Code Reuse Analysis

Transforming a Disadvantage into a Game-Changing Advantage

INTEZER

Shaul Holtzman

Who Am I?

Shaul Holtzman

- Headed cybersecurity training operations in the Israeli Defense Force (IDF)
- Former incident response analyst at Verint
- Account and Intezer Analyze community manager

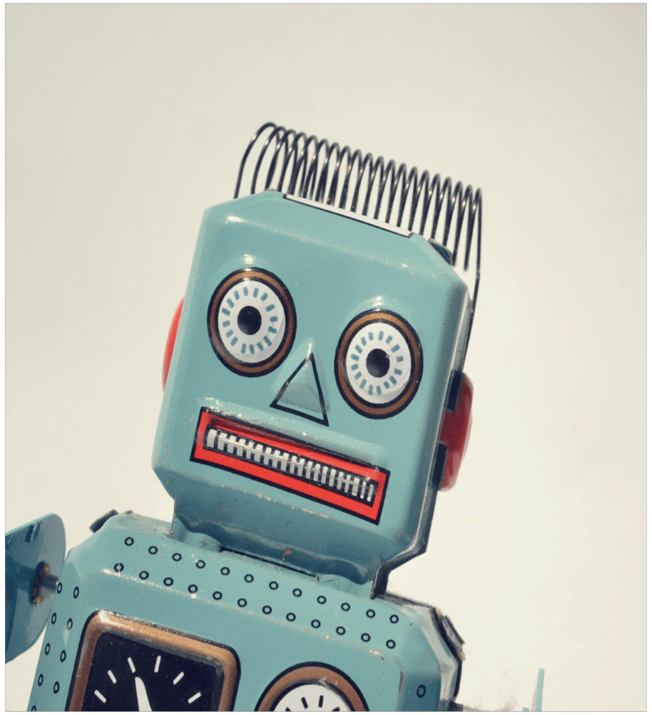
@ShaulHol

The Needle in the Haystack

Common Solutions

Beautify

Playbooks



Common Solutions

Beautify

1) Better looking SIEM UI

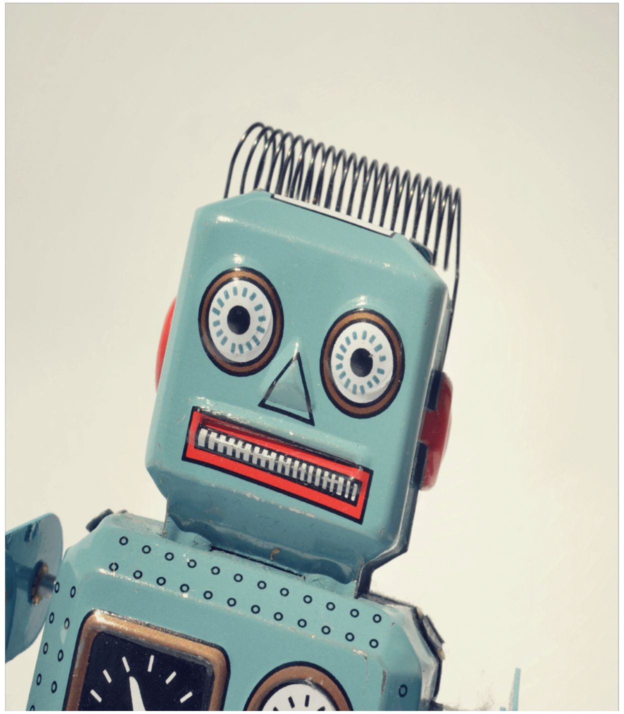
2) Organize and cluster alerts

3) Additional metadata on alerts

PROBLEM: It’s just a bit more convenient. Many alerts are still not handled.

