VMRAY

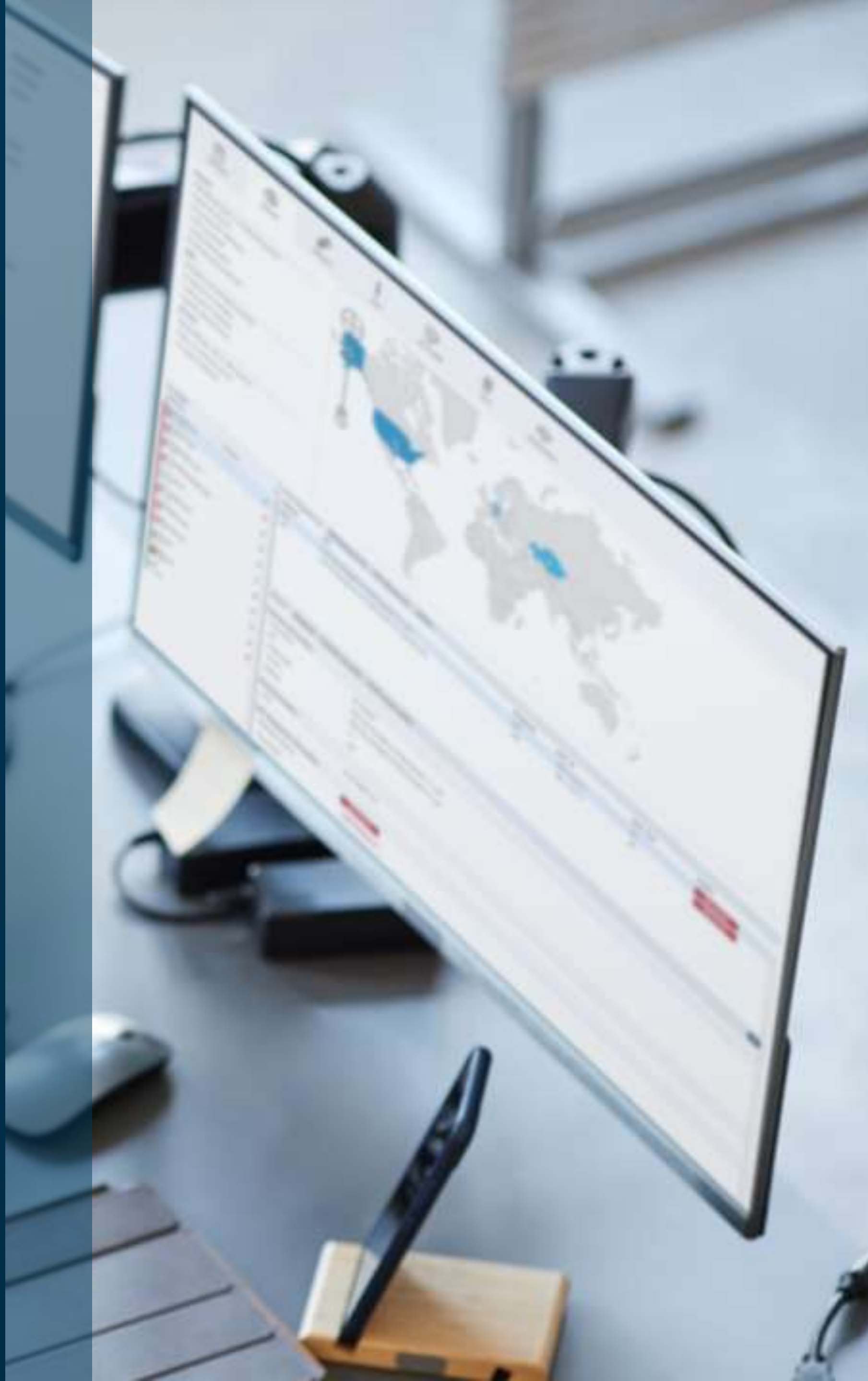
The right tool for the job:

Advanced Threat Analysis in the age of AI and Malware Evasion

Ertugrul Kara

Sr. Product Marketing Manager
VMRay

Tallinn, Estonia | ATEA Action 2024



Humans are good at using tools

as long as they solve a problem.

“We can be blind to the obvious,
and we are also blind to our blindness.”

Daniel Kahneman | Author of Thinking Fast and Slow
Nobel laurate in Economics

Problems of the industry

Cyber
poverty

Malware
& Threat Intelligence

Analyst
workload

VMRAY

Cyber poverty as a reality

70%

of organizations encountering human-operated ransomware had **fewer than 500 employees**

The Cyber Poverty Line

Unsettling questions:

1. Do our organization have the resources for adequate defense?
2. **What is the weight carried by SOC analysts?**

* https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Malware threat landscape

43%

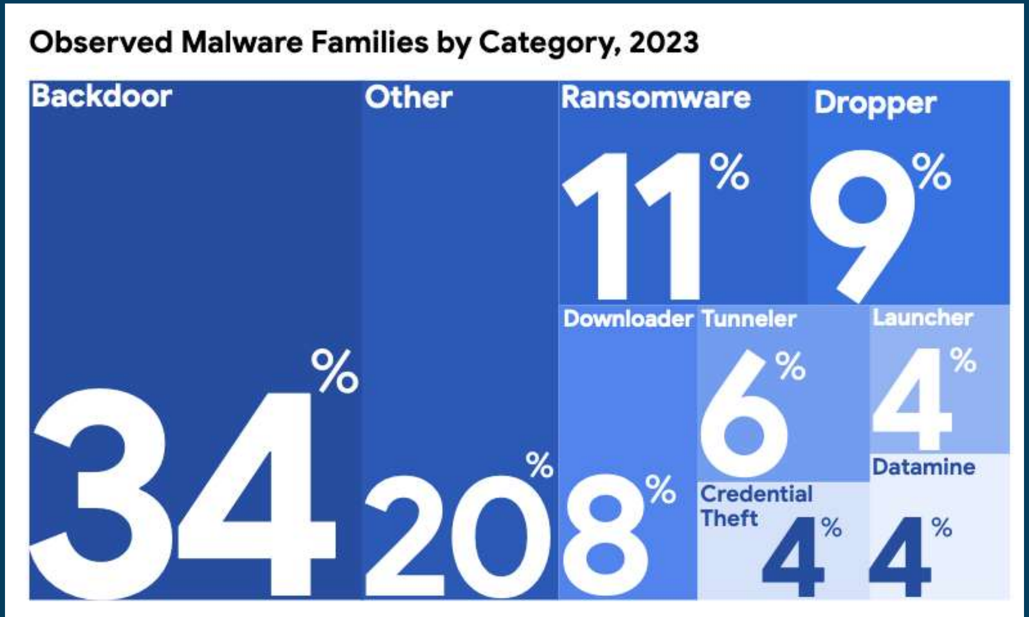
the most common action threat actors took on victim networks is **deployment of malware**

