



**Acronis**

# **Acronis Partner Day at MSP Global 2024**

**Time to Go Native.**

Acronis

# Actionable threat intelligence for the MSP community

#CyberFit



**Vicente Diaz**

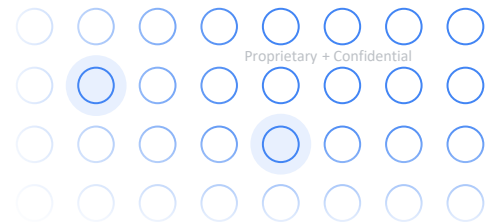
Security Engineer, Google  
Threat Intelligence Strategist,  
VirusTotal

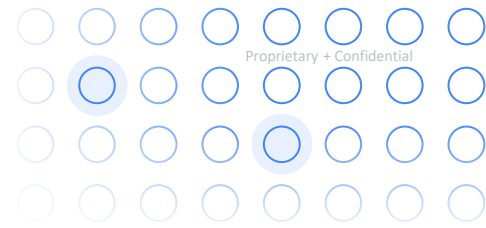
# Actionable Threat Intelligence for the MSSP Community

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

**1100+**

Investigations per year

**400k**

Incident investigation hours in 2023

**500+**

Researchers & analysts

**30+**

languages spoken

**350+**

Tracked threat groups

**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



```
1 rule CEO_Fraud
2 {
3   meta:
4     author = "Natalie"
5     date = "11/06/2018"
6     description = "This is a basic YARA rule for CEO fraud."
7
8   strings:
9     $text_a = "wire transfer"
10    $text_b = "CEO"
11    $hex = { E2 34 A1 C8 23 FB }
12
13   condition:
14     $text_a or $text_b or $hex
15 }
```





Malicious or not?



**Malicious**

GTI SCORE: 30/100

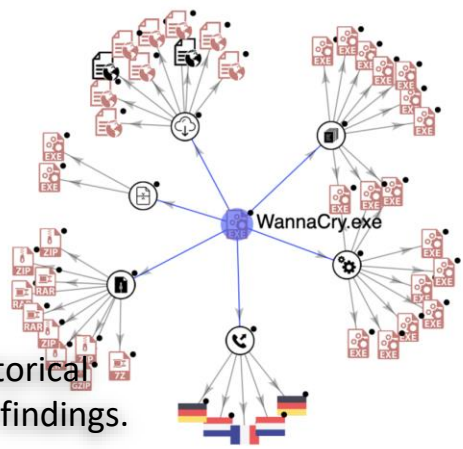
Severity level: **Low**

# 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.

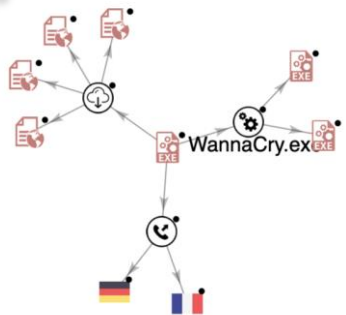
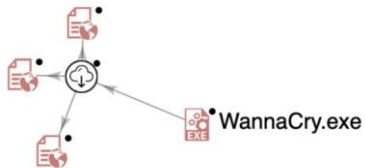


**THREAT CAMPAIGN EXPOSURE WINDOW (BLINDSPOT)**

*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)

The screenshot displays a security analysis tool interface. At the top left, a green circular progress indicator shows '0 / 59'. The main header area contains a green checkmark and the text 'No security vendors and no sandboxes flagged this file as malicious'. To the right of this are navigation options: 'Follow', 'Reanalyze', 'Download', 'Similar', and 'More'. Below the header, the file name 'steal\_session.ps1' is shown, along with its size '1.98 KB' and 'Last Analysis Date 3 months ago'. A list of tags includes 'powershell', 'url-pattern', 'detect-debug-environment', 'long-sleeps', 'direct-cpu-clock-access', and 'runtime-modules'. A 'Community Score' section is partially visible. Below the header is a navigation bar with tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', 'CONTENT', 'TELEMETRY', and 'COMMUNITY'. The 'Crowdsourced AI' section is active, showing a warning icon and the text 'NICS Lab flags this file as malicious'. A description follows: 'This PowerShell script is designed to stop and remove the Telegram process, delete Telegram data folders, compress the Telegram data folder, and upload the compressed data to an FTP server. The script uses various techniques to avoid detection, such as using ErrorAction SilentlyContinue to suppress errors and Write-Host to hide output. The script also includes variables for the FTP server, username, and Show more'. Below this is a 'Code Insight' section with an information icon and a description: 'The code snippet is designed to stop and remove the Telegram process, remove Telegram data folders, compress Telegram data folder, and upload the compressed data to an FTP server.' This is followed by several paragraphs of detailed analysis: 'The code first stops the Telegram process. It does this by using the 'Get-Process' cmdlet to get a list of all running processes. It then uses the 'Stop-Process' cmdlet to stop the process with the name 'telegram'.', 'The code then removes Telegram data folders. It does this by using the 'Remove-Item' cmdlet to remove the folders 'C:\Users\\${userName}\AppData\Roaming\Telegram Desktop\data\user\_data' and 'C:\Users\\${userName}\AppData\Roaming\Telegram Desktop\data\emoji'.', 'The code then compresses Telegram data folder. It does this by using the 'System.IO.Compression.FileSystem' namespace to create a compressed file from the folder 'C:\Users\\${userName}\AppData\Roaming\Telegram Desktop\data'. The compressed file is named 'C:\Users\\${userName}\AppData\Roaming\Telegram Desktop\data.zip'.', 'The code then uploads the compressed data to an FTP server. It does this by using the 'System.Net.Http' namespace to create a web request to the FTP server. The request is sent to the URL 'ftp://ftp.your\_ftp\_server.com/steal/\${date}.zip'. The request is authenticated using the username and password 'xxxx' and 'yyyy', respectively.', and 'The code is written in PowerShell. PowerShell is a powerful scripting language that is used to manage Windows systems. PowerShell can be used to automate tasks, create scripts, and manage files.' The final paragraph states: 'The code is malicious. It is designed to stop and remove the Telegram process, remove Telegram data folders, compress Telegram data folder, and upload the compressed data to an FTP server. The code could be used to steal data or to damage a computer.' At the bottom of the 'Code Insight' section is a 'Show less' link. The interface also features social media-style icons for thumbs up and thumbs down.