Common Solutions

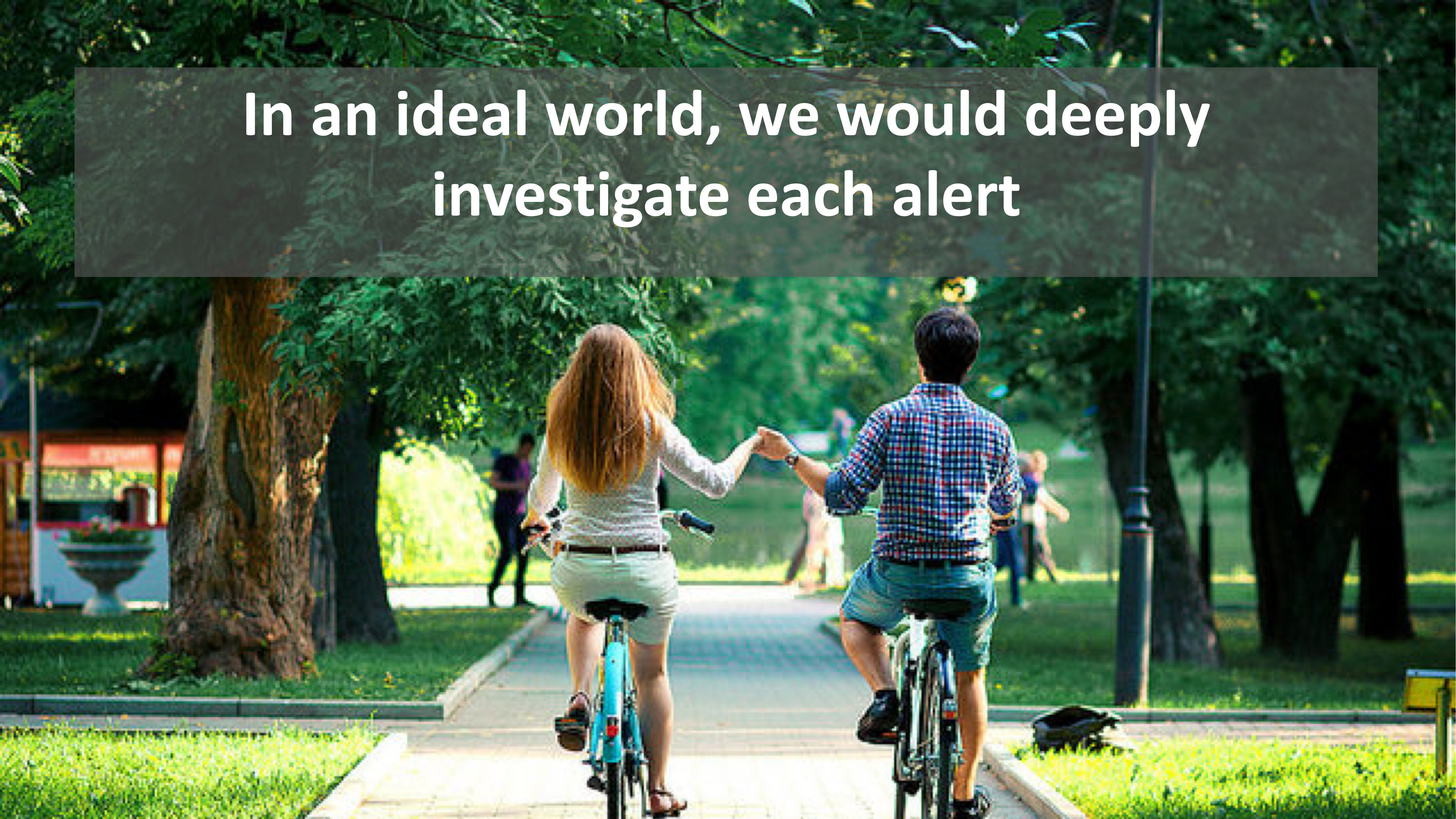
Playbooks



1) Automatic playbooks for handling alerts

2) Utilizes external security systems for analysis and response

PROBLEM: If you don't have the "brains", automation is limited to simple cases.



In an ideal world, we would deeply investigate each alert

Alert Analysis

Files

A handy team of reverse engineers would be able to answer the most critical questions about each alert:

1) Is it **good or bad**?

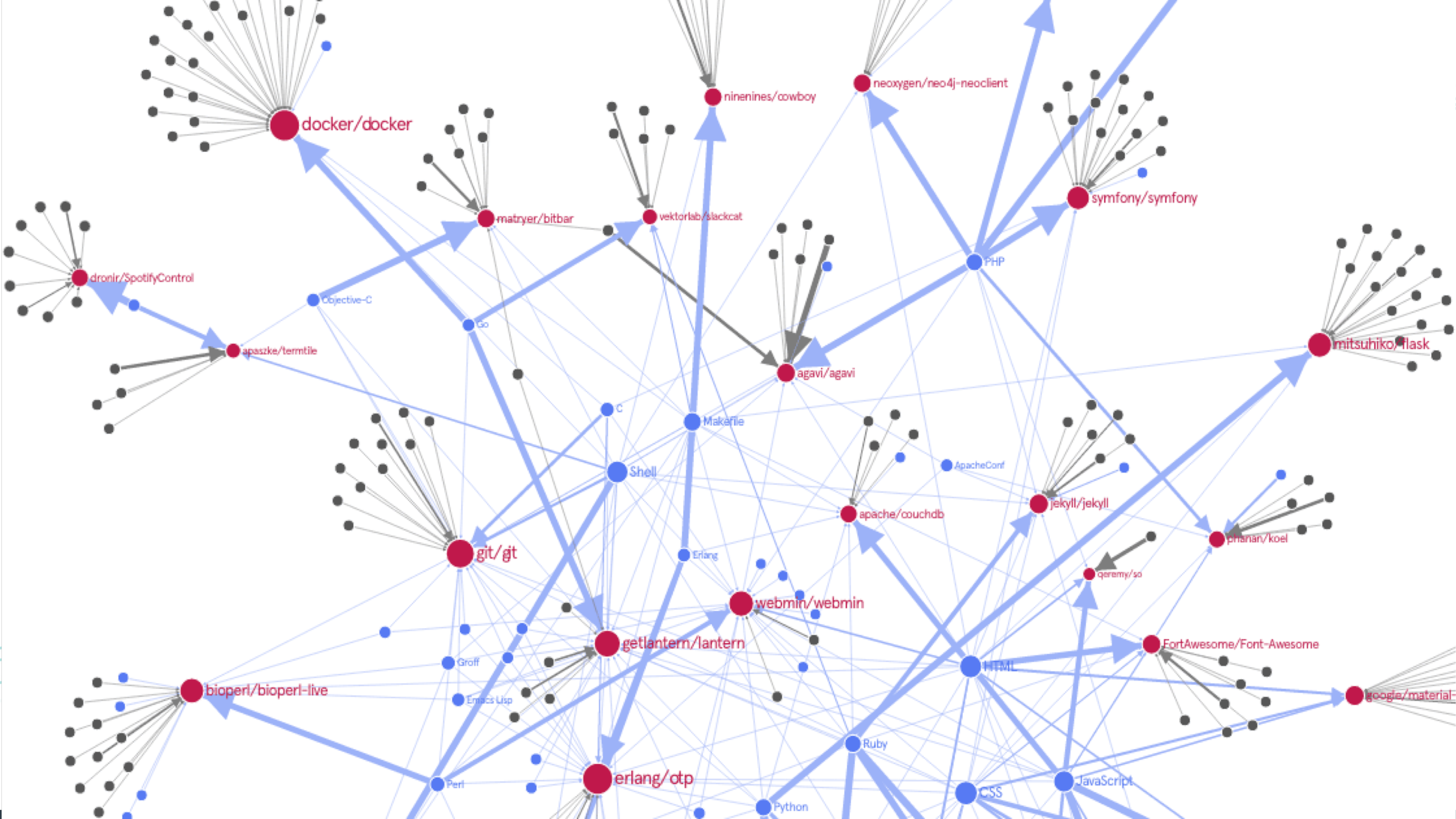
2) What is the **risk level** or priority?

