Acronis

Acronis Partner Day at MSP Global 2024

Time to **Go Native.**

Acronis

Actionable threat intelligence for the MSP community

#CyberFit

Vicente Diaz

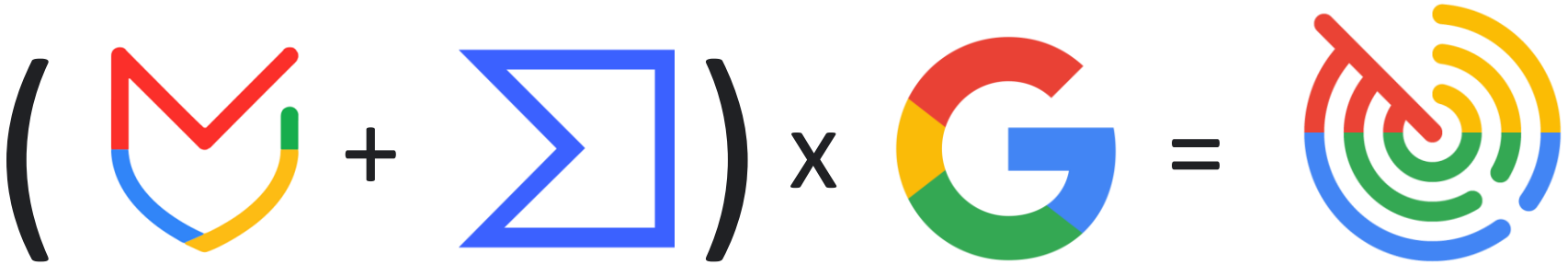
Security Engineer, Google Threat Intelligence Strategist, VirusTotal

Actionable Threat Intelligence for the MSSP Community

Cutting Through the Noise to Protect Your Clients

Google Threat Intelligence

Combining respected security brands into a transformational new offering



Google Threat Intelligence

Combine frontline, curated, open source, and crowdsourced intelligence

Frontline expertise

Research, analysis, threat actors, TTPs, and reporting

Crowdsourced intelligence

Verdicts, OSINT, crowdsourced rules, community

Threat insights

Security scanning devices, URLs, and files

AI-infused threat intelligence: risk profiling; digested threat intel; AI-assisted malware analysis

Unmatched visibility into threats

Far reaching **breadth** and detailed **depth**

50B+ files
Across thousands of file formats for all operating systems

1.5B+
Sandbox reports

2M
Analyses per day

232
ISO COUNTRIES submitting files

3M+
MONTHLY USERS sourcing data

6B+ URLs
6M+ URL analyses per day

5B+
Domains

170B+
pDNS
Resolutions

45/71

70+ Antivirus
90+ URL blocklists
20+ Sandboxes
30+ Crowdsourced {YARA, SIGMA, IDS} repos
100K+ Crowdsourced rules

1000+
Total employees supporting IR

300+
Incident response consultants

500+
Researchers & analysts

30+
languages spoken

1100+
Investigations per year

350+
Tracked threat groups

400k
Incident investigation hours in 2023

53+
Countries with incident response engagements

4 Billion
Google Safe Browsing user devices protected each day from malware and social engineering

1.5 Billion
Active Gmail users protected against phishing, malware, and spam through embedded security monitoring

Evolving attacks

Malwareless attacks

Cloud infrastructure

The death of IOCs

Evolving defenses

Data lake / SIEM

Anomaly / pattern detection

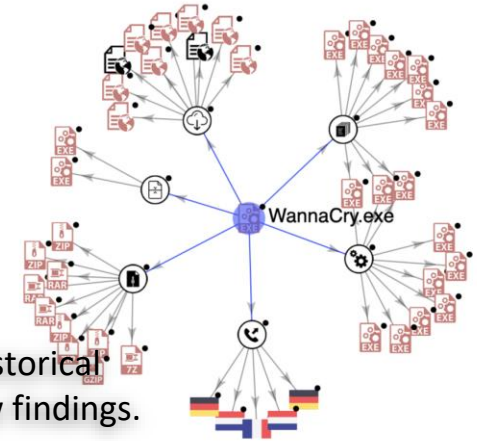
Customized intelligence

```
rule CEO_Fraud
{
    meta:
        author = "Natalie"
        date = "11/06/2018"
        description = "This is a basic YARA rule for CEO fraud."

    strings:
        $text_a = "wire transfer"
        $text_b = "CEO"
        $hex = { E2 34 A1 C8 23 FB }

    condition:
        $text_a or $text_b or $hex
}
```

Malicious or not?

