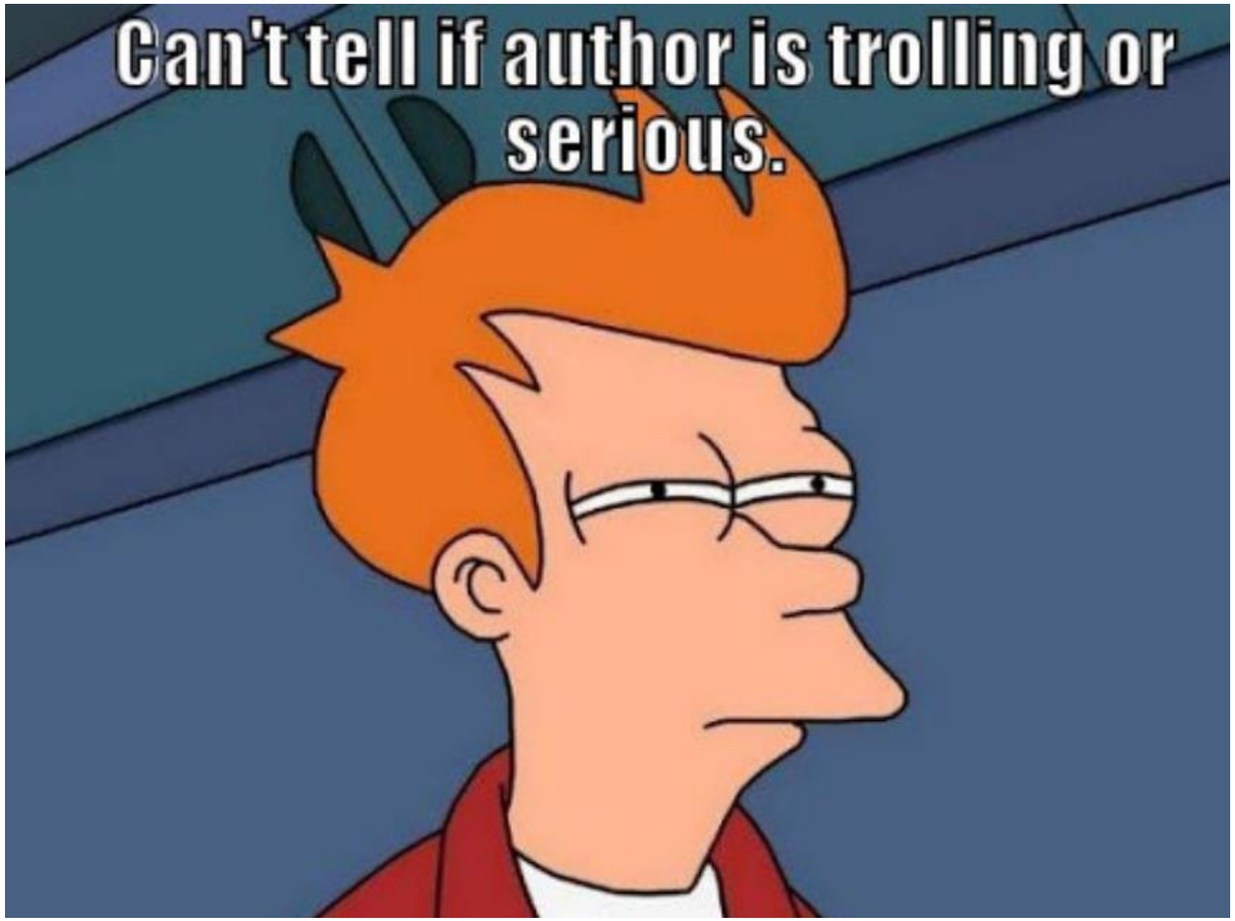
Detection Lifecycle – from a hypothesis to remediation in a DevOps style

ISSA Polska – Stowarzyszenie ds. Bezpieczeństwa Systemów Informacyjnych,

Lech Lachowicz
Dyrektor ds. Profesjonalnego Rozwoju

Disclaimer



Who am I:
IT Security freak with decent background in dev
Threat Defense lead responsible for detections, hunting, automation and breach simulation
Big fan of opensource and automation

Who I'm not:
NOT a full time Developer
NOT A DEVOPS
NOT Alfa and Omega, you can actually do it differently

What is it going to be about:
Better SECURITY

What is it not going to be about:
Software development
Writing code
I won't give you the ultimate recipe… just hints and ideas

Agenda

- The basics
- Detection Lifecycle
- Automating stuff
  - Transforming
  - Testing
  - Deploying

The basics

detection

/dɪˈtɛkʃ(ə)n/

noun

the action or process of identifying the presence of something concealed.
"the early detection of fetal abnormalities"

Synonim: observation | noticing | noting | discernment | perception | spotting

- the work of a detective in investigating a crime.
  plural noun: **detections**
  "modern technology is essential to crime detection"

  Synonim: discovery | uncovering | unearthing | rooting out | exposure | revelation

In Cyber it's usually a **search** executed in an analytical platform (SIEM typically) or a more complex **set of rules and searches** that work together to discover adversary and trigger Incident.

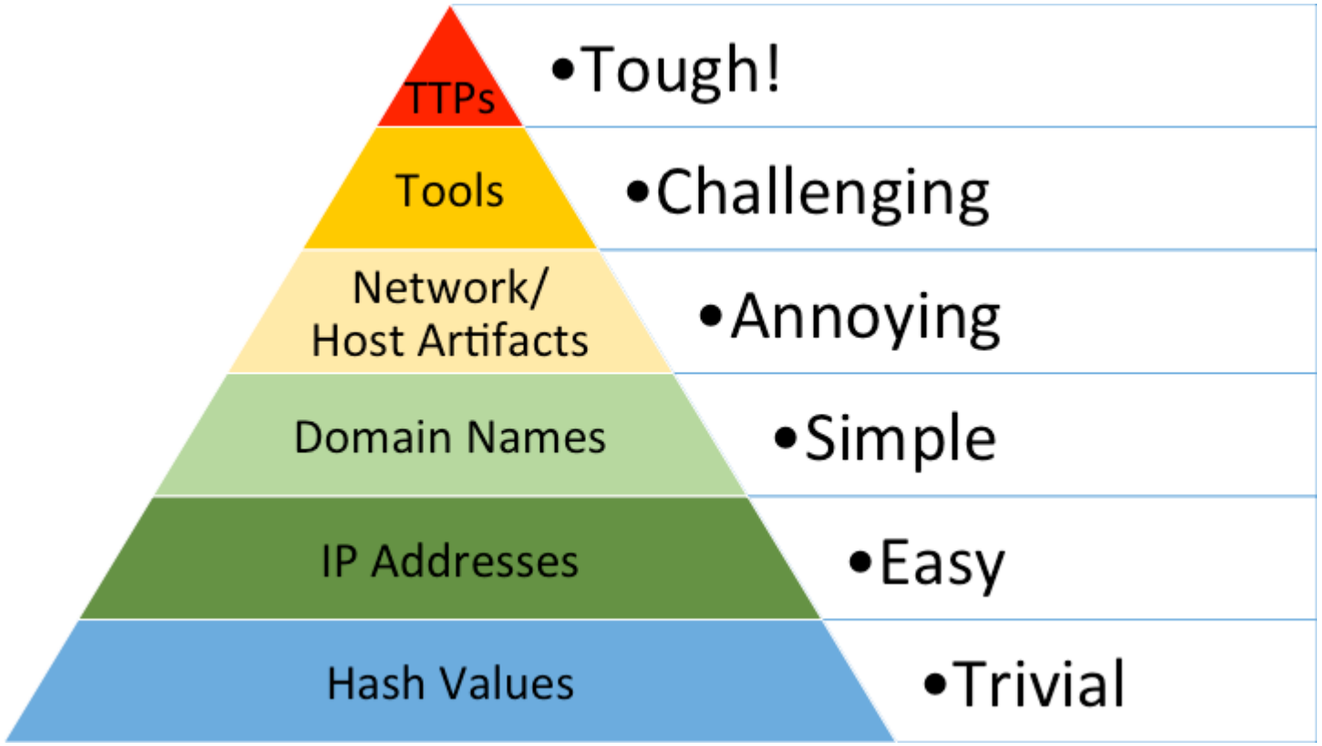
Questions without answers

What are we looking for?

How well are we doing?

How should we prioritize?