## An unique opportunity

Summarization /  
customization capabilities

Auto Hunting / Monitoring

Auto triage with full context

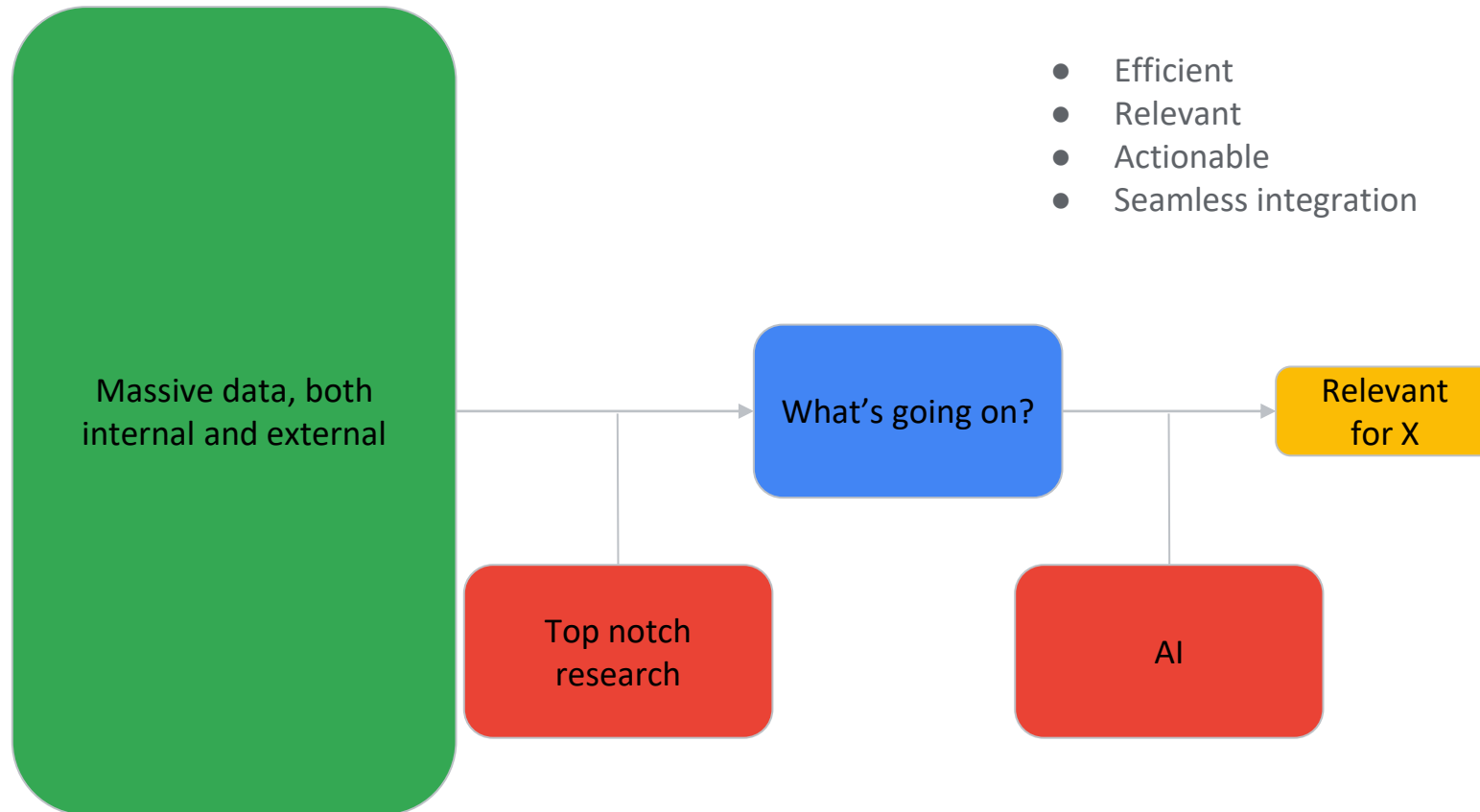


Massive data ingestion

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!





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](https://go.acronis.com/MSPGlobal2025)

