Jérôme Leonard,
TheHive Project

UYBHYS'18 / 2018-11-17

TLP:WHITE

THEHIVE & CORTEX

OVERVIEW

THEHIVE PROJECT

GOALS

- DRIVE THE TIME TO DETECT & REACT
- CONTRIBUTE TO THE COMMUNITY

HOW

- ALERT/EVENT COLLECTION
- AUTOMATION
- COLLABORATION

WHAT (TOOLS)

- CYBER THREAT INTELLIGENCE
- INCIDENT RESPONSE
- DIGITAL FORENSICS

WHAT (TAKE TWO)

- LIBRARIES
- SYNAPSE
- 'FEEDERS'

WHO

- THEHIVE CORE TEAM (6 MEMBERS)
- A LARGE COMMUNITY (SOC/CSIRT/CERT)

SINCE WHEN

AGPL V3

- OCT 2014 (PRIVATE VERSION)
- NOV 2016 (FLOSS)
- FEB 2017 (CORTEX)


SPECS

AUTOMATION & COLLABORATION

- Let many analysts work on multiple cases, sometimes simultaneously
- Store observables, mark some as IOCs, make their analysis as simple as possible
- Index observables, cases and any noteworthy evidence or reference
- Let analysts search through them

AUTOMATION & COLLABORATION

- Maintain history & an audit trail
- Offer open, documented API to extract IOCs or create cases out of MISP events or SIEM alerts
- Generate statistics to drive and improve the activity
- Facilitate report writing

OPSEC ISSUES

- All observables are not created equal
- Their TLP, among other attributes, may vary
- A single case may involve observables from multiple sources
- TLP drive analysis and sharing
- Ex. a TLP:AMBER file must not be submitted to VT
- But its hash may be

SHARING IS CARING

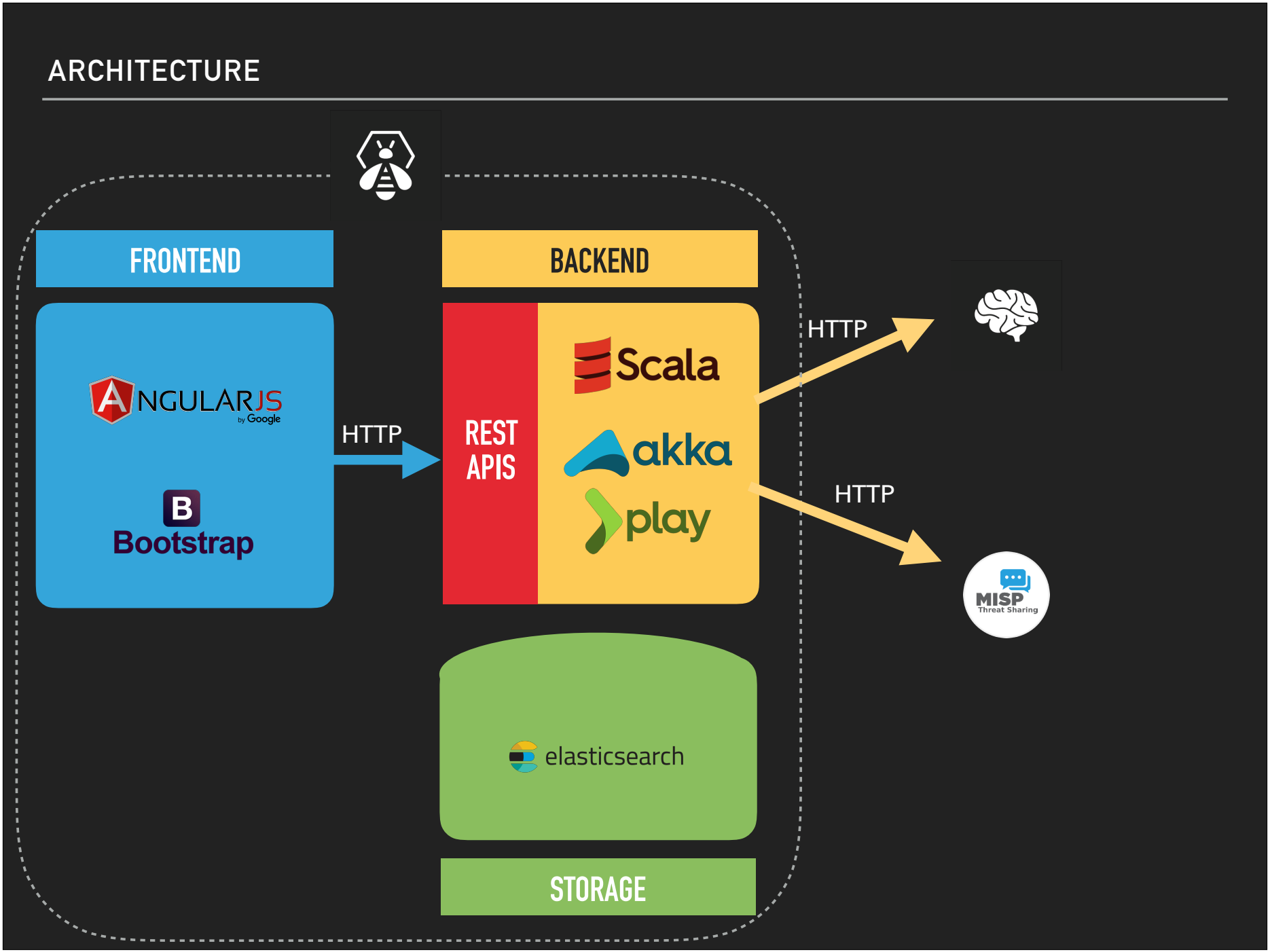
- And here we are, tired but happy
- The case has been investigated, IOCs found and proper response done
- Wait!
- Wouldn’t they be useful to peers to defend themselves?
- And maybe they will come up with complementary IOCs that went past our eyeballs undetected…