* IBM X-Force Incident Response Data

56%

of the investigated incidents **involved malware**

* Palo Alto Unit 42



Observed Malware Families by Category, 2023

* Mandiant M-Trends

Bumblebee | The story of a malware evolution

Active since 03/2022

Successor to BazarLoader

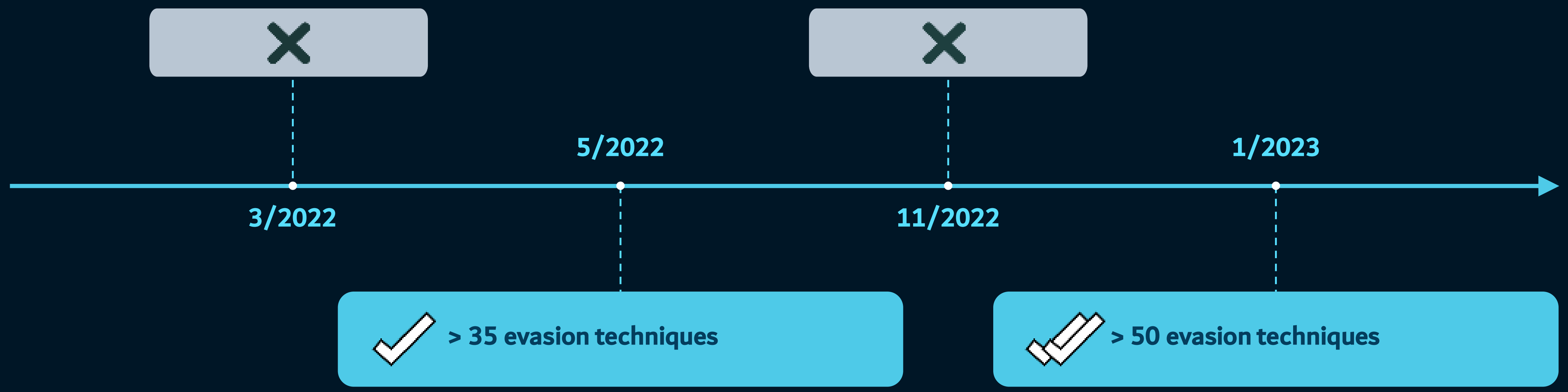
Acts as a loader for other malware

Unique and customized packer

Novel hooking method

Numerous evasion techniques

Bumblebee | Evasion effort in action



✗

3/2022

5/2022

✓ > 35 evasion techniques

✗

11/2022

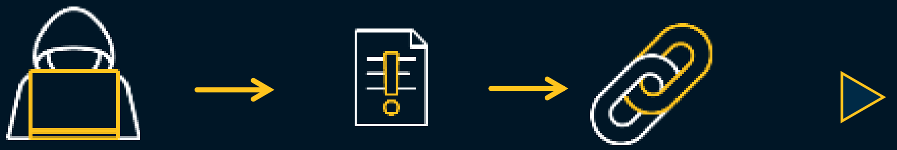
1/2023

✓✓ > 50 evasion techniques

Phishing | Legit-apps abused to push malware

Hiding in plain sight on GitHub CDN

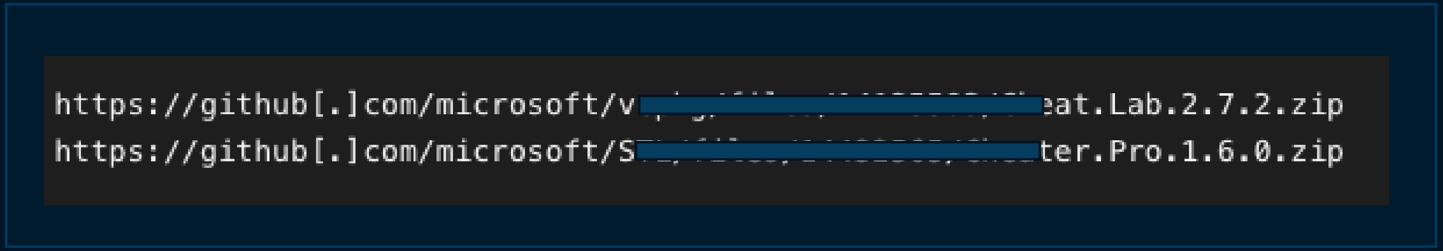
- Generated link for a file attachment
- Looking like it was published by Microsoft



Comment with a file attached

Legit-look URL to push **LUA Malware**

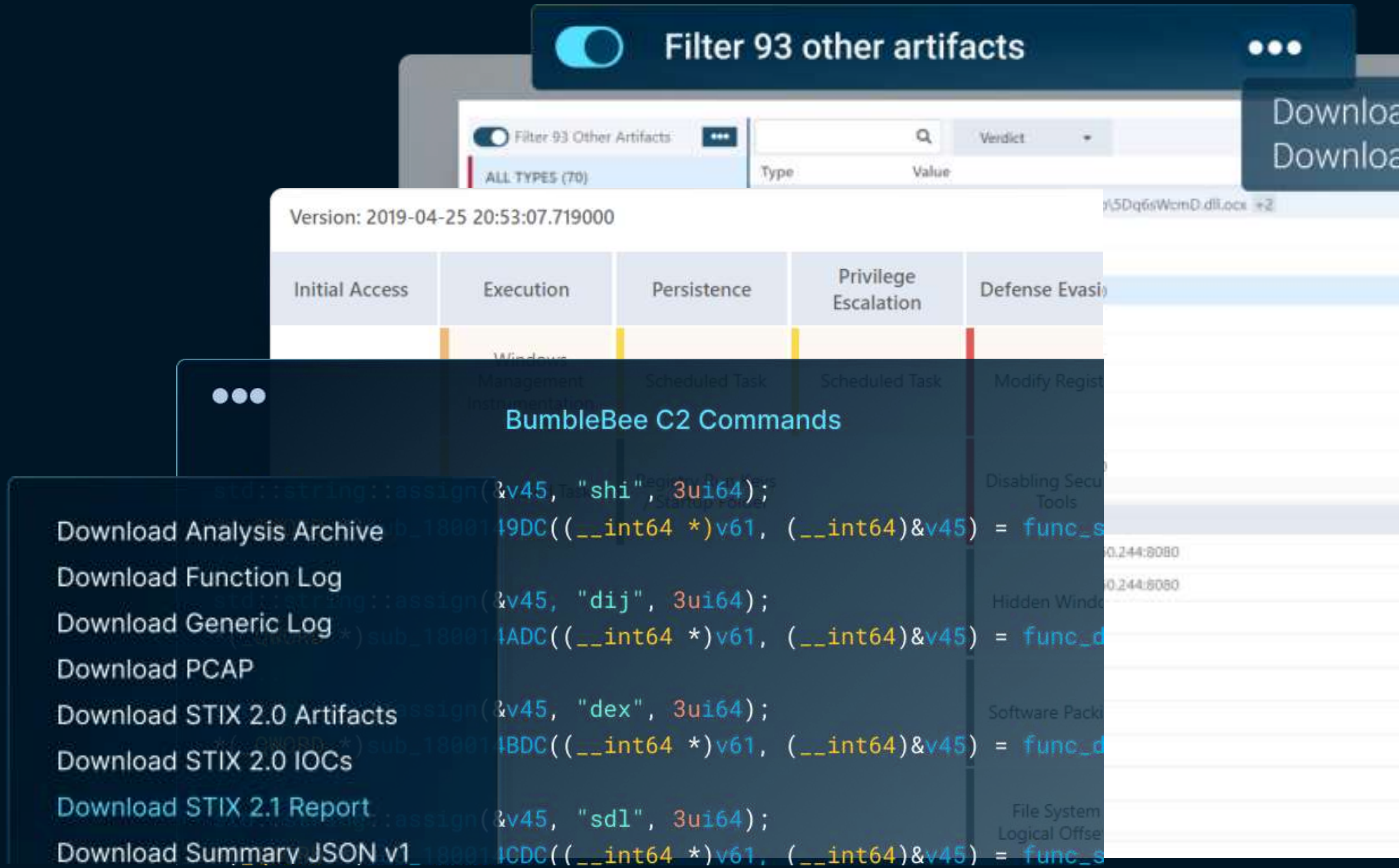
Bypassing Email Security Tools checking only URL reputation



```
https://github[.]com/microsoft/v[redacted]eat.Lab.2.7.2.zip
https://github[.]com/microsoft/S[redacted]ter.Pro.1.6.0.zip
```

How to keep up: malware analysis capability

CLARITY ENGINE
MACHINE LEARNING
SANDBOX
FOR MALWARE AND PHISHING
STATIC
ANALYSIS
REPUTATION
ANALYSIS



Version: 2019-04-25 20:53:07.719000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasi
	Windows Management Instrumentation	Scheduled Task	Scheduled Task	Modify Regist

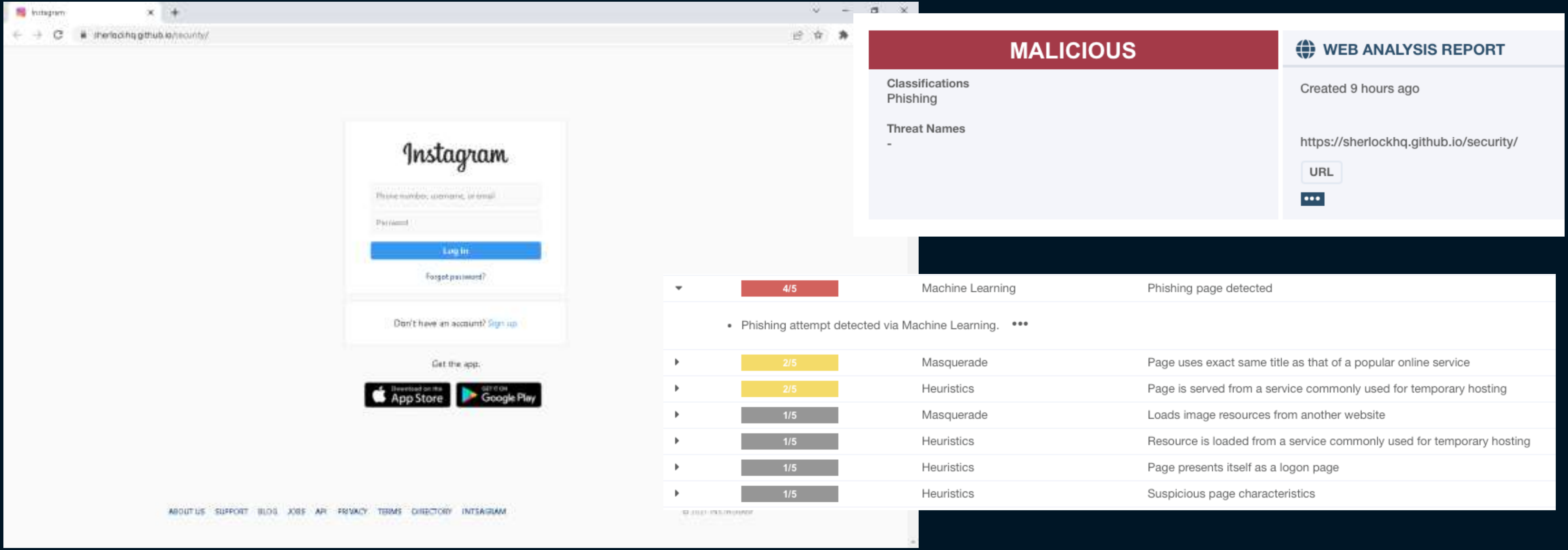
BumbleBee C2 Commands

```
&v45, "shi", 3ui64);
49DC((__int64 *)v61, (__int64)&v45) = func_s

&v45, "dij", 3ui64);
4ADC((__int64 *)v61, (__int64)&v45) = func_d

&v45, "dex", 3ui64);
4BDC((__int64 *)v61, (__int64)&v45) = func_d

&v45, "sdl", 3ui64);
4CDC((__int64 *)v61, (__int64)&v45) = func_s
```

