YAML, Schema, LLM-ready

Detection-as-Code

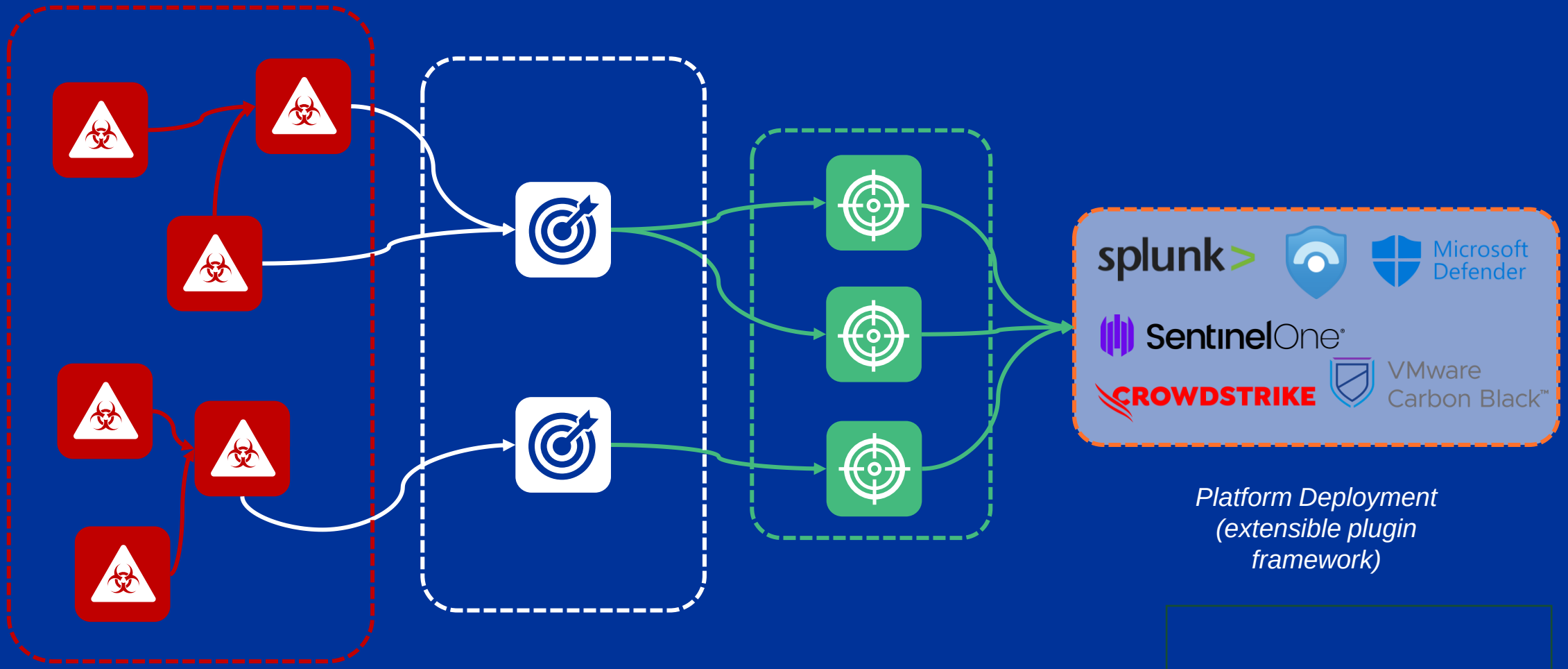
- Multi-system state of the art framework
- Multi-tenant ready
- Dynamic modifiers
- Staging and Production Workflows
- Powerful schemas and tooling
- Near or Full GUI Parity

Common DevOps Workflows, Threat Driven, Repeatable, Measurable

OpenTide Objects and Graph

Standard Schemas and CI/CD Automation

Unstructed Threat Intelligence, Red Teaming Reports, Lessons Learned, Risk Analysis…