The pyramid of pain

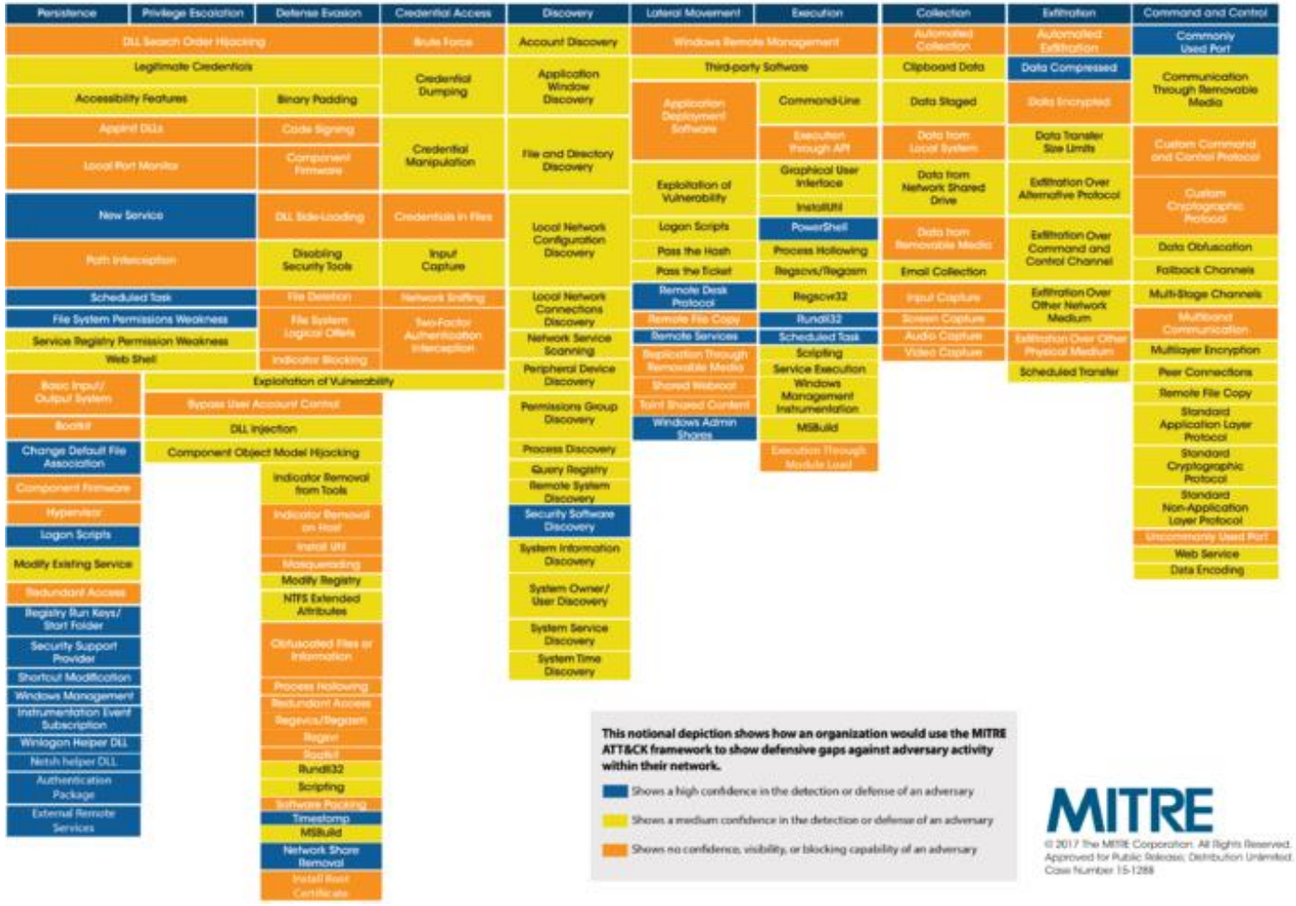


Posted 1st March 2013 by DavidJBianco

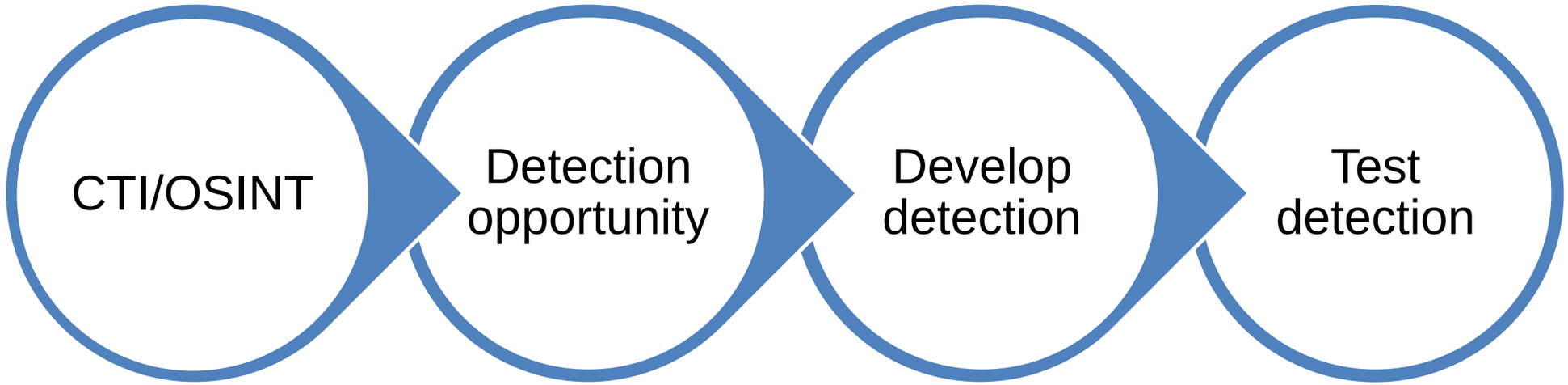
Source: https://detect-respond.blogspot.com//the-pyramid-of-pain.html

Mitre Att&ck Framework

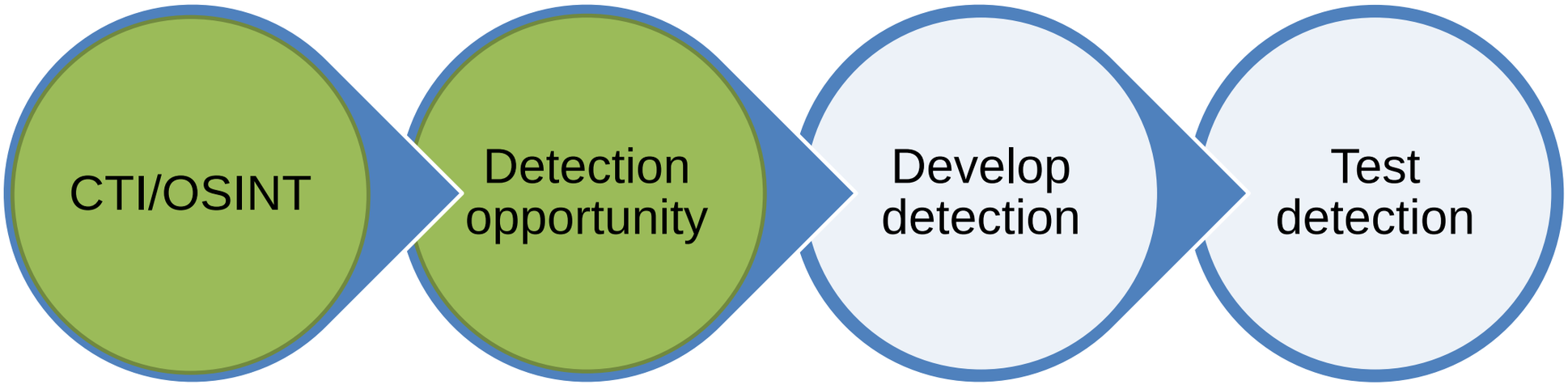
The ATT&CK matrix provides a framework for identifying tactics and techniques used by threat actors