Lack of resources and maturity

Day 1. New attack, AV heuristic detection. Industry knows nothing about it, no context.

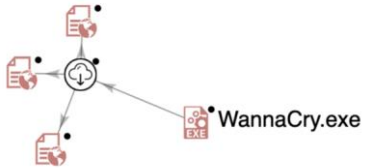


Day 30. Org re-checks historical events, learns about new findings. Suboptimal.

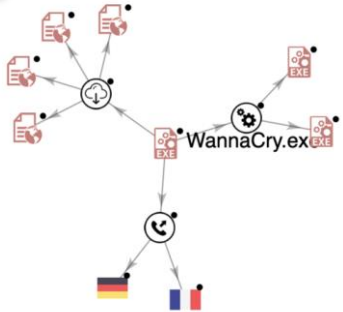
THREAT CAMPAIGN EXPOSURE WINDOW (BLINDSPOT)

time

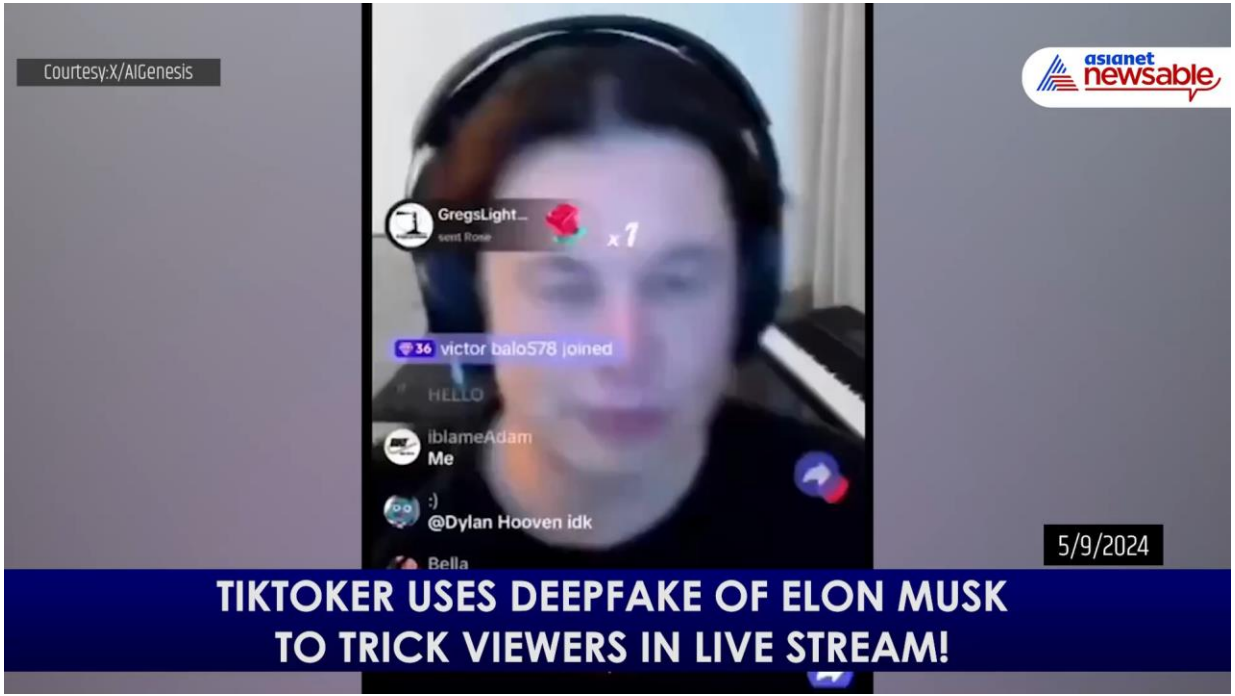
Day 3. New observations in terms of download URLs.