- Download Analysis Archive
- Download Function Log
- Download Generic Log
- Download PCAP
- Download STIX 2.0 Artifacts
- Download STIX 2.0 IOCs
- Download STIX 2.1 Report
- Download Summary JSON v1

How to keep up: Machine Learning in action

sherlockhq[.]github[.]io


Instagram
sherlockhq.github.io/security/
Instagram
Phone number, username, or email
Password
Log In
Forgot password?
Don't have an account? Sign up
Get the app.
Download on the App Store
GET IT ON Google Play
ABOUT US SUPPORT BLOG JOBS API PRIVACY TERMS DIRECTORY INSTAGRAM

MALICIOUS

WEB ANALYSIS REPORT

Classifications
Phishing

Threat Names
-

Created 9 hours ago

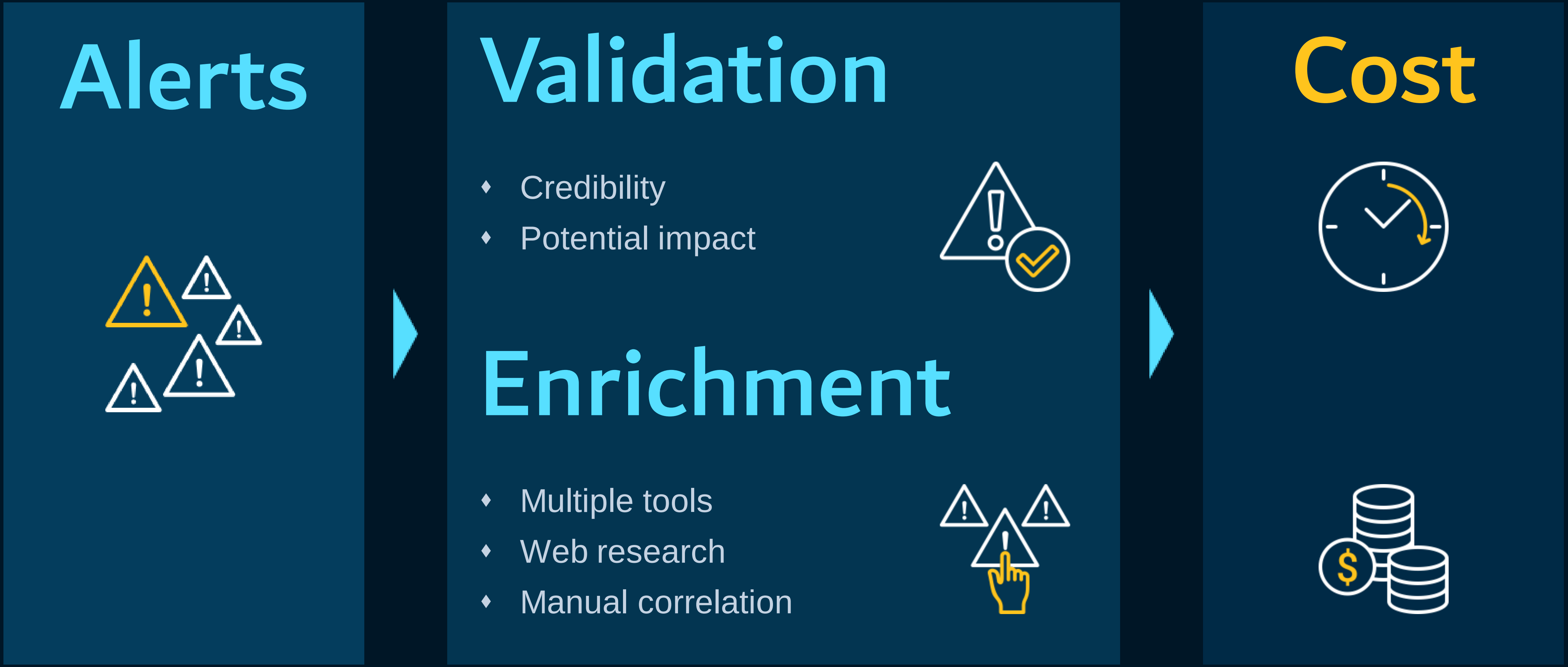
https://sherlockhq.github.io/security/

URL

4/5	Machine Learning	Phishing page detected
2/5	Masquerade	Page uses exact same title as that of a popular online service
2/5	Heuristics	Page is served from a service commonly used for temporary hosting
1/5	Masquerade	Loads image resources from another website
1/5	Heuristics	Resource is loaded from a service commonly used for temporary hosting
1/5	Heuristics	Page presents itself as a logon page
1/5	Heuristics	Suspicious page characteristics