The detection lifecycle



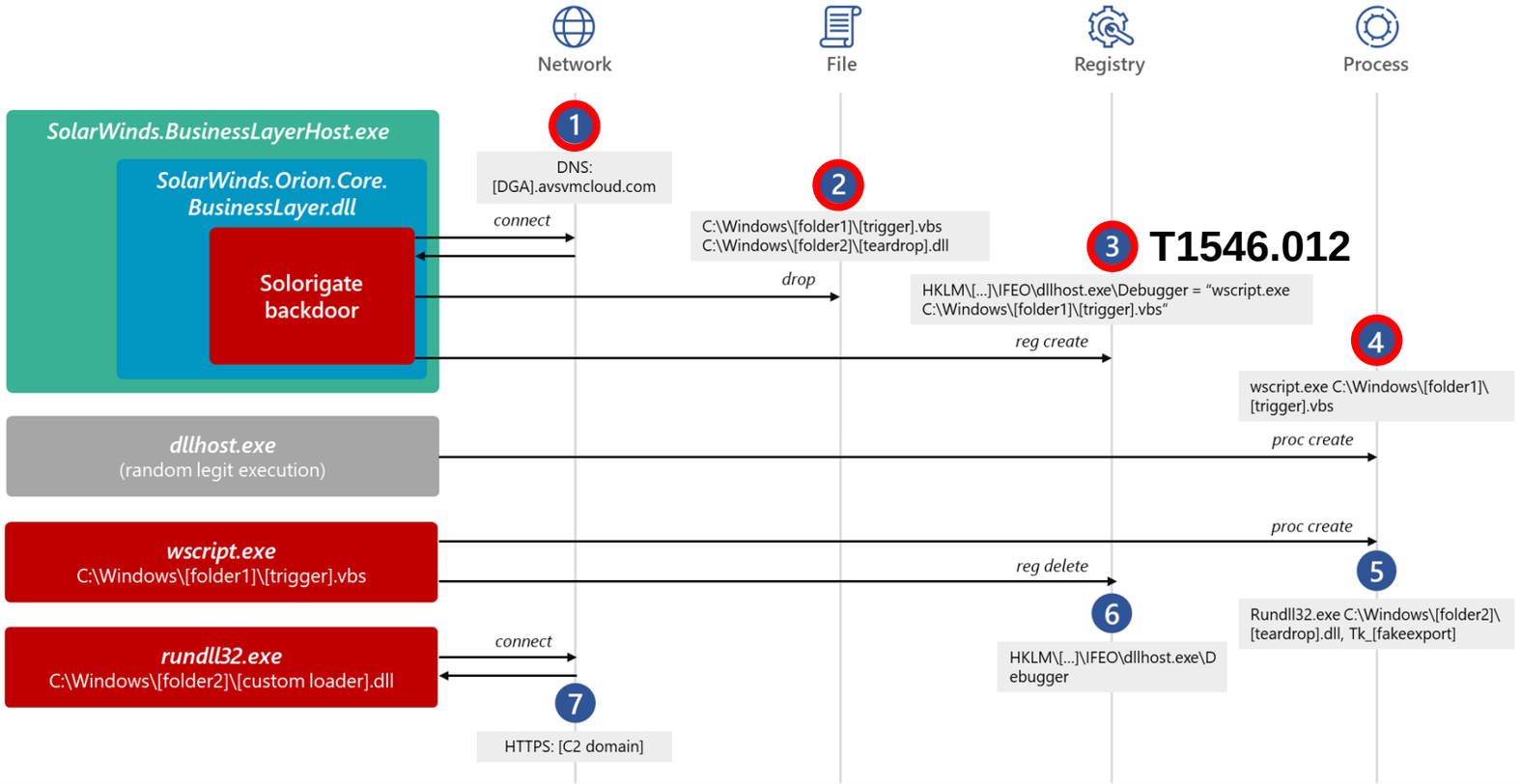
The detection lifecycle



Lets start with OSINT

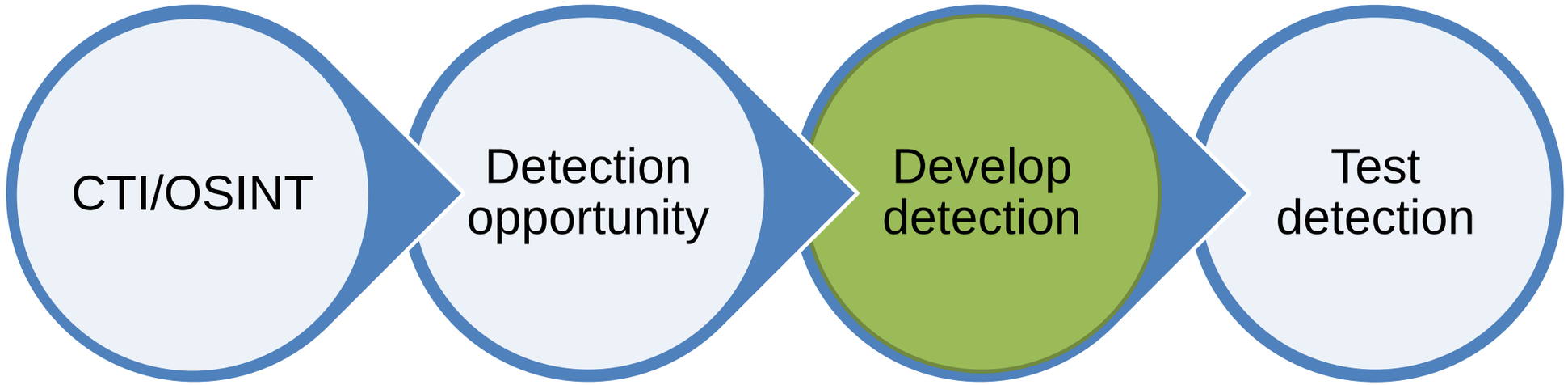
Recently hot topic – Solorigate: From SUNBURST to TEARDROP and Raindrop

Source: https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/



1. Not worth bothering
2. Better but will be FP prone if used without process name
3. Now that's something – wscript as debugger… no thanks!
4. We'll get wscript run every time dllhost.exe is spawned. This will cut the process ancestry here!

The detection lifecycle



Option 1 – use the SIEM language

Splunk Security Content

Open sourced and yaml based

Contains a lot more than just the search

Splunk optimized, fits EnterpriseSecurity and Core perfectly

Well documented with a lot of content and app ecosystem to support analyst

IMHO – still work in progress….

```yaml
name: Detect New Login Attempts to Routers
id: 104658f4-afdc-499e-9719-17243rr826f1
version: 1
date: '2017-09-12'
author: Bhavin Patel, Splunk
type: batch
datamodel:
- Authentication
description: The search queries the authentication logs for assets that are categorized
  as routers in the ES Assets and Identity Framework, to identify connections that
  have not been seen before in the last 30 days.
search: '| tstats `security_content_summariesonly` count earliest(_time) as earliest
  latest(_time) as latest from datamodel=Authentication where Authentication.dest_category=router
  by Authentication.dest Authentication.user| eval isOutlier=if(earliest >= relative_time(now(),
  "-30d@d"), 1, 0) | where isOutlier=1| `security_content_ctime(earliest)`| `security_content_ctime(latest)`
  | `drop_dm_object_name("Authentication")` | `detect_new_login_attempts_to_routers_filter`'
how_to_implement: To successfully implement this search, you must ensure the network
  router devices are categorized as "router" in the Assets and identity table. You
  must also populate the Authentication data model with logs related to users authenticating
  to routing infrastructure.
known_false_positives: Legitimate router connections may appear as new connections
references: []
tags:
```

https://github.com/splunk/security_content

Elastic EQL

Open sourced and yaml based, but… requires Enterprise

Good documentation

Elastic optimized, wont work with anything else

Not too many examples and out of box detections

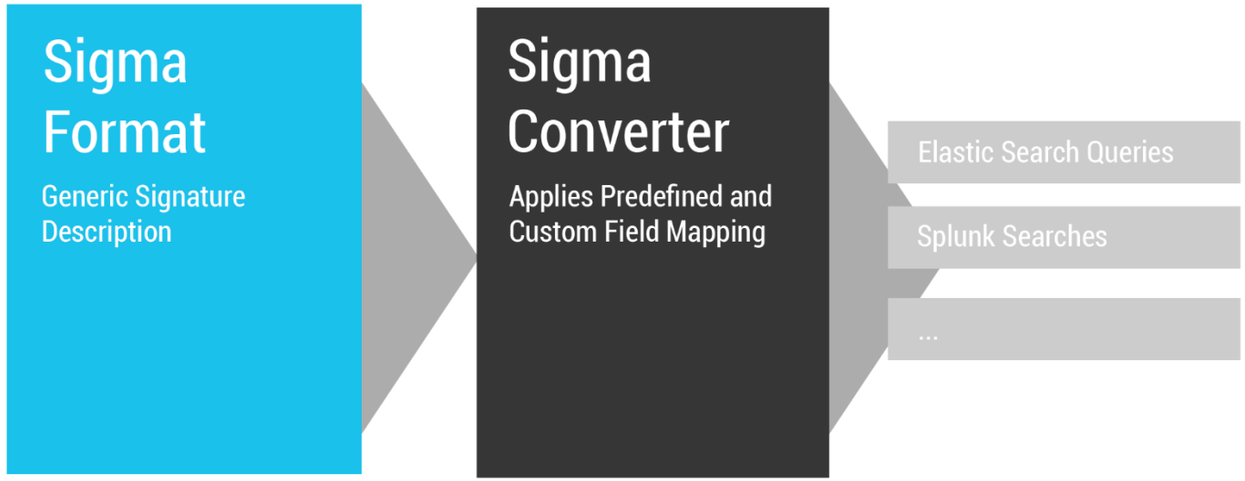
Uses ECS – Elastic Common Schema

```
{
  "query": """
    sequence
      [ process where process.name == "regsvr32.exe" ]
      [ file where stringContains(file.name, "scrobj.dll") ]
  """
}
```

https://www.elastic.co/guide/en/ecs/1.9/index.html

Option 2 – use SIGMA

Quote: “*Sigma is for log files what **Snort** is for network traffic and **YARA** is for files.*”