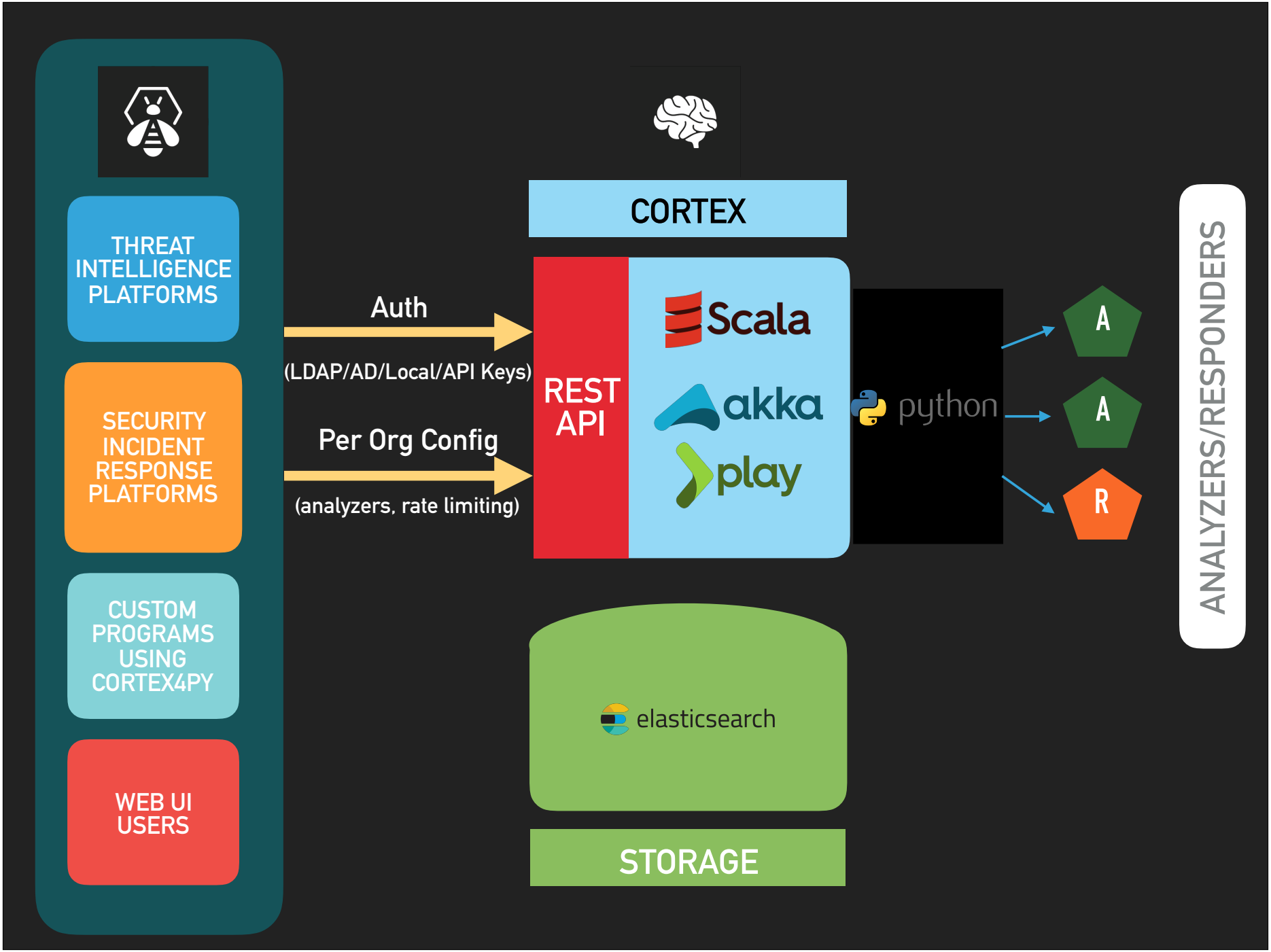
WHAT'S ON THE MARKET

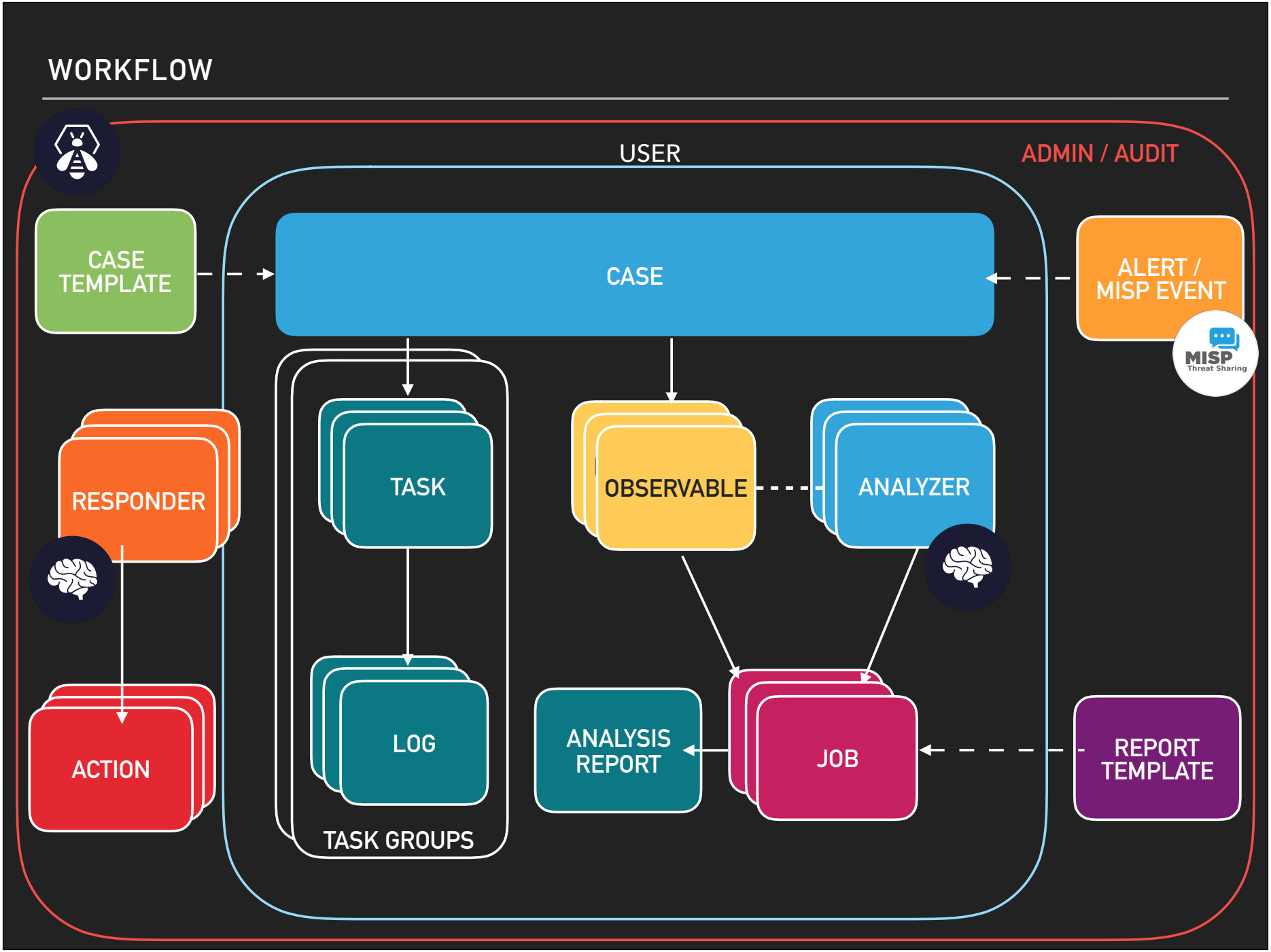
- Hunting for a solution started in early 2014
- Solutions existed but partially fulfilled the requirements
- Office (*cough*), AbuseHelper, RTIR, MISP, CIF and Resilient Systems (commercial)…
- Build vs. buy: given the requirements and our skills, we decided to build


