BEERUMP 17 / 2017-06-22

TLP:WHITE

HOW AN IOC CAN LEAD TO ANOTHER?

Saâd Kadhi

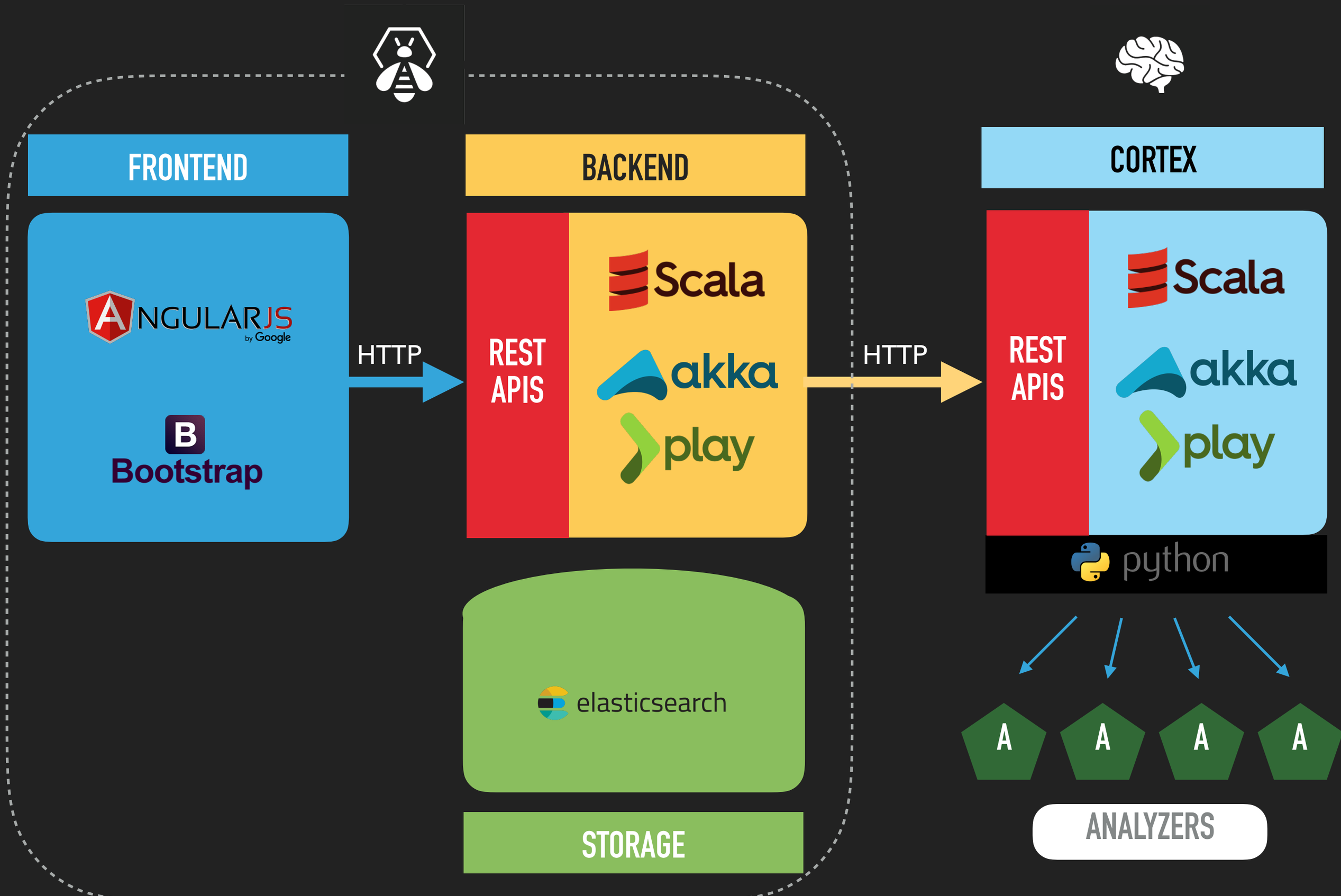
TheHive Project

Cortex

MADE IN FRANCE

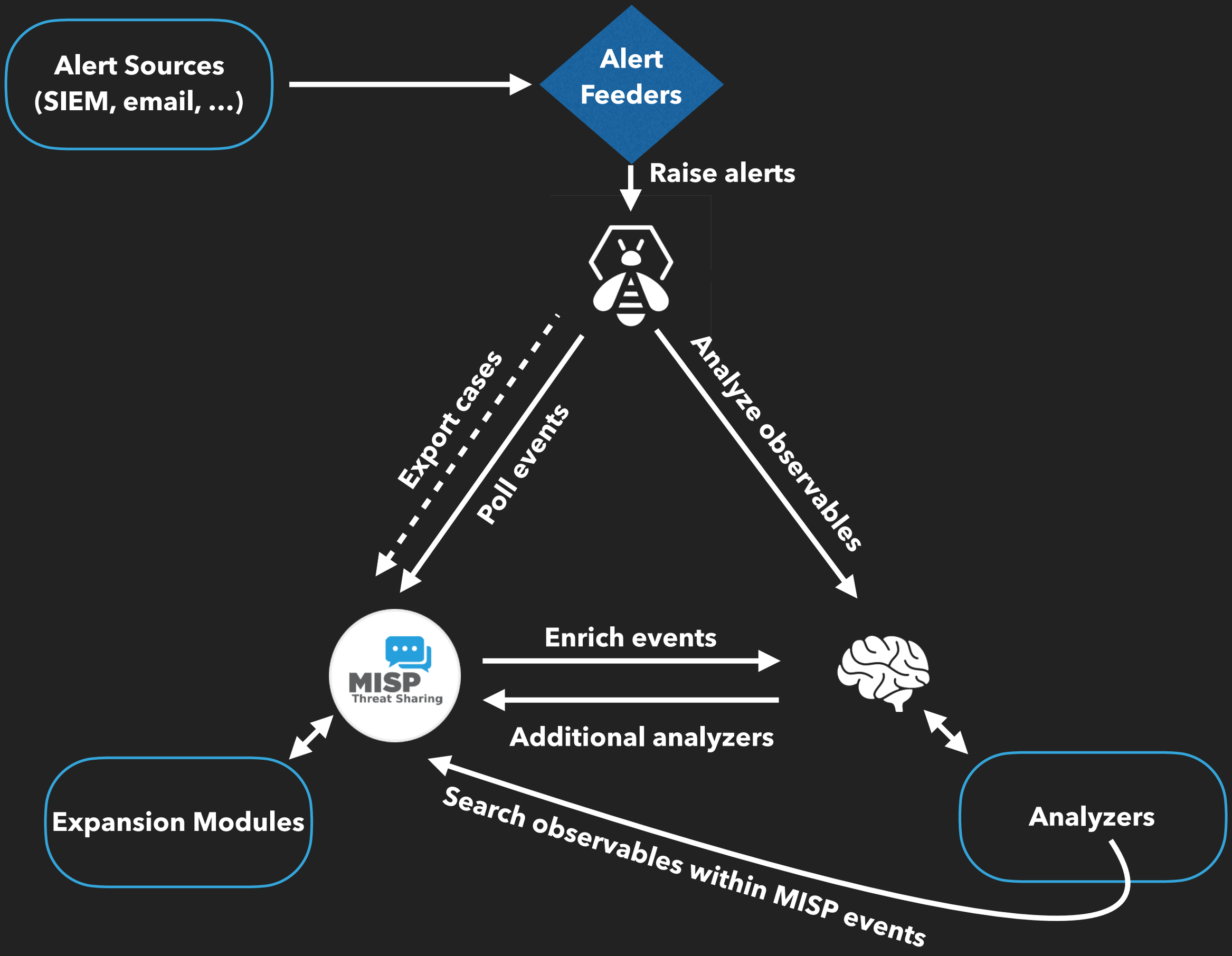
- Automate bulk observable analysis through a REST API
- Can be queried Web UI
- Analyzers can be developed in any programming language that is supported by Linux
- Two-way MISP integration
- While originally created for Blue Teams, Cortex can be useful for Red Teams too

ARCHITECTURE



23 ANALYZERS (AND MORE ARE COMING)

PASSIVETOTAL
FORTIGUARD URL CATEGORY
HIPPOCAMPE
MAXMIND
SPLUNK SEARCH
CIRCL PSSL
CIRCL PDNS
GOOGLE SAFE BROWSING
JOE SANDBOX
CUCKOO
MISP SEARCH
VIRUSTOTAL
DNSDB
VMRAY
MCAFEE ATD
DOMAINTOOLS
ABUSE FINDER
YARA
FIREHOL
IRMA
FILEINFO
NESSUS
PHISHING INITIATIVE
FAME
WHOISXMLAPI
OUTLOOK MSG PARSER
OTXQUERY
PHISHTANK
INTELMQ
FIREEYE AX
HYBRID ANALYSIS


Alert Sources
(SIEM, email, ...)
Alert
Feeders
Raise alerts
Export cases
Poll events
Analyze observables
MISP
Threat Sharing
Enrich events
Additional analyzers
Expansion Modules
Analyzers
Search observables within MISP events

LET'S GET TO WORK

- In February, numerous Polish FIs were infected after visiting the Polish Supervision Authority (www[.]knf[.]gov[.]pl) -> Watering hole attack -> Custom EK with exploits stolen from Neutrino & RIG
- Later on, it was found that other websites were used to carry the same attack: Comisión Nacional Bancaria y de Valores (MX), Banco República (UY)
- https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/

HOW CAN AN IOC LEAD TO ANOTHER?

- IOC = www[.]knf[.]gov[.]pl
- How can we pivot to find other IOCs (that are less brittle maybe?)

knf[.]gov[.]pl	MISP Search	1 event
knf[.]gov[.]pl	VirusTotal	hxxp://knf.gov.pl/DefaultDesign/Layouts/KNF2013/resources/accordian-src.js?ver=11
d4616f9706403a0d5a2f9a8726230a4693e4c95c58df5c753ccc684f1d3542e2	VirusTotal	47/61
sap[.]misapor[.]ch	MISP Search	Galaxy Lazarus Group, Target Finance

GET THE SOFTWARE

- Cortex is available under an AGPL license
- Can be installed using RPM, DEB, Docker image, binary package or built from the source code
- Pre-requisites: Linux with JRE 8+, Chrome, Firefox, IE (11), and a decent computer
- https://thehive-project.org/