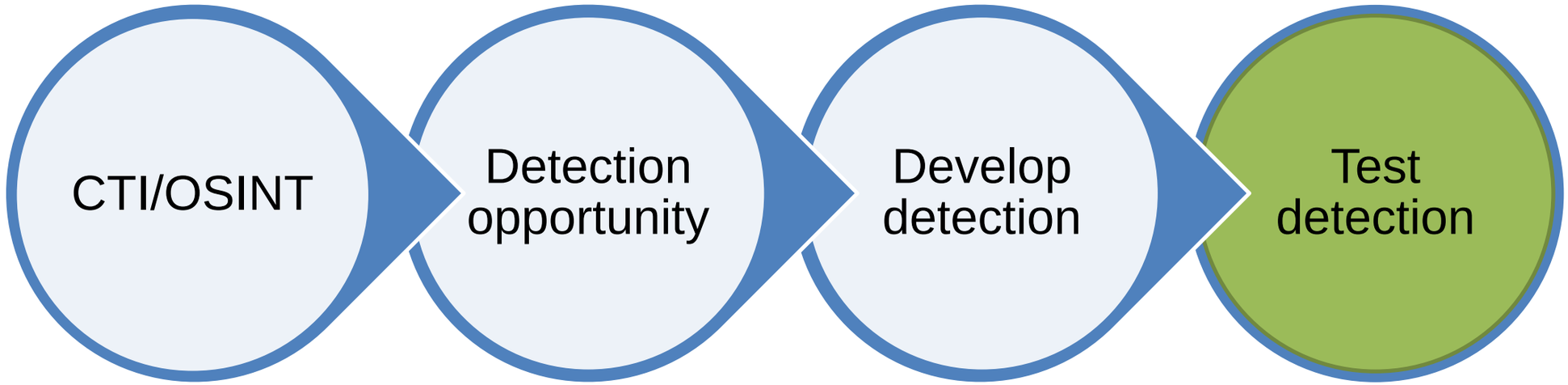
Yaml based and open sourced
Great documentation
Extensible
Flexible
Soooo many examples!

Good enough but not perfect…
Good for detections
but not right for lifecycle tracking

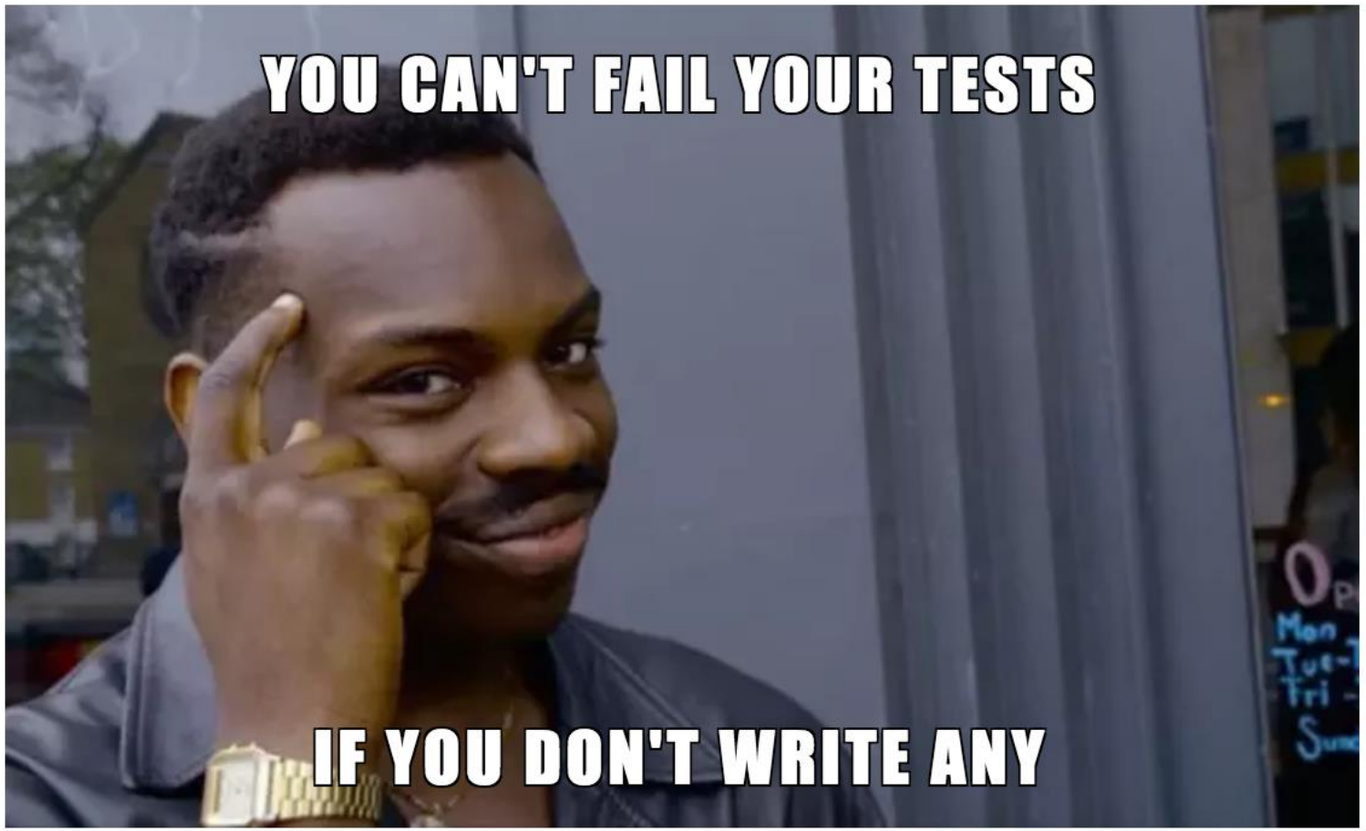
Source: https://github.com/Neo23x0/sigma

How to use SIGMA

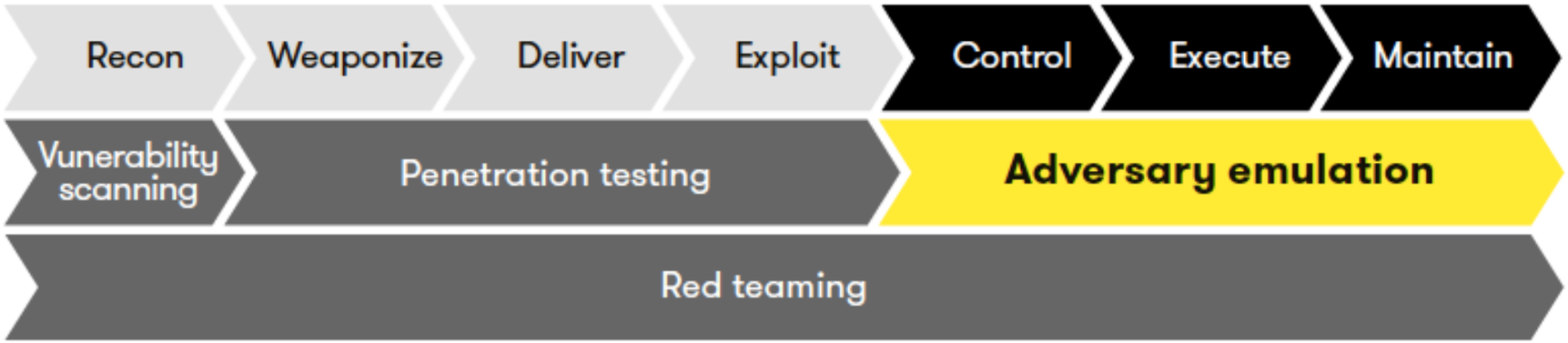
The detection lifecycle



What for?