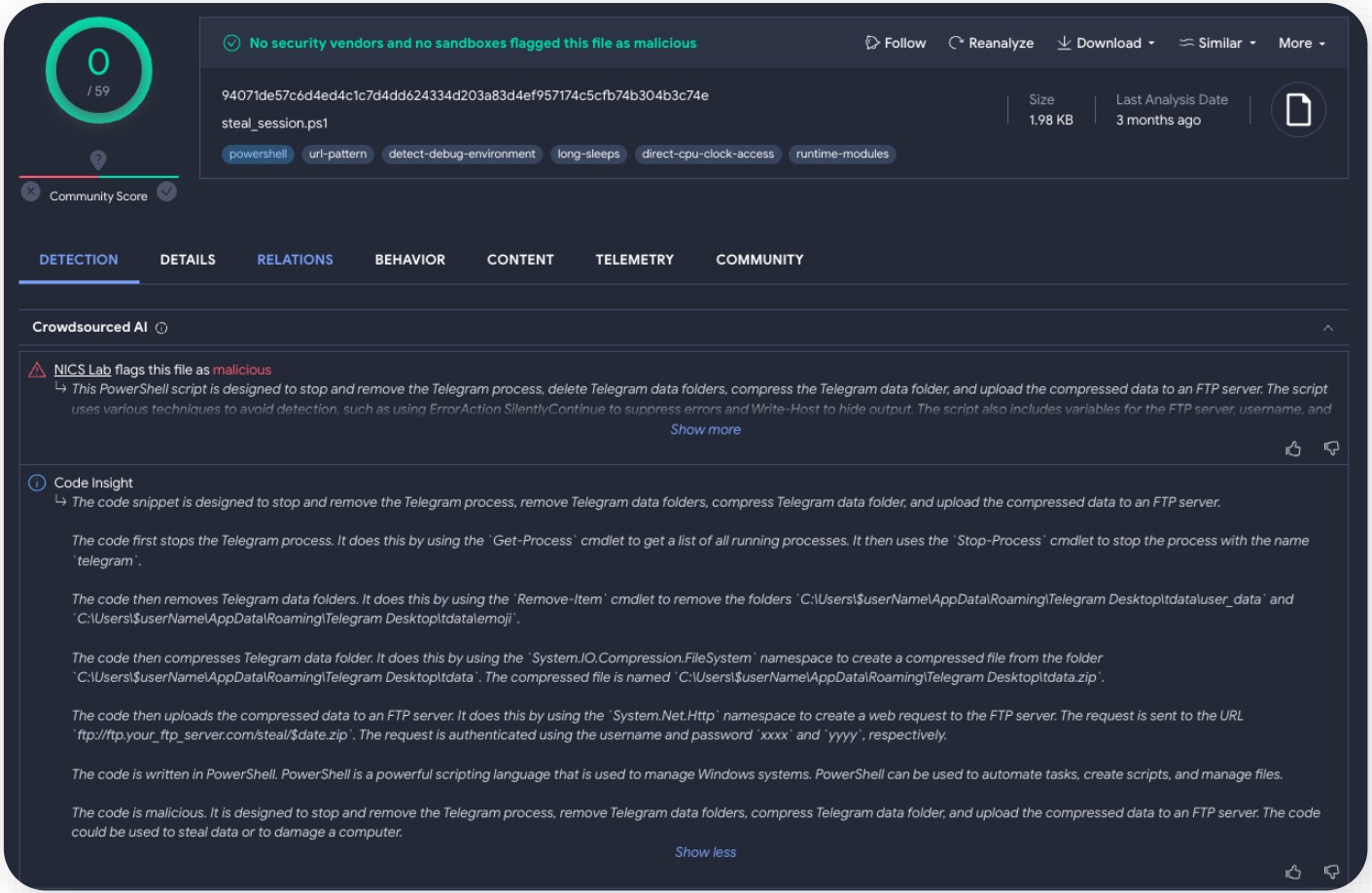
Day 7. Execution parents (droppers) and network comms.