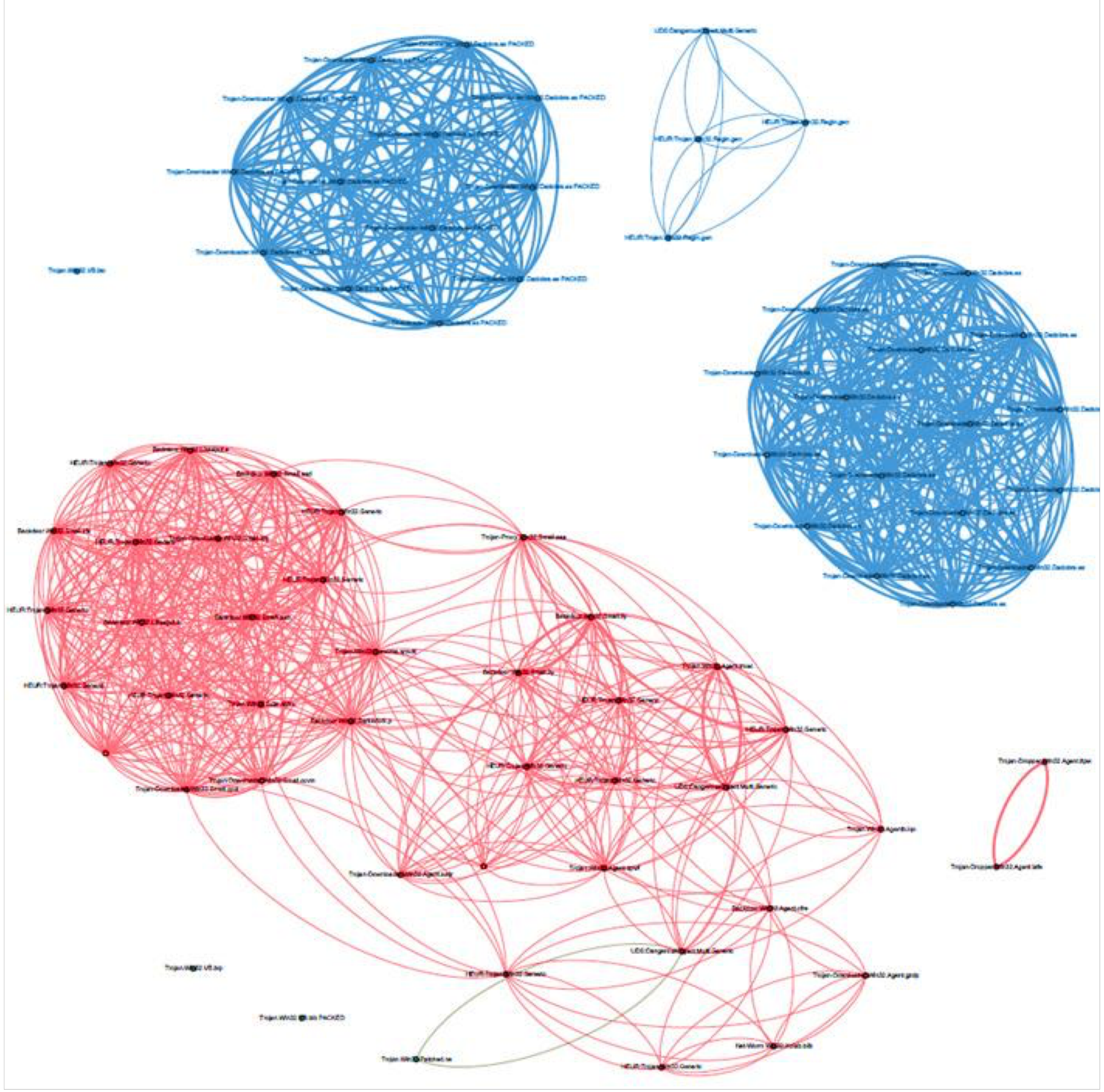
3) What is the **goal of the attacker**?