Breach/Attack/adversary Simulation platforms



SafeBreach

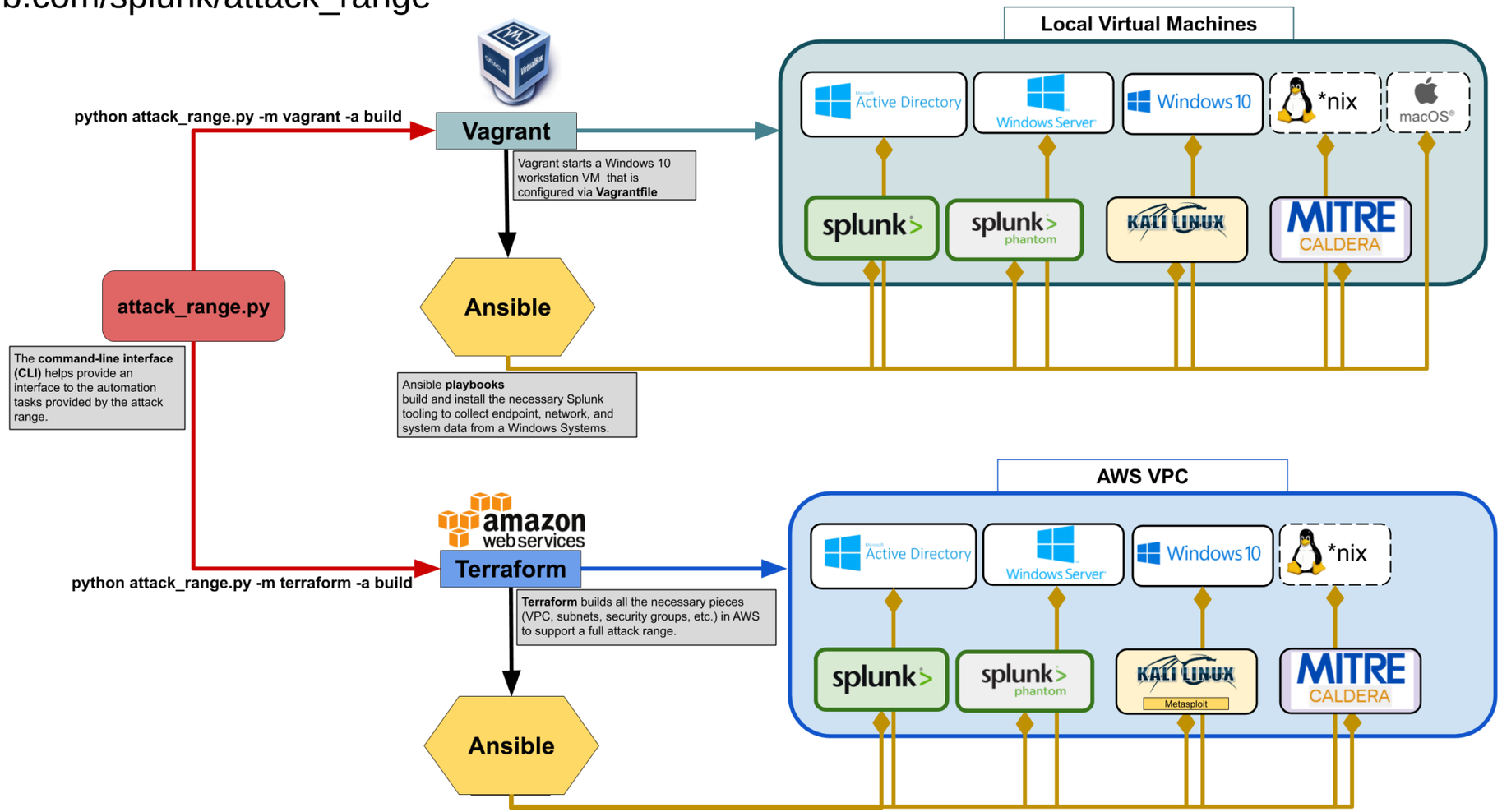
SCYTHE

CYMULATE
BREACH & ATTACK SIMULATION

ATTACKIQ®

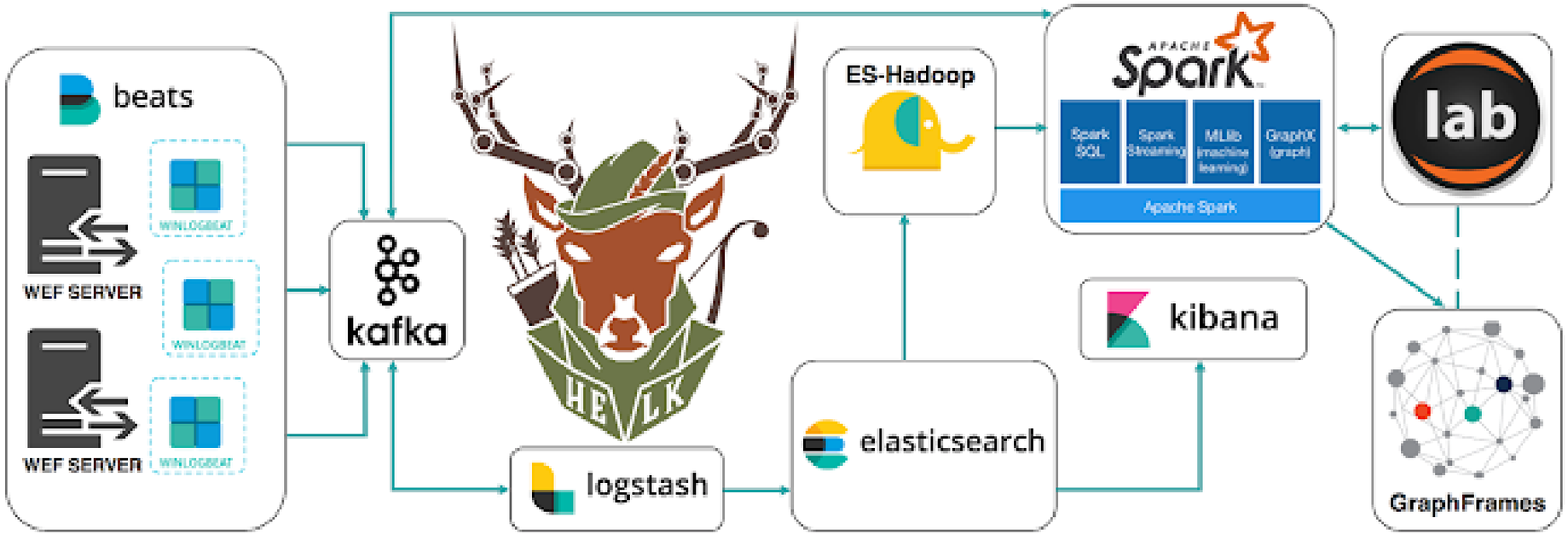
Building test environment - Splunk

https://github.com/splunk/attack_range



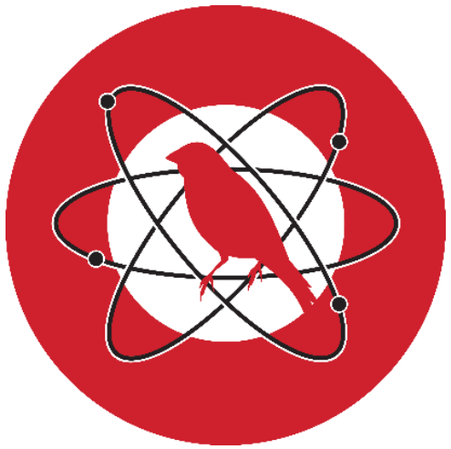
Building test environment - HELK

https://github.com/Cyb3rWard0g/HELK



No attack simulation platform ready out of box. Will have to add it ☺.

Atomic Red Team



Atomic Red Team allows every security team to test their controls by executing simple "atomic tests" that exercise the same techniques used by adversaries (all mapped to Mitre's ATT&CK).

https://github.com/redcanaryco/atomic-red-team

Atomic Red Team

Atomics – test description

Atomic Test #1 - Regsvr32 local COM scriptlet execution

Regsvr32.exe is a command-line program used to register and unregister OLE controls. Upon execution, calc.exe will be launched.