- Phishing attempt detected via Machine Learning. •••

Inefficiencies of Alert Handling



Alerts

Validation

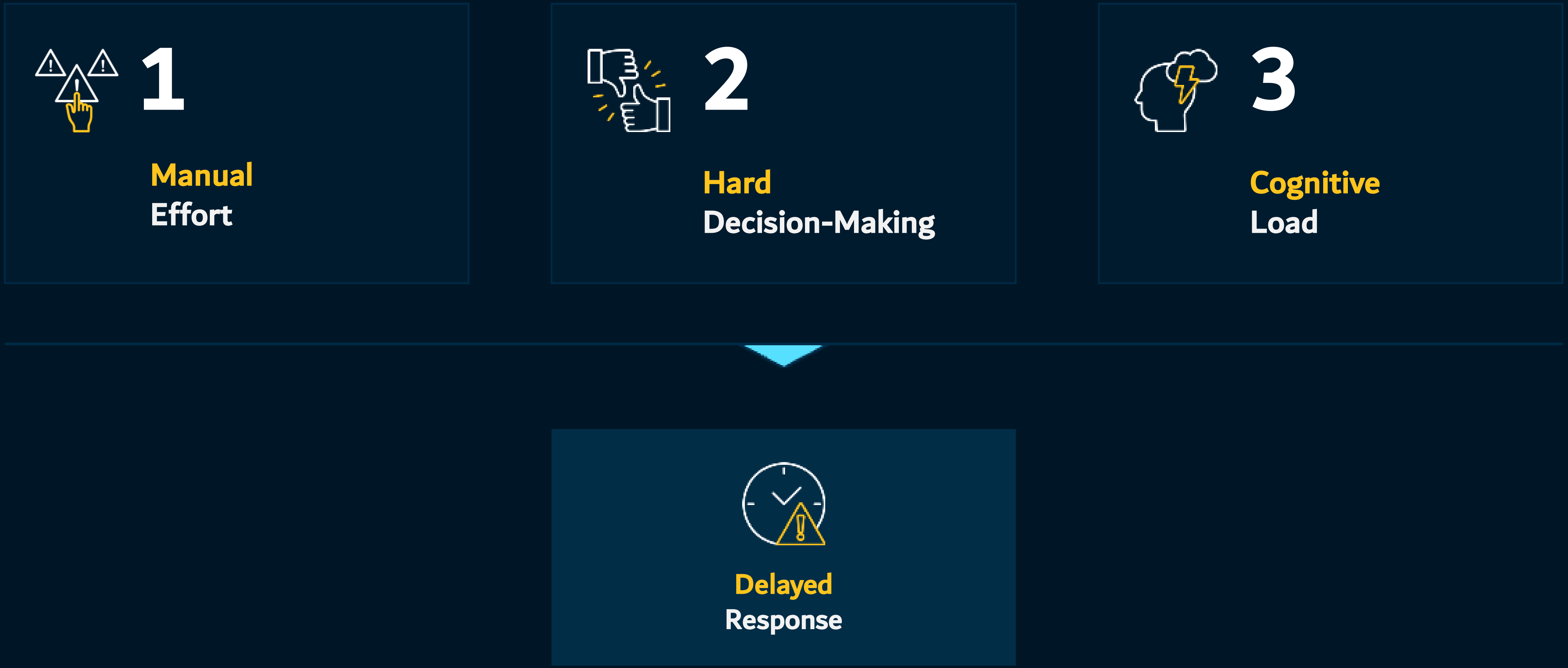
- Credibility
- Potential impact

Enrichment

- Multiple tools
- Web research
- Manual correlation

Cost

Analyst Experience



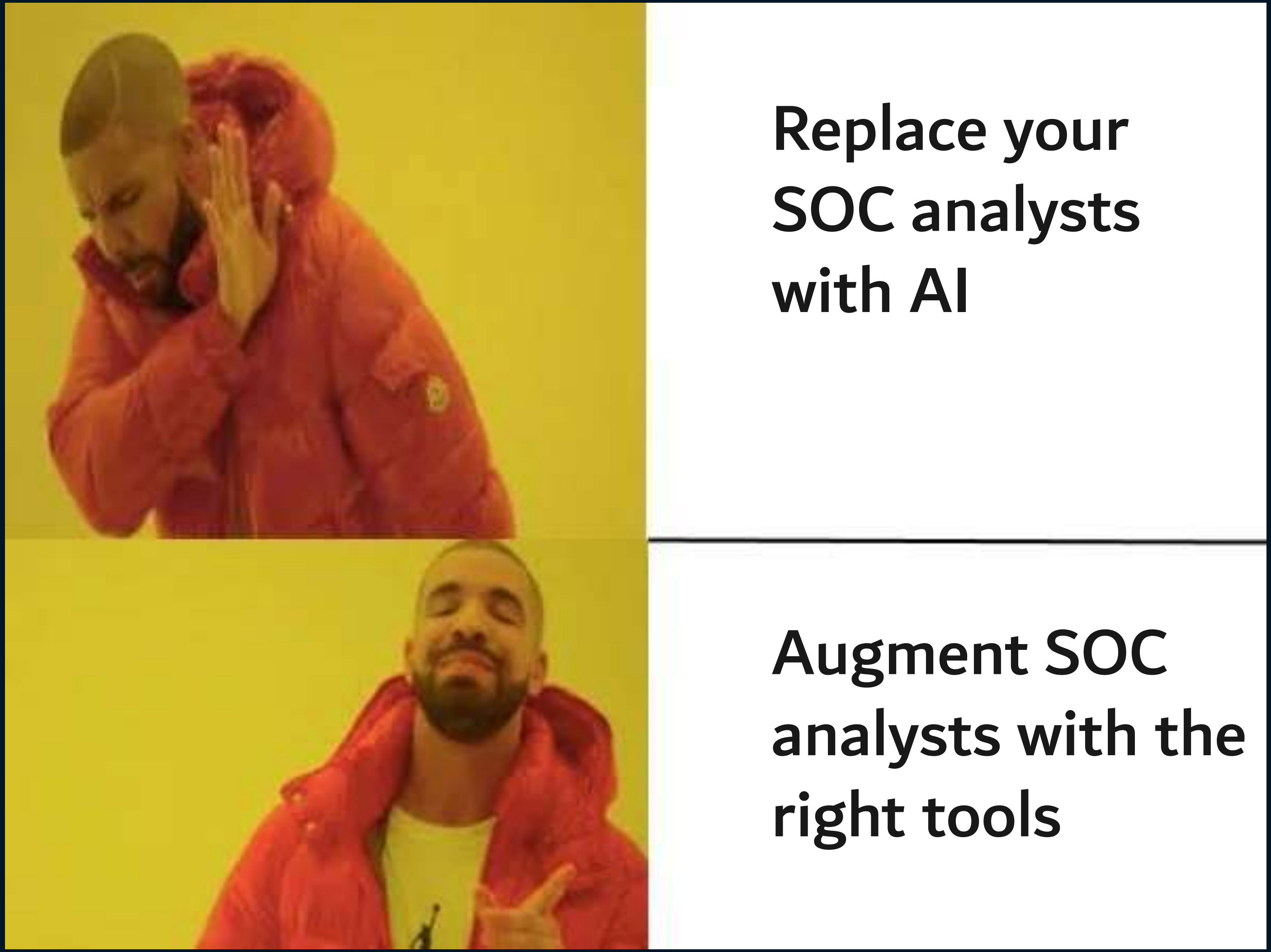
1 **Manual** Effort

2 **Hard** Decision-Making

3 **Cognitive** Load

Delayed Response

Solution perspective



Replace your SOC analysts with AI

Augment SOC analysts with the right tools

Malware analysts
Reverse engineers

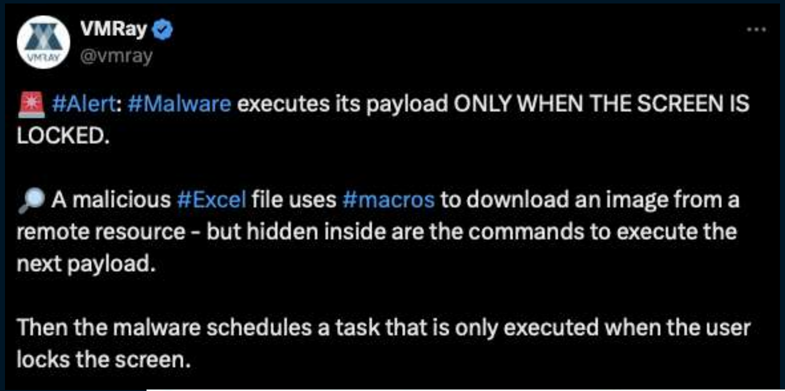
↓

Time-consuming analysis
Skills shortage

↓

Automated malware analysis

Anti-evasive automated sandbox vs AI

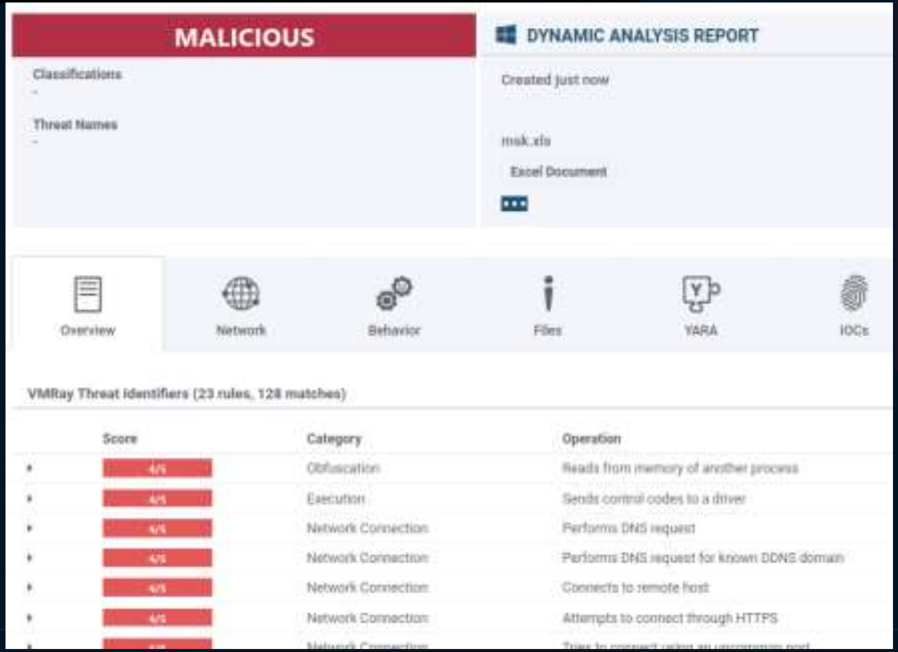


VMRay
@vmray

🚨 #Alert: #Malware executes its payload ONLY WHEN THE SCREEN IS LOCKED.

🔎 A malicious #Excel file uses #macros to download an image from a remote resource - but hidden inside are the commands to execute the next payload.

Then the malware schedules a task that is only executed when the user locks the screen.



MALICIOUS

Classifications
-

Threat Names
-

DYNAMIC ANALYSIS REPORT

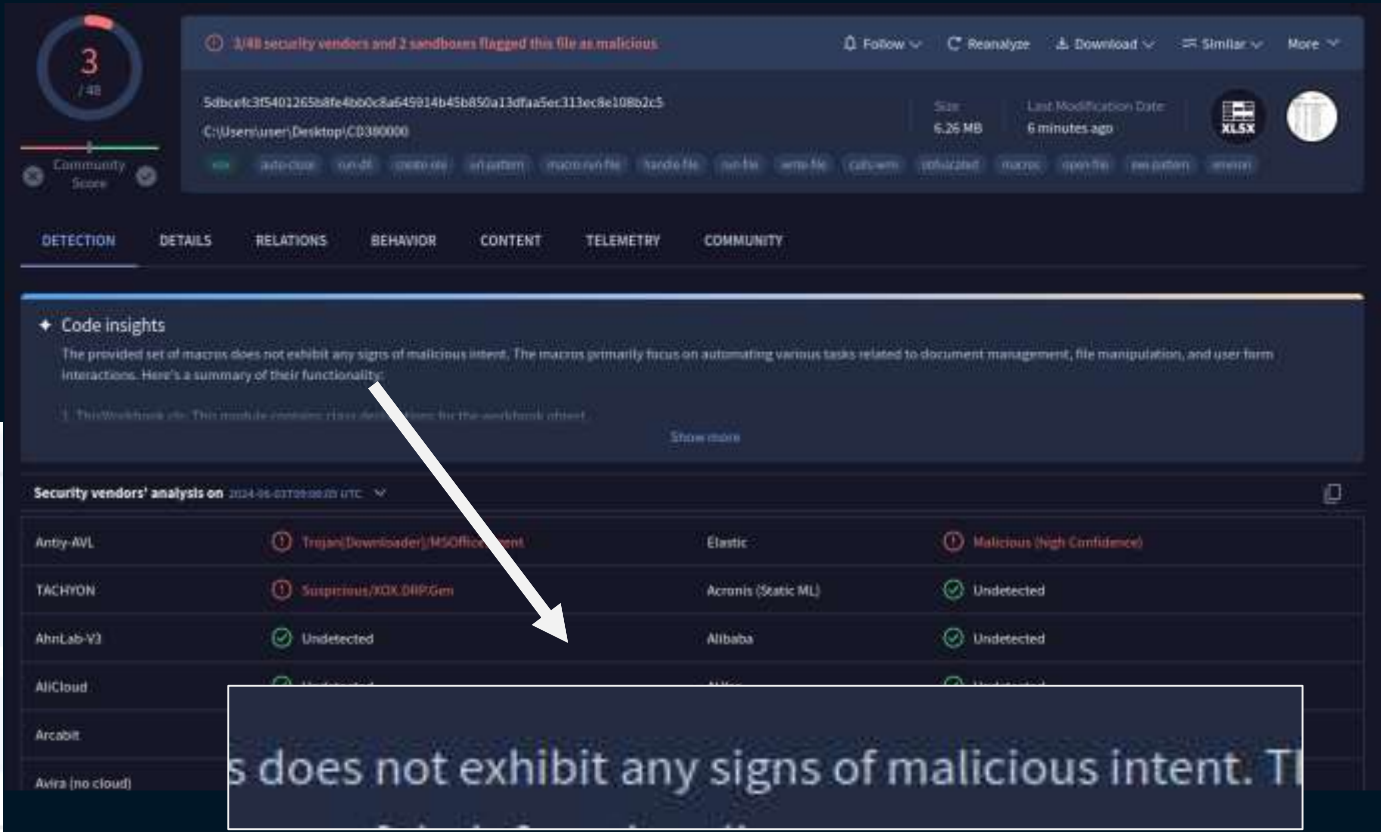
Created just now

msk.xls

Excel Document

VMRay Threat Identifiers (23 rules, 128 matches)