The role of AI (I)



The role of AI (II)



An unique opportunity

Summarization / customization capabilities

Auto Hunting / Monitoring

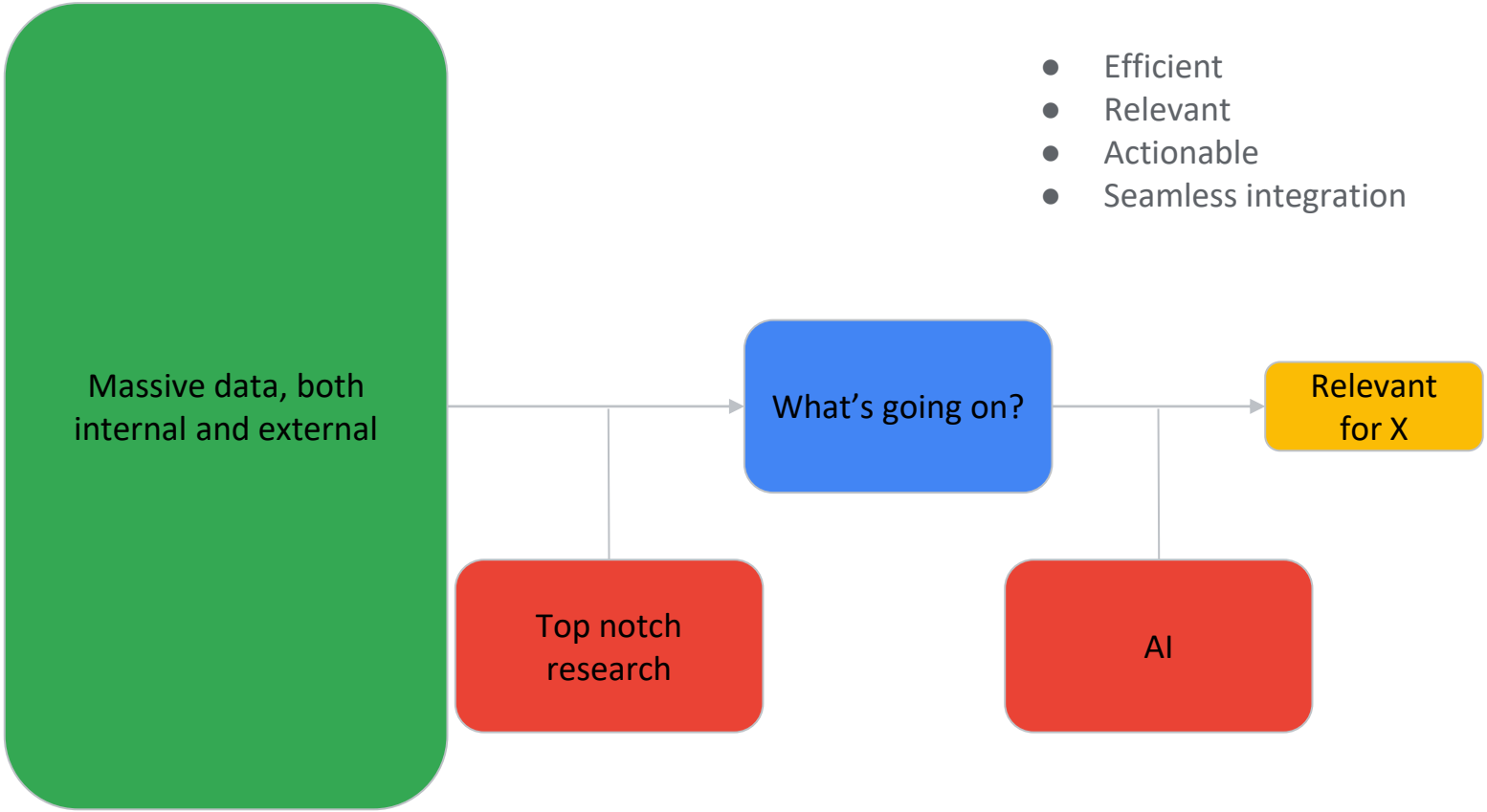
Auto triage with full context

Massive data ingestion

Multiple deliverables

The recipe for success

- Efficient
- Relevant
- Actionable
- Seamless integration



Conclusions

TI data without context is just noise

Actionable TI goes way beyond data

Context - absolutely essential

Customization and efficiency

Integration

The relevance of research - Timely, relevant, proactive

Google Cloud

Thank You

Acronis

Acronis Partner Day at MSP Global 2024

Time to **Go Native.**

Thank you, Ecosystem partners!

MSPGLOBAL | in association with Acronis

Join us in 2025!

Acronis Partner Day at MSP Global

October 20-21 | PortAventura, Spain

Register today:

go.acronis.com/MSPGlobal2025