Supported Platforms: Windows

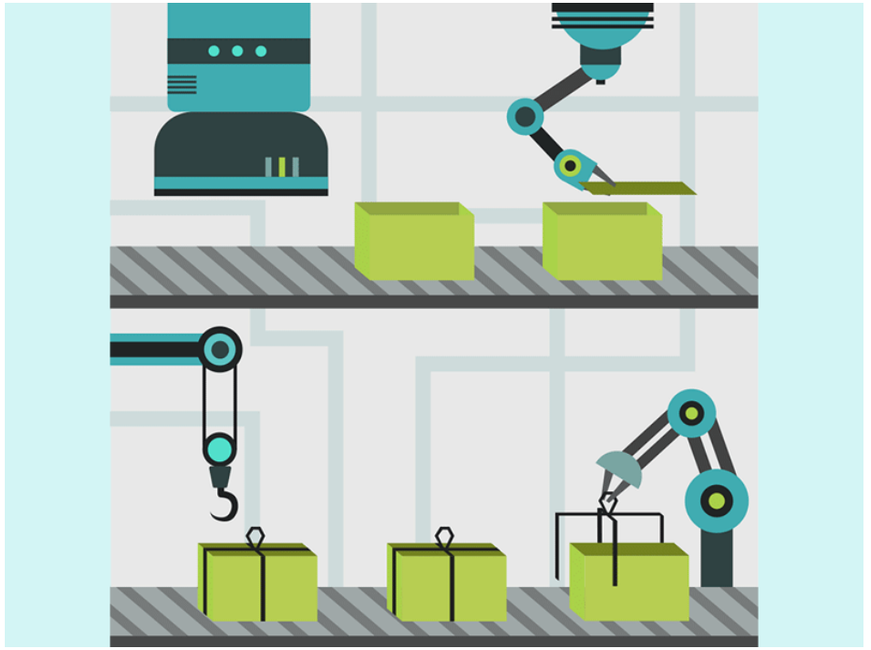
Inputs:

Name	Description	Type	Default Value
filename	Name of the local file, include path.	Path	PathToAtomicsFolder\T1218.010\src\RegSvr32.sct

Attack Commands: Run with `command_prompt` !

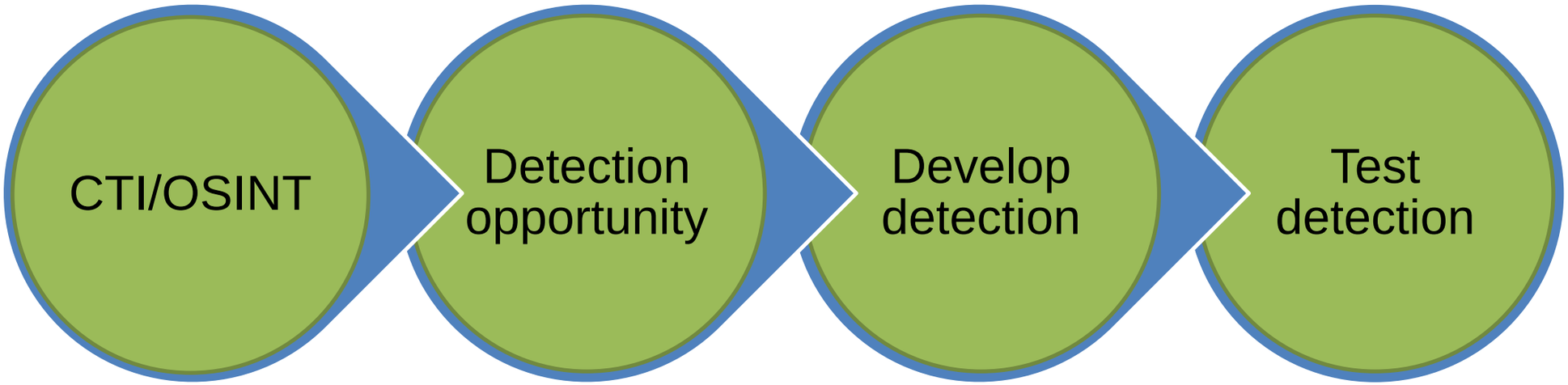
```
regsvr32.exe /s /u /i:#{filename} scrobj.dll
```

Execution Framework

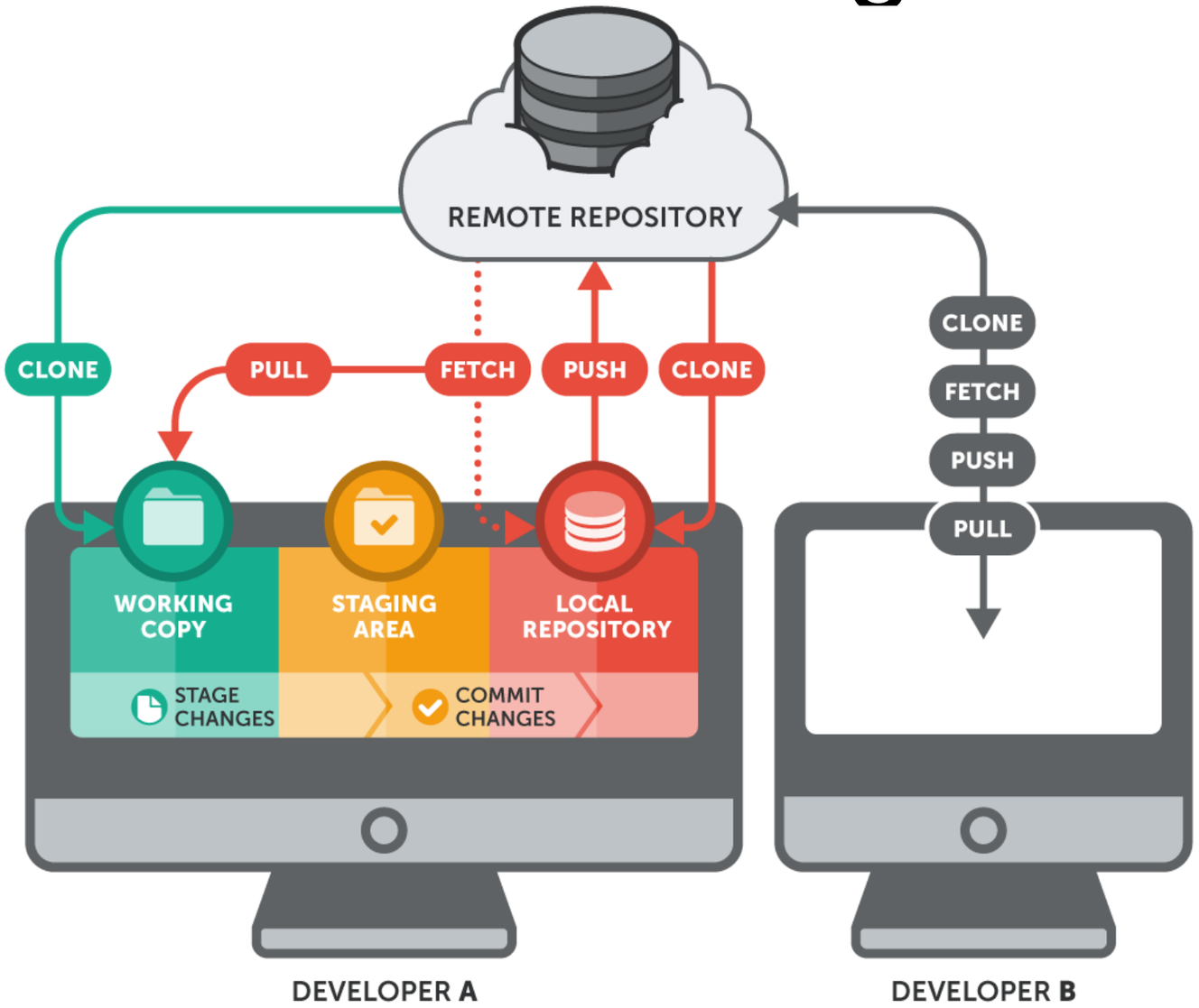


Atomic Red Team - demo

The detection lifecycle



GIT as Detection Catalog

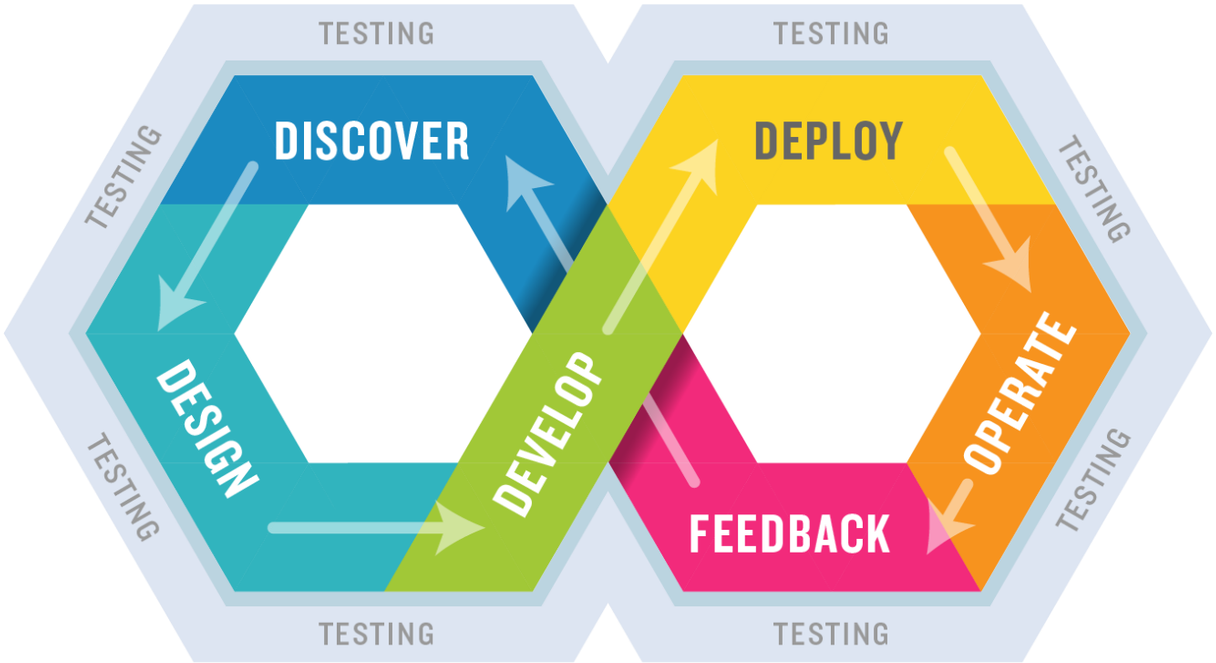


So, what's so hard about it?