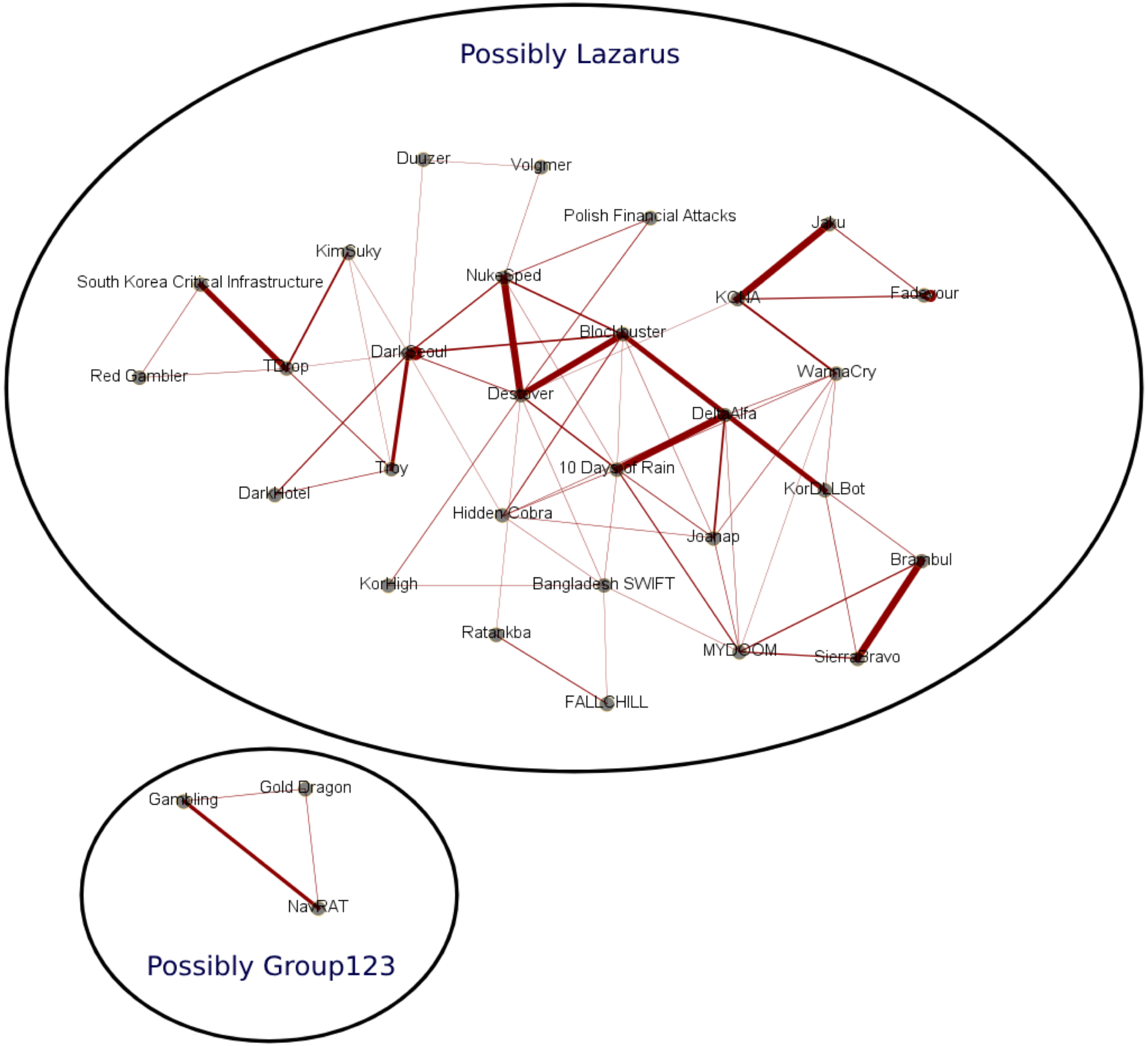
4) Is the threat related to a **previous incident** we had?