Score	Category	Operation
4/5	Obfuscation	Reads from memory of another process
4/5	Execution	Sends control codes to a driver
4/5	Network Connection	Performs DNS request
4/5	Network Connection	Performs DNS request for known DDNS domain
4/5	Network Connection	Connects to remote host
4/5	Network Connection	Attempts to connect through HTTPS
4/5	Network Connection	Tries to connect using an uncommon port



3 / 48

Community Score

3/48 security vendors and 2 sandboxes flagged this file as malicious

5dbcefc3f5401265b8fe4bb0c8a645914b45b850a13dfaa5ec313ec8e108b2c5
C:\Users\user\Desktop\C0380000

Size
6.26 MB

Last Modification Date
6 minutes ago

✦ Code insights

The provided set of macros does not exhibit any signs of malicious intent. The macros primarily focus on automating various tasks related to document management, file manipulation, and user form interactions. Here's a summary of their functionality:

1. ThisWorkbook.cls: This module contains class declarations for the workbook object.

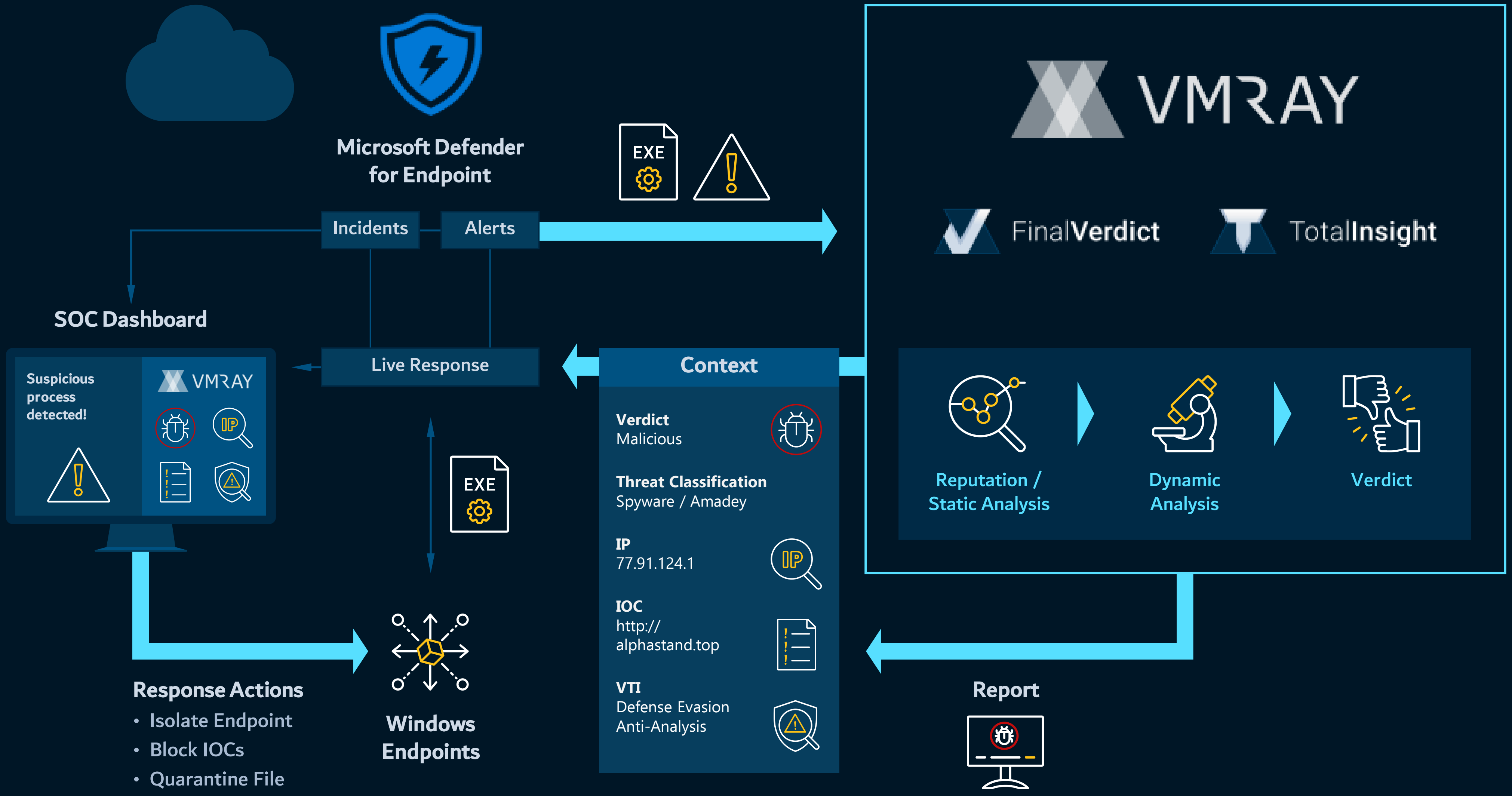
Show more

Security vendors' analysis on 2024-06-03T09:00:05 UTC

Antiy-AVL	ⓘ Trojan[Downloader]/MSOffice.Agent	Elastic	ⓘ Malicious (high Confidence)
TACHYON	ⓘ Suspicious/XOX.DRP.Gen	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
AliCloud	✓ Undetected	ALYac	✓ Undetected
Arcabit			
Avira (no cloud)			