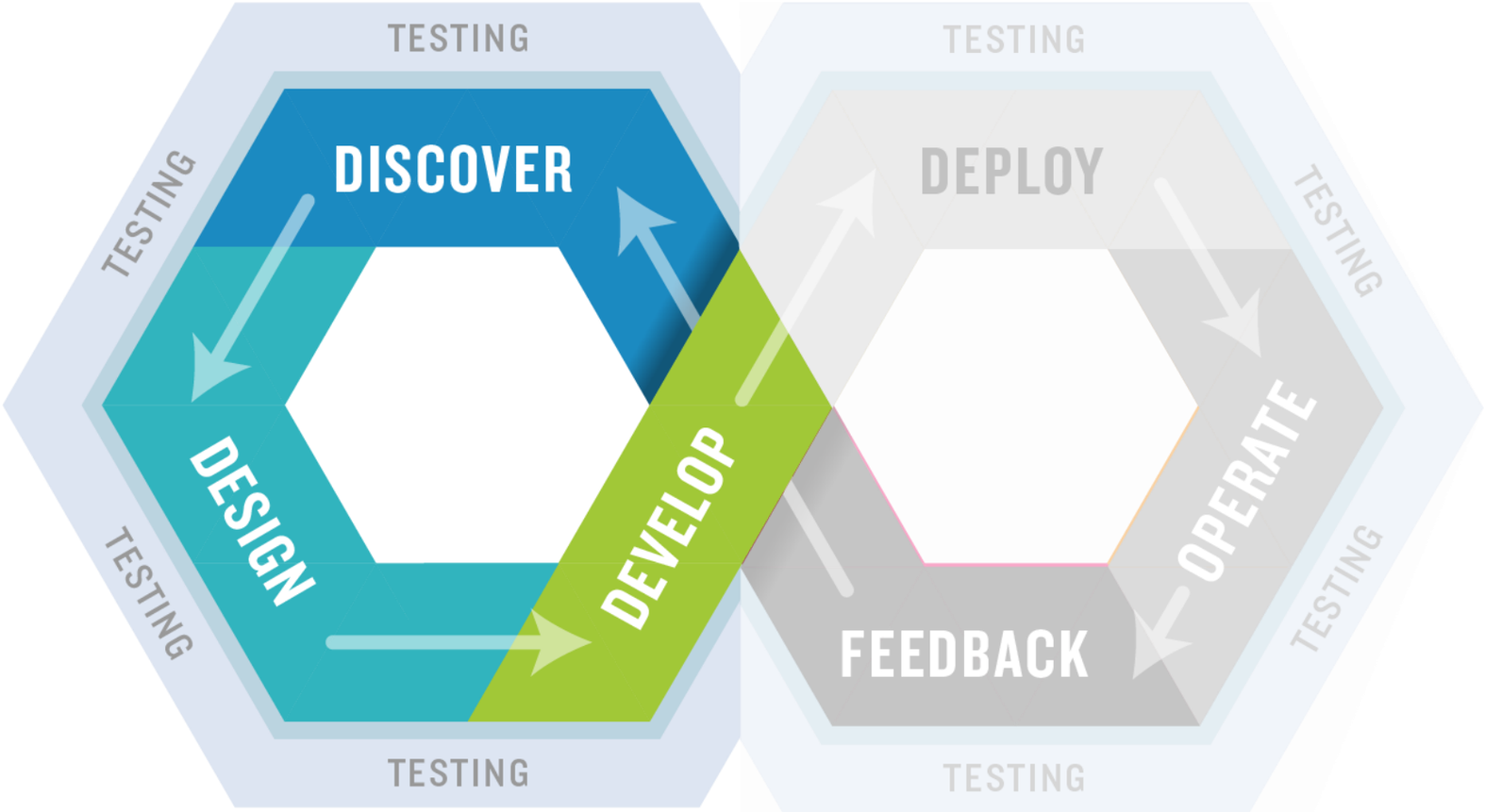
- We set it up and forget
- Some are complex to create and test
- It’s a “fingers crossed” approach – we hope it works
- Many tweaks by multiple analysts
- Changing datasets
- Changing technologies
- We need to track the effectiveness

That’s where DevOps kicks in

- Provides interoperability of software and operations to ensure the maximal data access, knowledge dissemination, and automation
- Bridges the siloed operations and development teams
- Leverages semi autonomous technologies to facilitate data driven development and communication
- Complex tasks are handed off to the machine automation to mitigate the burden of distraction and context switching
- Addresses the challenge of managing and maintaining the software development process and tools



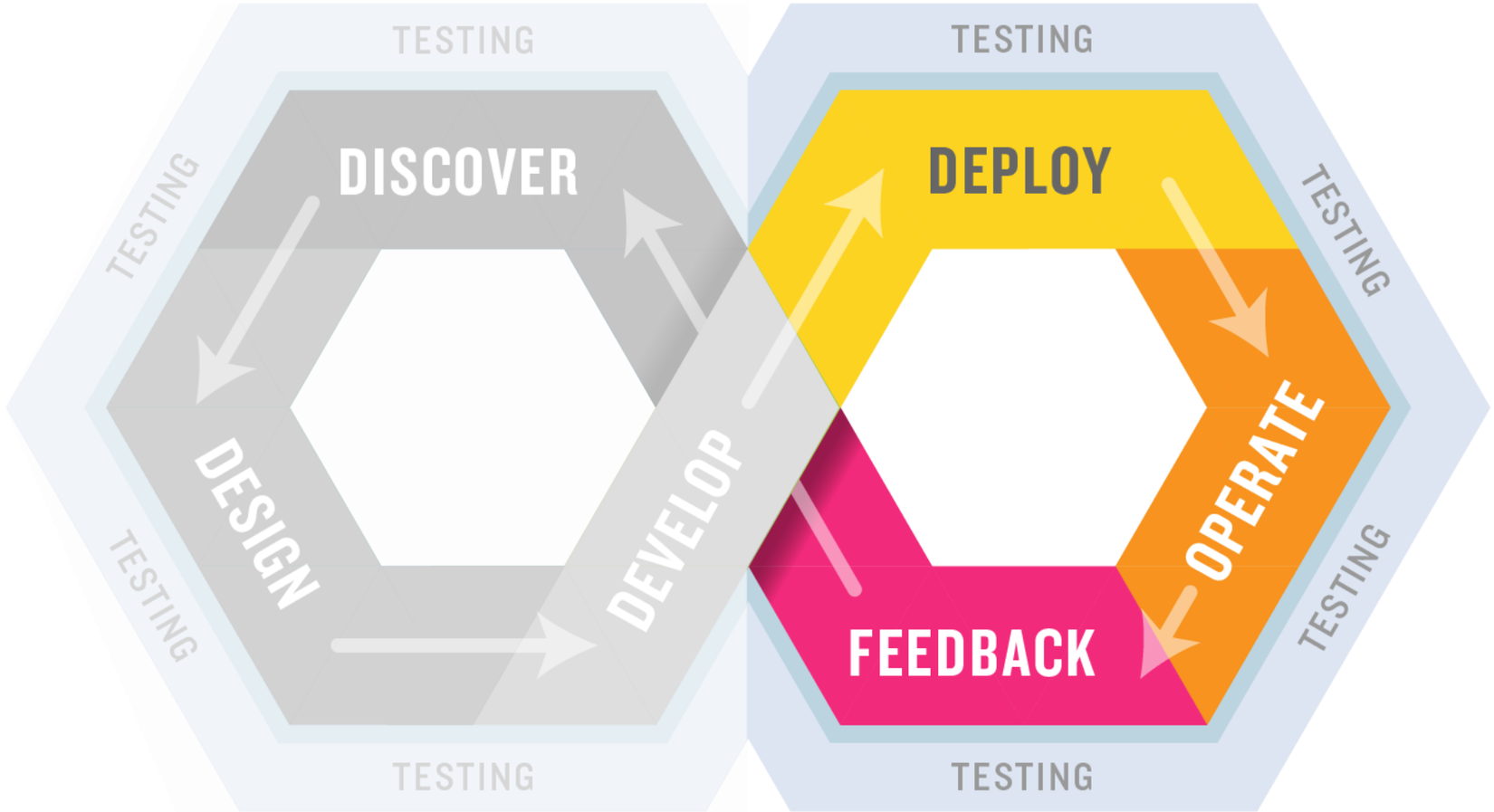
Shifting Left – Testing Earlier in the Process



Integrate automated unit, functional, API, performance, and security testing into your CI process.