Automating Malware Analysis & Reverse Engineering

How is that possible?


docker/docker
ninenines/cowboy
neoxygen/neo4j-neoclient
symfony/symfony
matryer/bitbar
vektorlab/slackcat
dronir/SpotifyControl
Objective-C
Go
apaszke/termtile
PHP
agavi/agavi
mitsuhiko/flask
C
Makefile
Shell
ApacheConf
apache/couchdb
jekyll/jekyll
phanan/koel
git/git
Erlang
webmin/webmin
qeremy/so
getlantern/lantern
Groff
FortAwesome/Font-Awesome
HTML
bioperl/bioperl-live
Emacs Lisp
google/material-
Ruby
erlang/otp
Perl
Python
CSS
JavaScript




Possibly Lazarus
Duuzer
Volgmer
Polish Financial Attacks
Jaku
KimSuky
NukeSped
South Korea Critical Infrastructure
KONA
Fadeyour
Blockbuster
DarkSeoul
TDrop
Red Gambler
Destover
WannaCry
DeltaAlfa
10 Days of Rain
Troy
DarkHotel
KorDLLBot
Hidden Cobra
Joanap
Brambul
KorHigh
Bangladesh SWIFT
Ratankba
MYDOOM
SierraBravo
FALLCHILL
Gambling
Gold Dragon
NavRAT
Possibly Group123

INTEZER

Software is Evolutionary

- Just like in biology, software has ancestral relations

- Every piece of software is based on previously written code

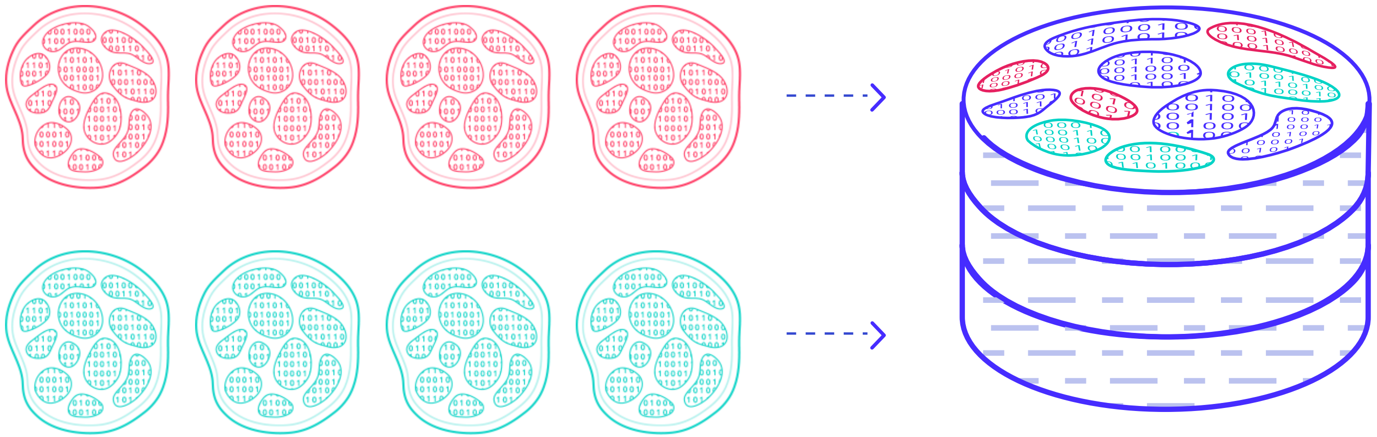
- Detecting **code reuse** is equivalent to mapping the DNA of an organism