s does not exhibit any signs of malicious intent. Th

Advanced Threat Analysis + SOC Tools



Context

Verdict
Malicious

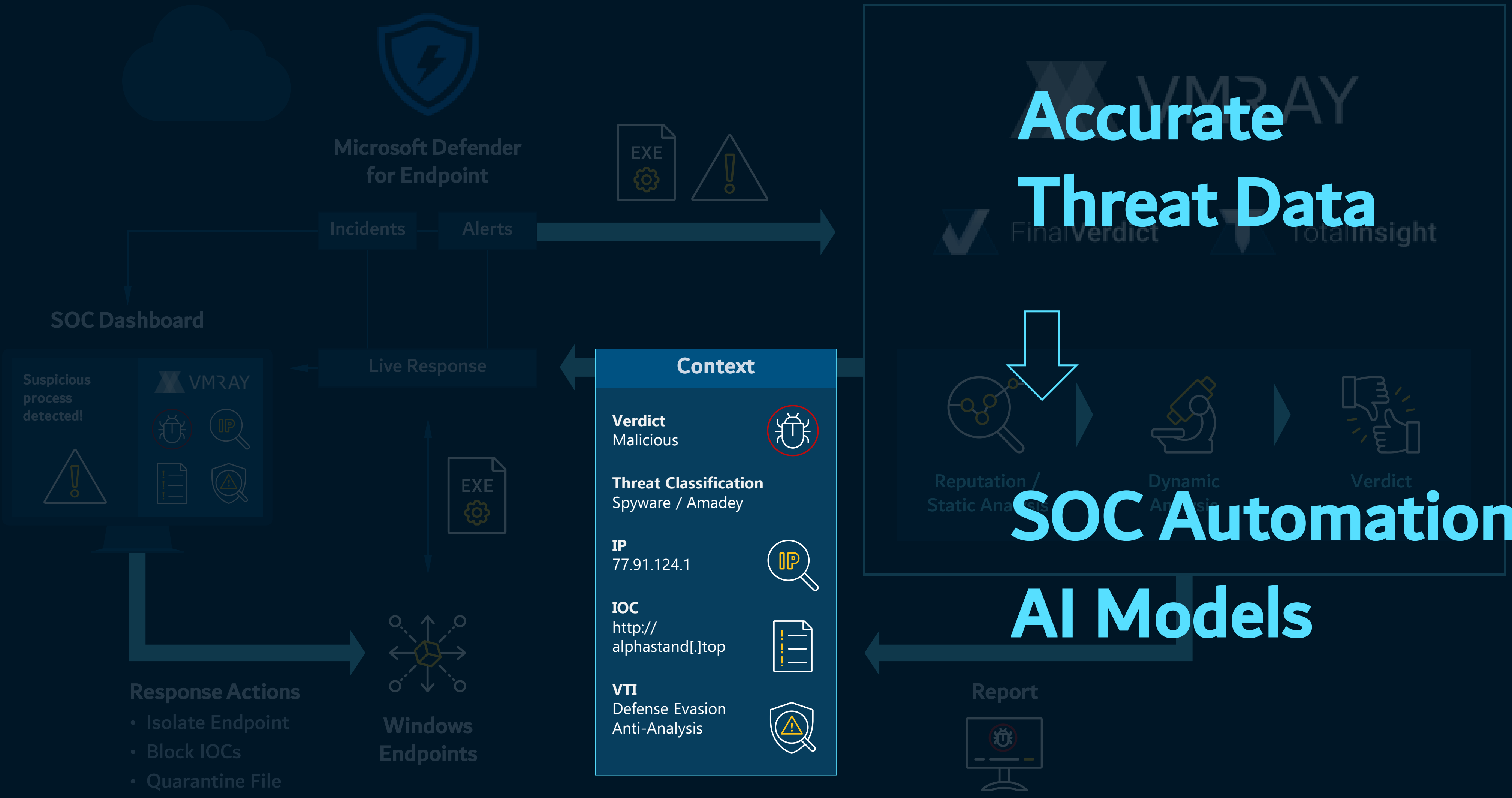
Threat Classification
Spyware / Amadey

IP
77.91.124.1

IOC
http://
alphastand.top

VTI
Defense Evasion
Anti-Analysis

Advanced Threat Analysis + SOC Tools



Context

Verdict
Malicious

Threat Classification
Spyware / Amadey

IP
77.91.124.1

IOC
http://alphastand[.]top

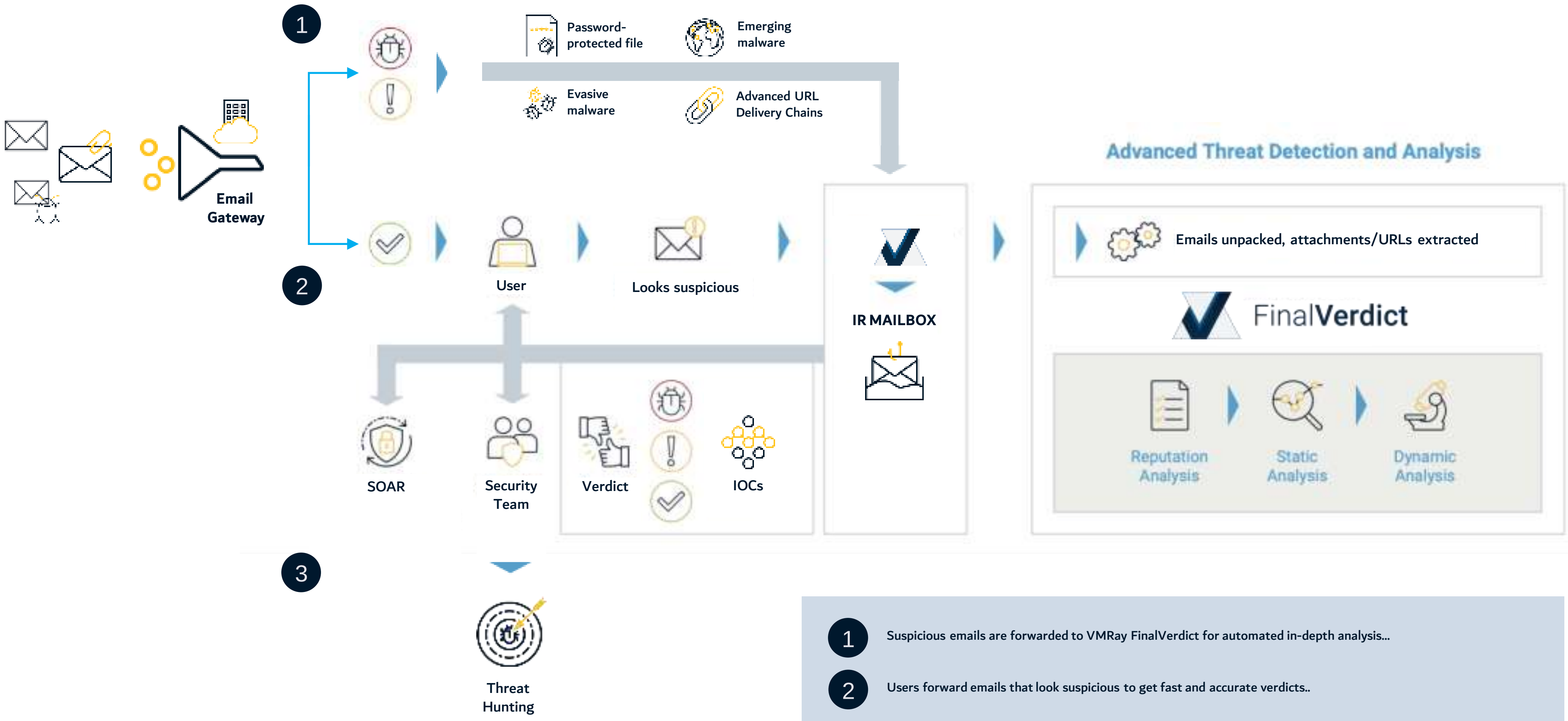
VTI
Defense Evasion
Anti-Analysis

Accurate Threat Data

SOC Automation

AI Models

Advanced Threat Analysis + Email Security



1 Suspicious emails are forwarded to VMRay FinalVerdict for automated in-depth analysis...

2 Users forward emails that look suspicious to get fast and accurate verdicts..

3 IOCs and TTPs extracted from malicious samples are used for effective threat hunting via integrations with SIEM/SOAR and EDR tools.

Key Takeaways

1. Evolving threats demand **advanced analysis**

2. Data quality and accuracy is critical both for **automation and AI**

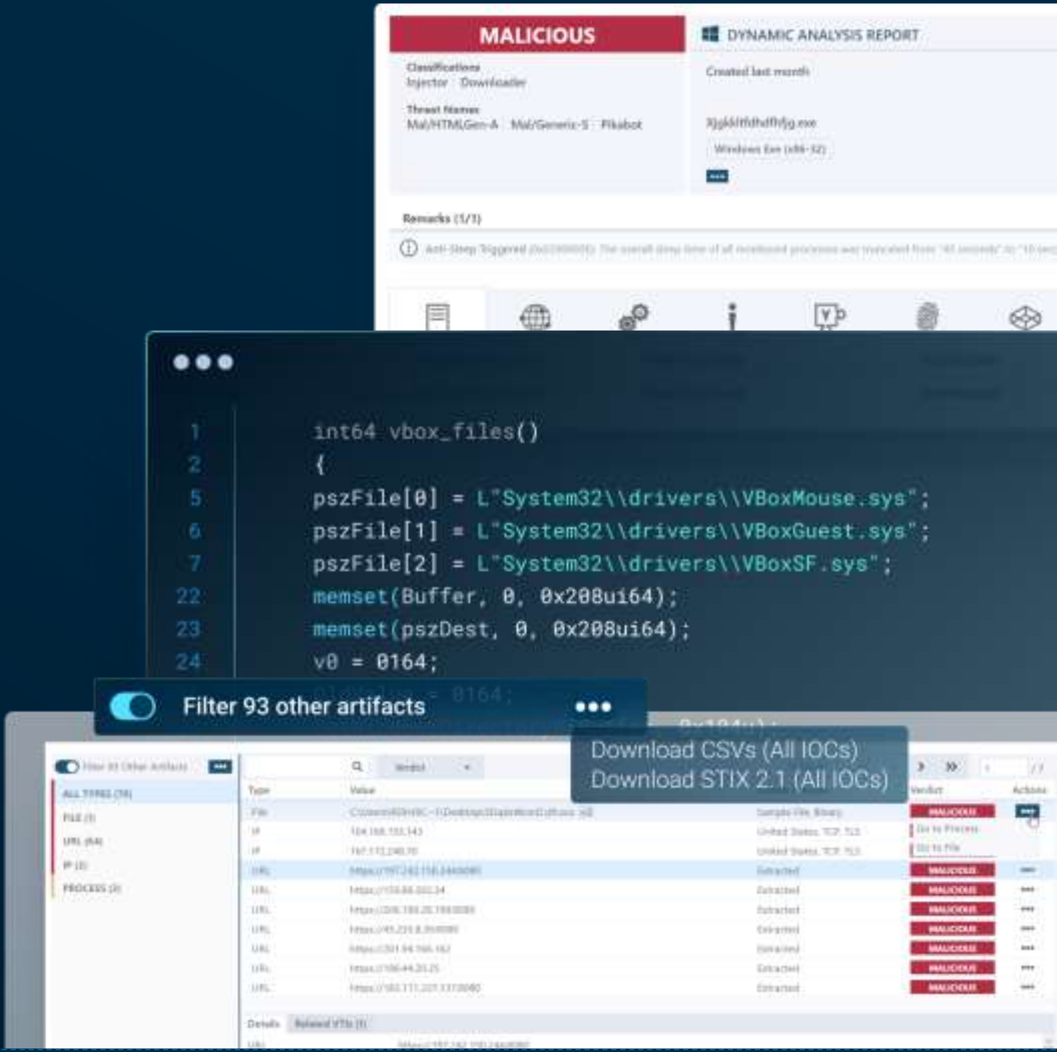
3. AI complements, **not replaces, human expertise**

Thank You.

Free for Community

For millions of **malware sandboxing** reports, check out our community portal: threatfeed.vmray.com

Appendix.