Exploratory testing before the code is finished.

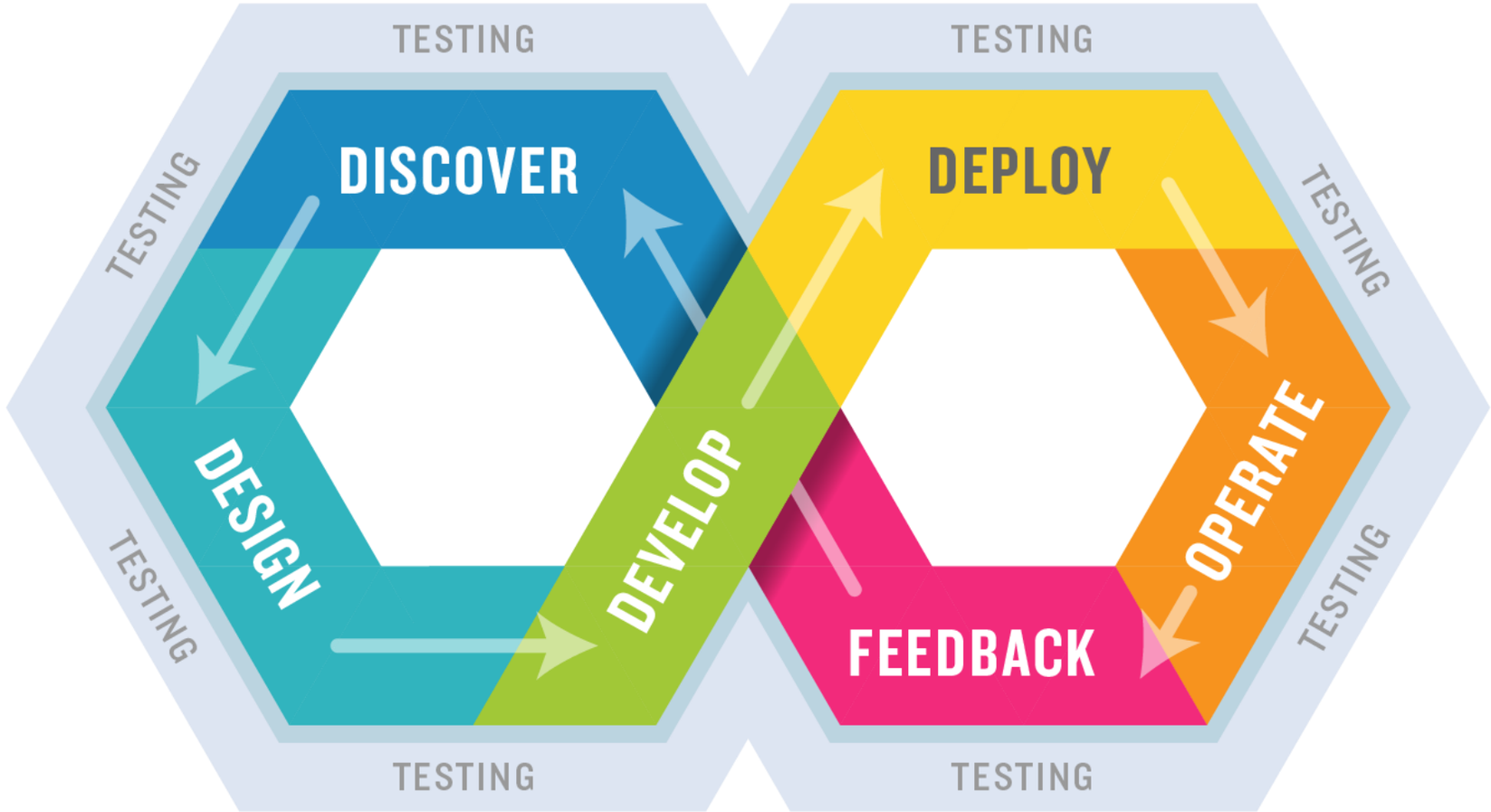
Shifting Right – Testing in Production



Integrate monitoring of the live application into your testing process.

Include system monitoring and metrics as well as input from customer support and the business.

CI/CD – automatically test and deploy



Integrate monitoring of the live application into your testing process.

Include system monitoring and metrics as well as input from customer support and the business.

CI/CD tools


Azure Pipelines


GitLab


Bamboo

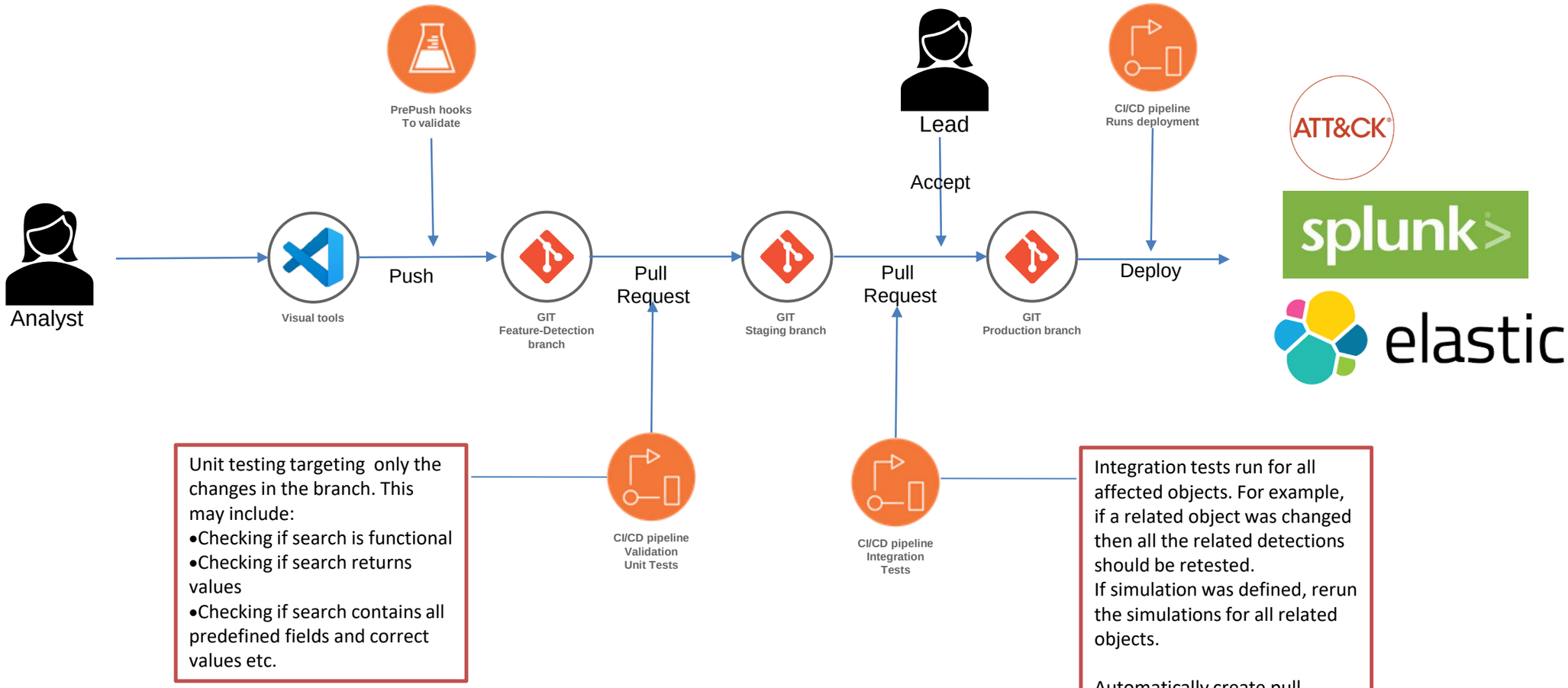

Jenkins


Bitbucket


TC
TeamCity


circleci

Detection CI/CD pipeline



Questions

Thank you

Lech Lachowicz
Mail to: lech.Lachowicz@issa.com.pl