Genetic Malware Analysis

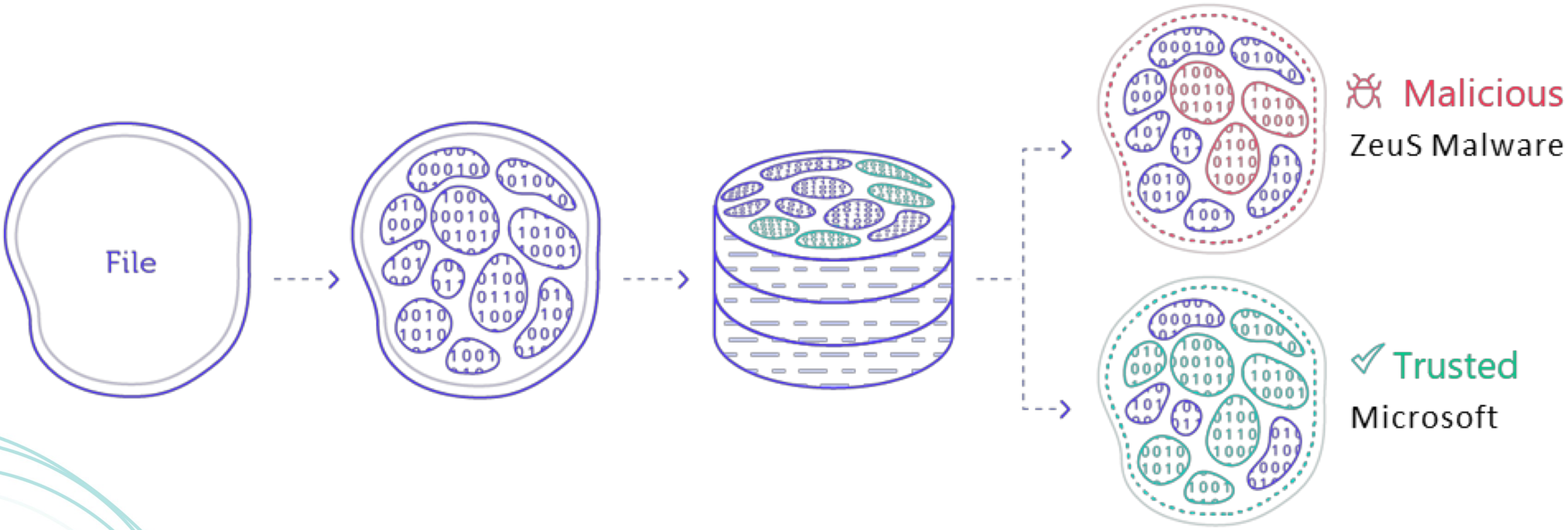
Code Genome Database

Malware

Trusted software



Genetic Malware Analysis



Unknown file

Extracting genes

Code genome database containing billions of genes

Identifying and classifying unknown and reused code

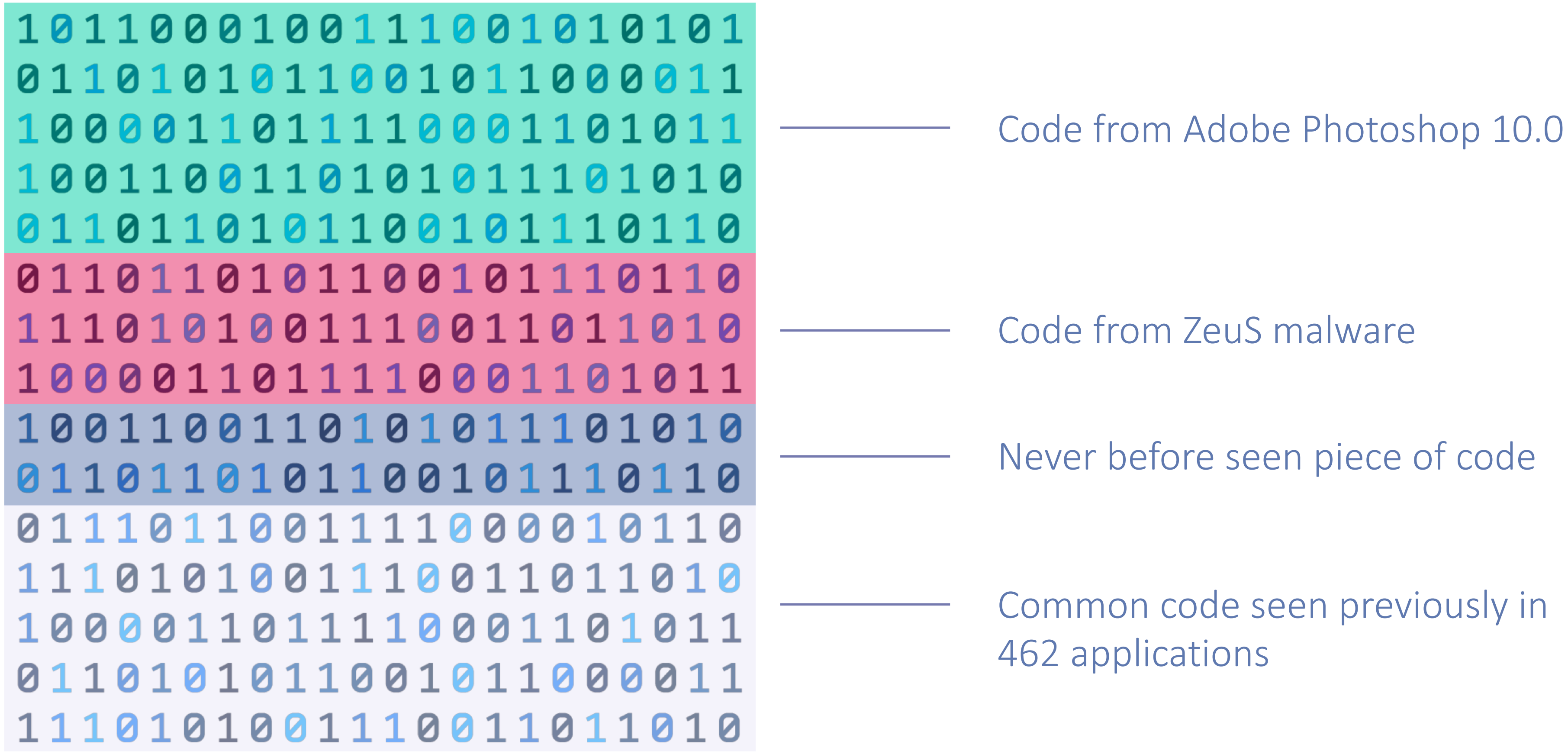
Malicious

ZeuS Malware

✓ Trusted

Microsoft

Genetic Malware Analysis



```
1011000100111001010101
0110101011001011000011
1000011011110001101011
1001100110101011101010
0110110101100101110110
0110110101100101110110
1110101001110011011010
1000011011110001101011
1001100110101011101010
0110110101100101110110
0111011001111000010110
1110101001110011011010
1000011011110001101011
0110101011001011000011
1110101001110011011010
```