MALICIOUS

DYNAMIC ANALYSIS REPORT

Classifications
Injector Downloader

Threat Names
Mal/HTMLGen-A Mal/Generic-S Pikabot

Created last month

Xjgkklfhfdhdfhfjg.exe

Windows Exe (x86-32)

Remarks (1/1)

Anti-Sleep Triggered [illegible]

```
int64 vbox_files()
{
pszFile[0] = L"System32\\drivers\\VBoxMouse.sys";
pszFile[1] = L"System32\\drivers\\VBoxGuest.sys";
pszFile[2] = L"System32\\drivers\\VBoxSF.sys";
memset(Buffer, 0, 0x208ui64);
memset(pszDest, 0, 0x208ui64);
v0 = 0164;
```

Filter 93 other artifacts

Download CSVs (All IOCs)
Download STIX 2.1 (All IOCs)

Type	Value		Verdict	Actions
File	[illegible]	Sample File, Binary	MALICIOUS	•••
IP	104.168.155.143	United States, TCP, TLS		
IP	167.172.248.70	United States, TCP, TLS		
URL	[illegible]	Extracted	MALICIOUS	•••
URL	[illegible]	Extracted	MALICIOUS	•••
URL	[illegible]	Extracted	MALICIOUS	•••
URL	[illegible]	Extracted	MALICIOUS	•••
URL	[illegible]	Extracted	MALICIOUS	•••
URL	[illegible]	Extracted	MALICIOUS	•••
URL	[illegible]	Extracted	MALICIOUS	•••

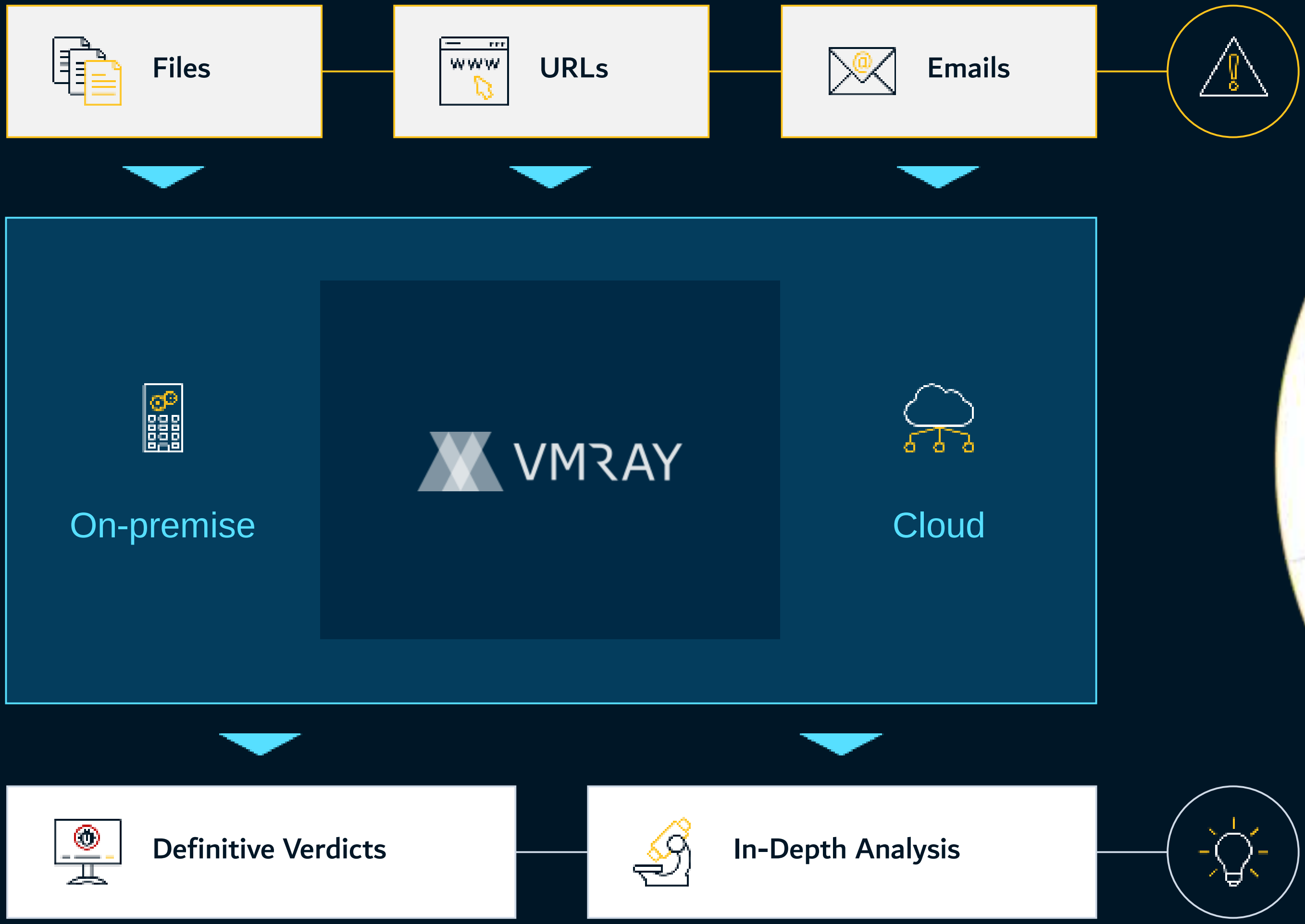
17
Fortune 100
Largest companies

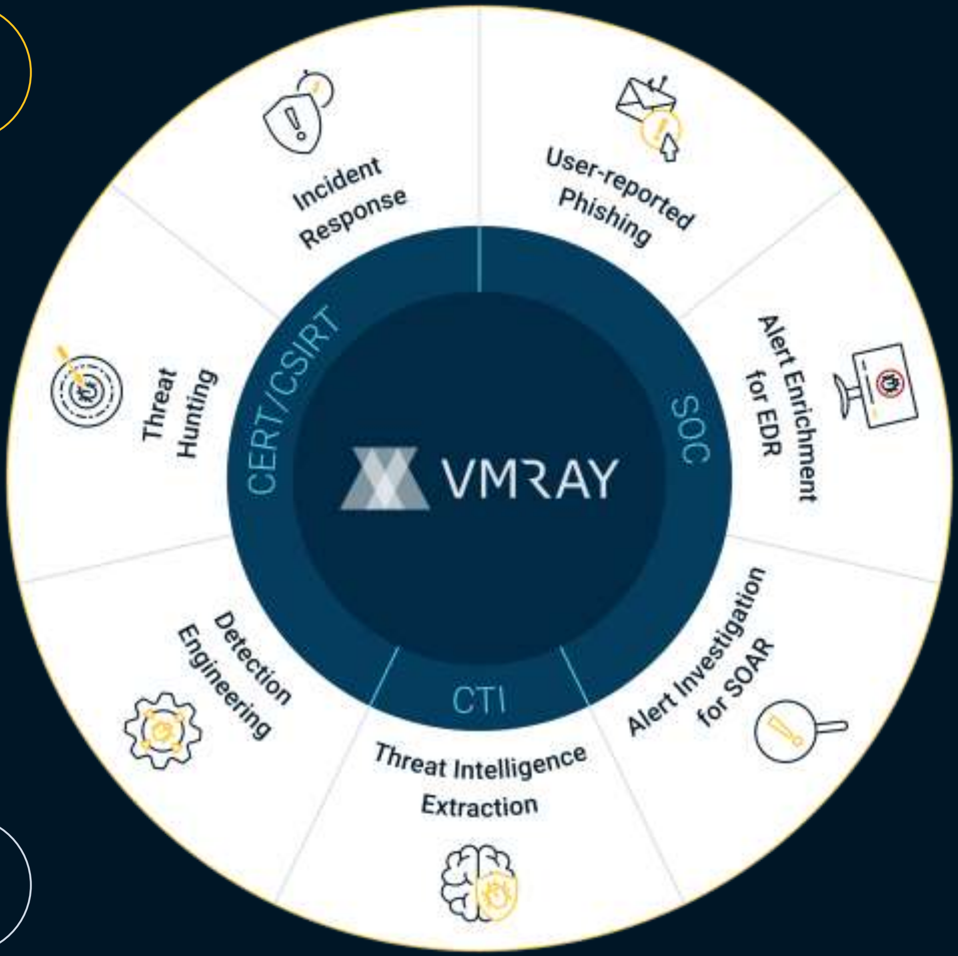
4 of 5
Top Tech Giants
of the world

82
Leading Banks
& Financial organizations

74
Government
organizations

Empower security teams **with the best-of-breed**





3 ways we lead innovation in advanced threat detection

Uncover the threats of today & tomorrow

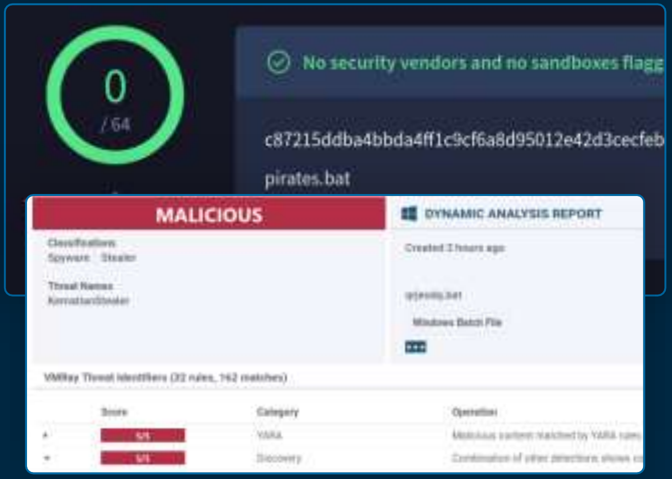
Aimed at detecting
unknown, targeted & evasive threats