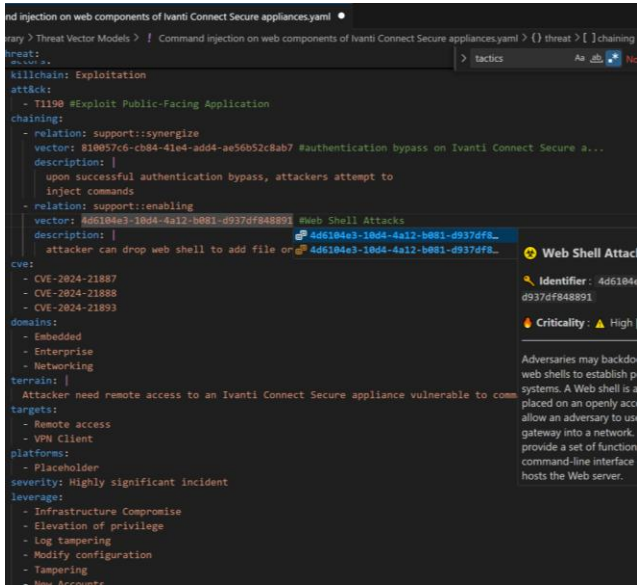
Atomic Threat Vector Graph

Detection Objectives

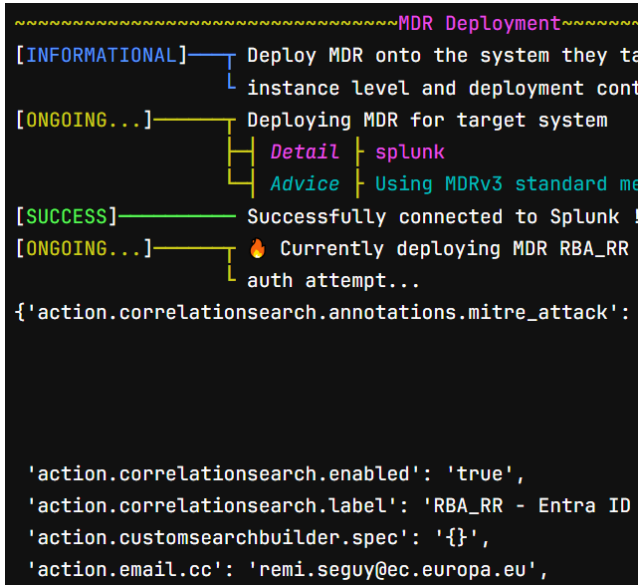
Detection Rules

Platform Deployment (extensible plugin framework)

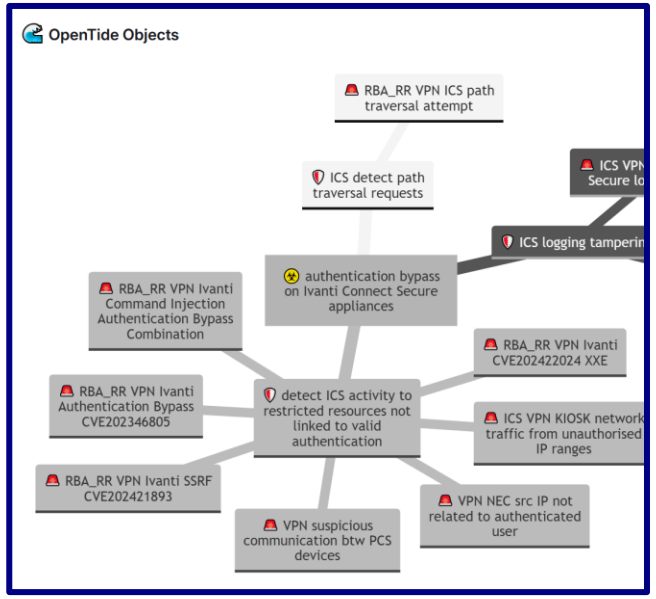
Examples



A Threat Vector File



Deployment CI Output



Auto Documentation

For who ?

Teams who want to adopt DaC

- Out-of-the-box detection-as-code framework
- Vendor agnostic standards
- Multi-system and multi-tenant ready

Teams who want to go further

- End-to-end detection coverage view
- Normalized way to process threat intelligence inputs
- Automated documentation, validation and more to boost engineering maturity

Give it a shot

- github.com/opentidehq
- Check out our whitepaper on Github
- See github.com/opentidehq/inittide for a starting repo and some documentation
- Stay in touch with the new Detection Engineering and Threat Hunting SIG within FIRST https://www.first.org/global/sigs/death/