Code from Adobe Photoshop 10.0

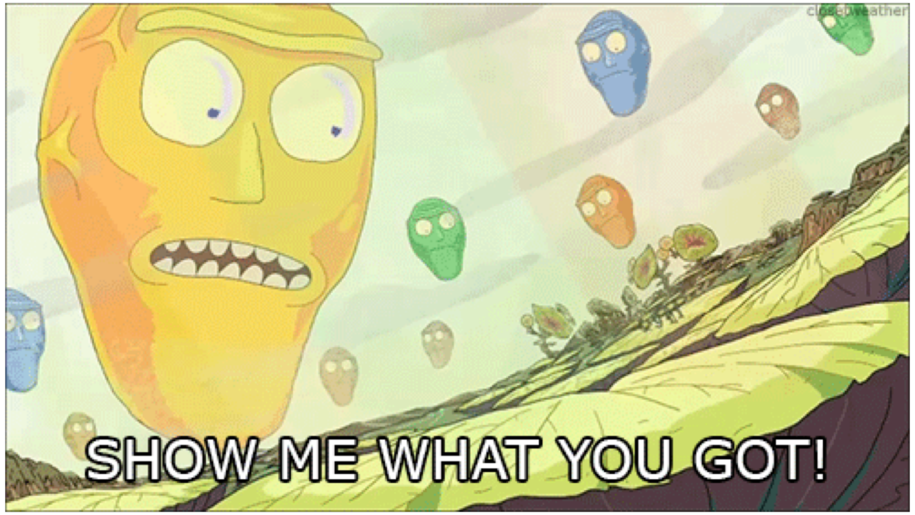
Code from ZeuS malware

Never before seen piece of code

Common code seen previously in 462 applications

INTEZER

Examples



Emotet

1) Most common banking trojan in the world

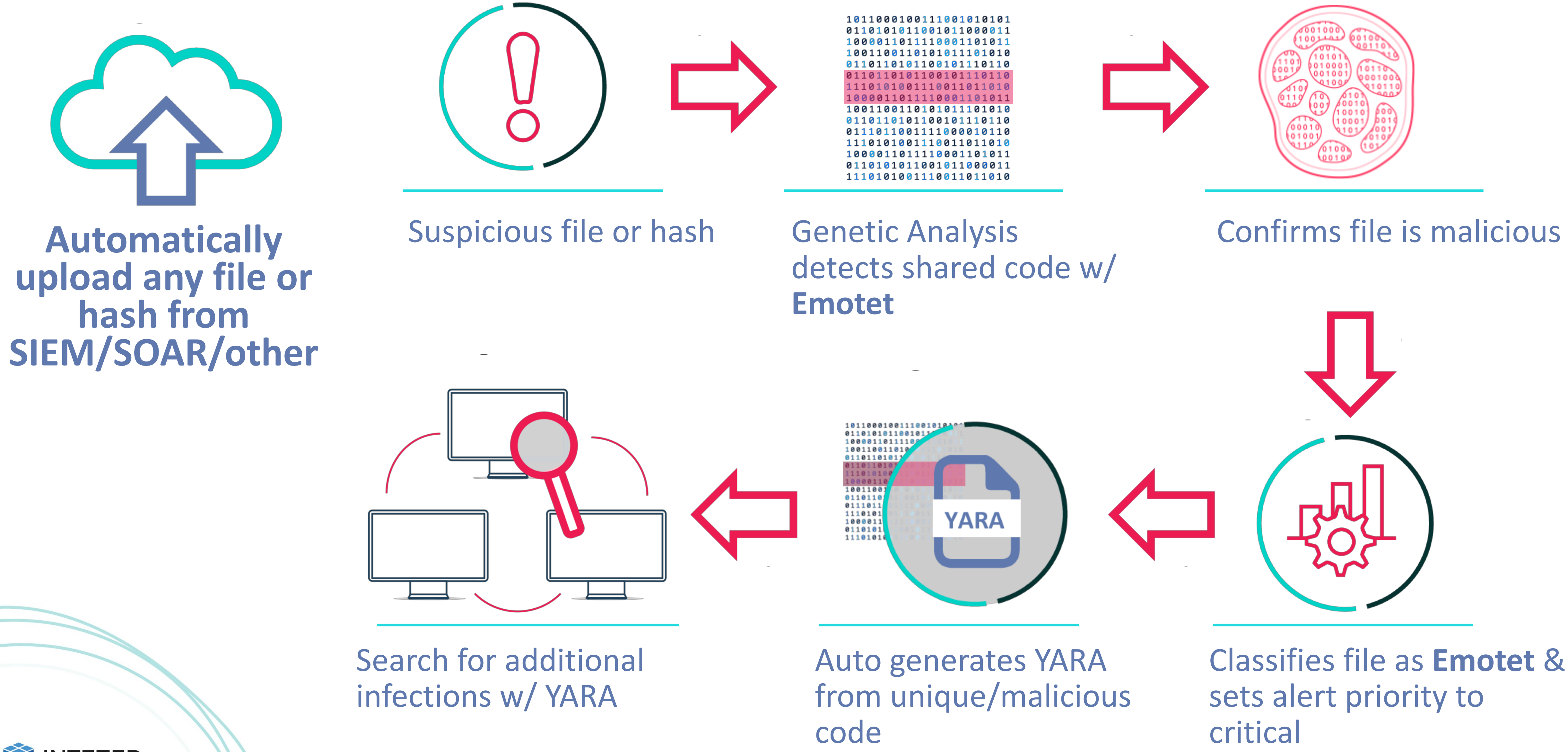
2) Self-propagation and password guessing