Turn complexity into clarity

30+ technologies to improve analysis &
generate clear insights

Expand to new use cases

Automate security tasks with
speed & scale



0 / 64

No security vendors and no sandboxes flagg

c87215ddba4bbda4ff1c9cf6a8d95012e42d3cecfeb

pirates.bat

MALICIOUS

DYNAMIC ANALYSIS REPORT

Classifications
Spyware Stealer

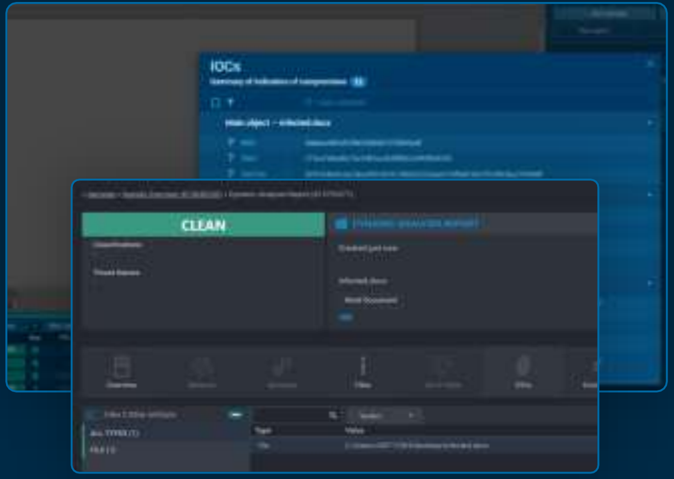
Threat Names

Created 3 hours ago

Windows Batch File

VMRay Threat Identifiers (32 rules, 162 matches)

Score	Category	Operation
5/5	YARA	Malicious content matched by YARA rules
5/5	Discovery	Combination of other detections shows



IOCs

CLEAN

5 Reasons why VMRay is different

VMRAY

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2024

Uncover the threats of today & tomorrow

- Best-in-class detection against **unknown, targeted, & evasive threats**

In-depth & complete visibility

- **Evasion-resistant analysis**
- Human & system activity simulation

Noise-free results

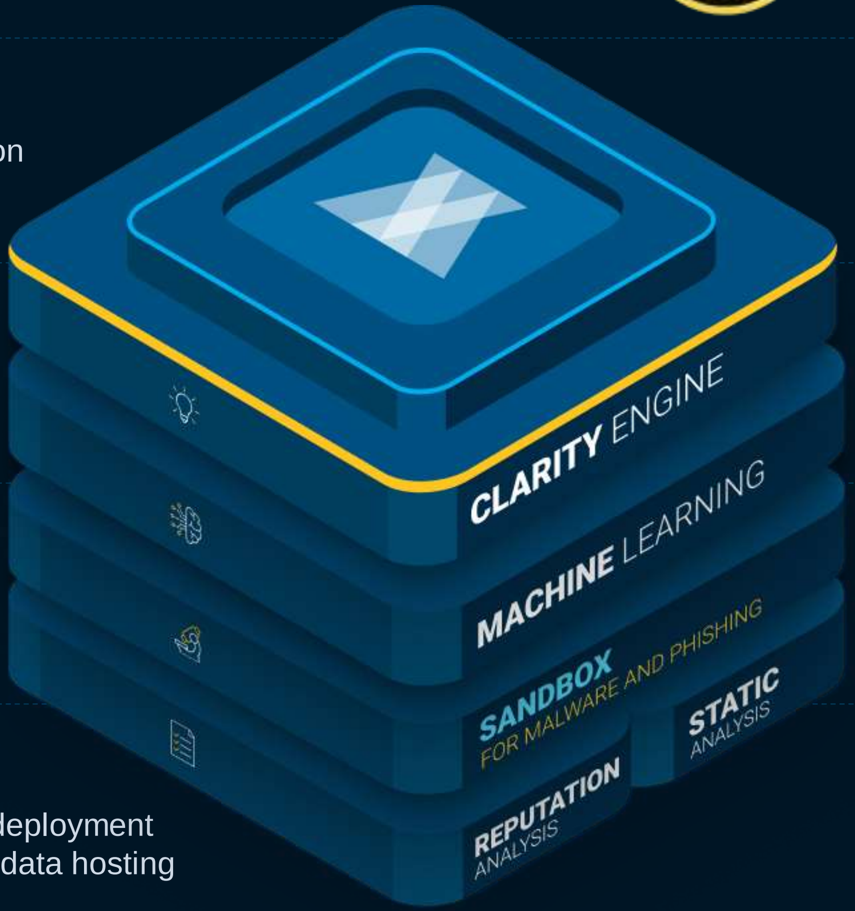
- Clear reports & reliable IOCs
- Upskilling security teams
- **Curate your own Threat Intel**

Automation at large scale

- Multi-use
- Integrate with other tools
- **Improve SOC efficiency**

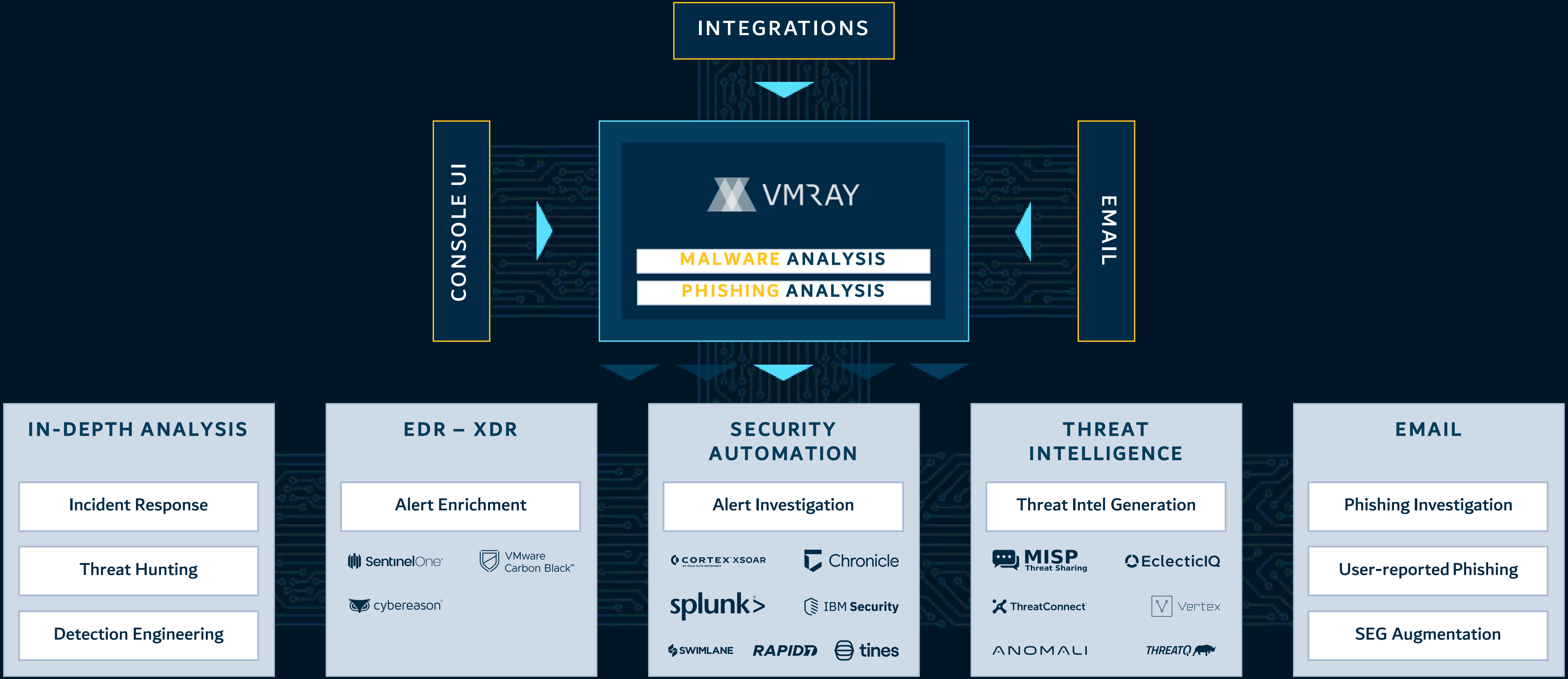
Privacy for enterprises & governments

- **Your data is only yours**
- Cloud, private cloud, on-premise deployment
- Choose the duration & location of data hosting



The Washington Post Forbes The Verge Technology Record

Supporting security teams at every stage of SOC maturity



INTEGRATIONS

CONSOLE UI

VMRAY

MALWARE ANALYSIS

PHISHING ANALYSIS

EMAIL

IN-DEPTH ANALYSIS

- Incident Response
- Threat Hunting
- Detection Engineering

EDR – XDR

- Alert Enrichment

SentinelOne · VMware Carbon Black · cybereason

SECURITY AUTOMATION

- Alert Investigation

CORTEX XSOAR · Chronicle · splunk> · IBM Security · SWIMLANE · RAPID7 · tines

THREAT INTELLIGENCE

- Threat Intel Generation

MISP Threat Sharing · EclecticIQ · ThreatConnect · Vertex · ANOMALI · THREATQ

EMAIL

- Phishing Investigation
- User-reported Phishing
- SEG Augmentation