ARCHITECTURE

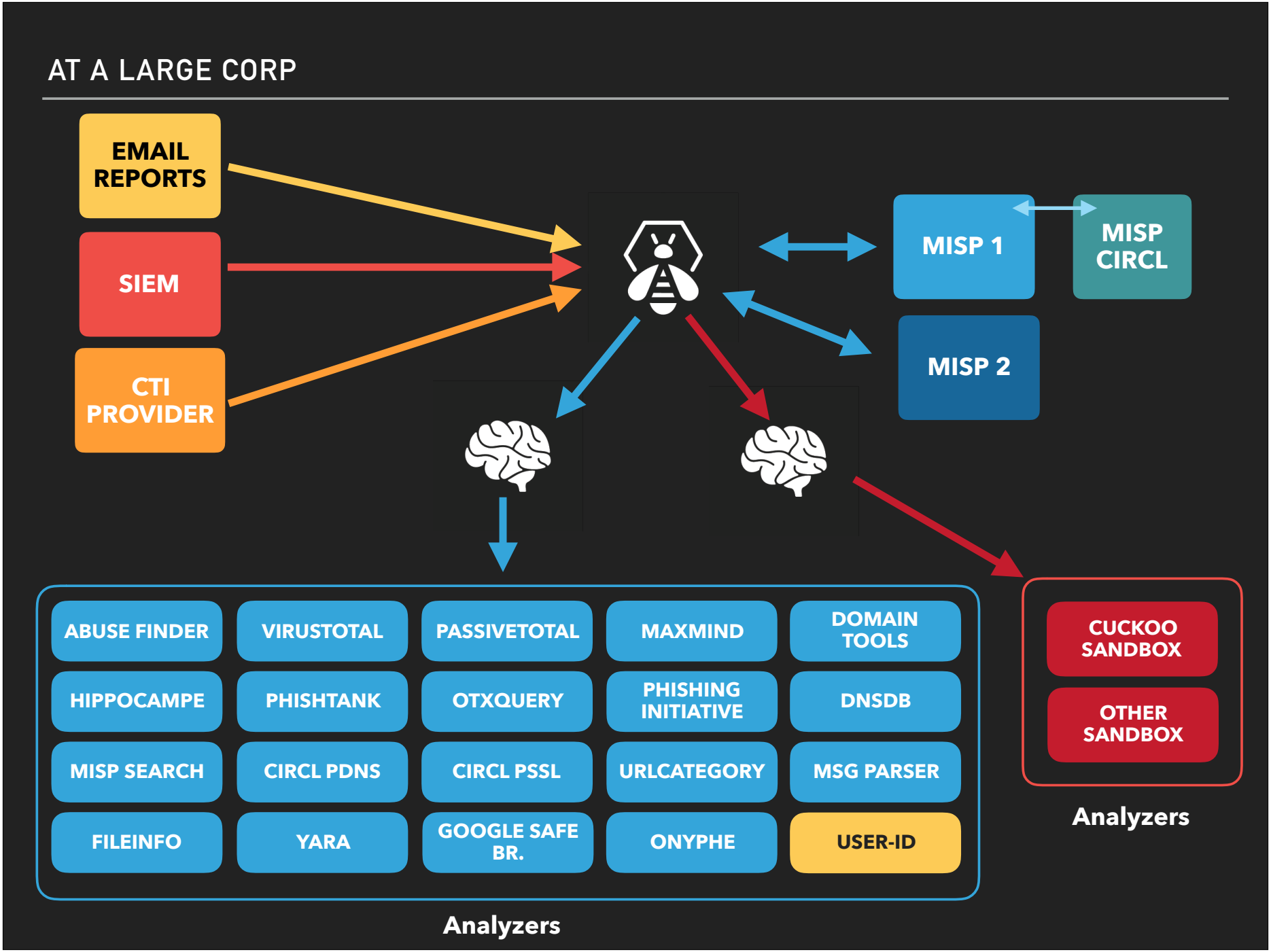
ARCHITECTURE




THREAT INTELLIGENCE PLATFORMS
SECURITY INCIDENT RESPONSE PLATFORMS
CUSTOM PROGRAMS USING CORTEX4PY
WEB UI USERS
Auth
(LDAP/AD/Local/API Keys)
Per Org Config
(analyzers, rate limiting)
CORTEX
REST API
Scala
akka
play
python
A
A
R
ANALYZERS/RESPONDERS
elasticsearch
STORAGE


WORKFLOW
USER
ADMIN / AUDIT
CASE TEMPLATE
CASE
ALERT / MISP EVENT
MISP Threat Sharing
RESPONDER
TASK
OBSERVABLE
ANALYZER
ACTION
LOG
ANALYSIS REPORT
JOB
REPORT TEMPLATE
TASK GROUPS


INTEGRATION


AT A LARGE CORP
EMAIL REPORTS
SIEM
CTI PROVIDER
MISP 1
MISP CIRCL
MISP 2
ABUSE FINDER
VIRUSTOTAL
PASSIVETOTAL
MAXMIND
DOMAIN TOOLS
HIPPOCAMPE
PHISHTANK
OTXQUERY
PHISHING INITIATIVE
DNSDB
MISP SEARCH
CIRCL PDNS
CIRCL PSSL
URLCATEGORY
MSG PARSER
FILEINFO
YARA
GOOGLE SAFE BR.
ONYPHE
USER-ID
Analyzers
CUCKOO SANDBOX
OTHER SANDBOX
Analyzers


USE CASE

SOFTWARE

- TheHive and Cortex are available under a, free, open source AGPL license
- TheHive and Cortex can be installed using RPM, DEB, Docker image, binary package or built from the source code
- Training VM available
- https://thehive-project.org/
- https://github.com/thehive-project/


THANK YOU!
@TheHive_Project