3) Modular malware

4) Steals banking details, reads emails, passwords and browser history

5) Packed with custom packer

Straw-by-Straw Analysis & Response



Automatically upload any file or hash from SIEM/SOAR/other

Suspicious file or hash

Genetic Analysis detects shared code w/ **Emotet**

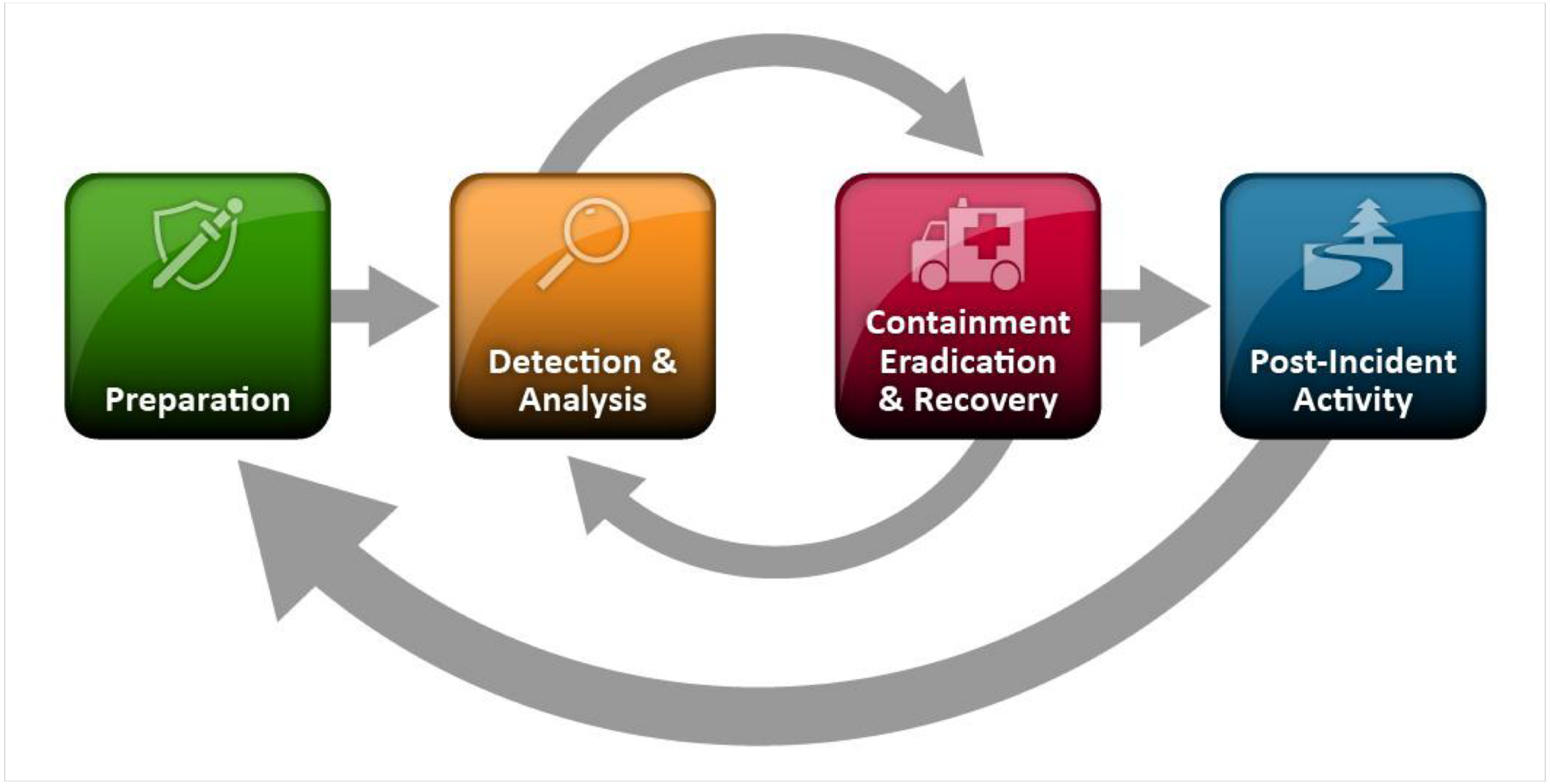
Confirms file is malicious

Classifies file as **Emotet** & sets alert priority to critical

Auto generates YARA from unique/malicious code

Search for additional infections w/ YARA

Improves Every Stage of IR Cycle



NIST "Computer Security Incident Handling Guide"

Summary

1) We should not compromise on investigating only a handful of alerts

2) We can use automated malware analysis solutions and implement integrations to achieve that

3) **Genetic Malware Analysis** is an effective way to automatically reverse engineer any suspicious file, at scale

Thank You!

You’re welcome to contact us:

programs@intezer.com

@IntezerLabs

INTEZER