Artificial Identity

Alessio Pennasilico, CS Clusit
Marco Lucchina, Country Manager Italy Cynet

Alessio Pennasilico

Partner, Information & Cyber Security Advisory Team **P4I**
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico **Clusit** Associazione Italiana per la Sicurezza Informatica

Membro del Comitato Direttivo di Informatici Professionisti **AIP ITCS**

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità **Lloyd's Register LRQA**

Membro del Comitato di schema **kiwa** **intertek** Total Quality. Assured.

Direttore Scientifico della testata **CYBERSECURITY360**

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano **osservatori.net digital innovation**

Marco Lucchina
Country Manager Italy

MITRE attack technics

- Golden Ticket attack

- Kerberoasting

- Pass-the-hash attack

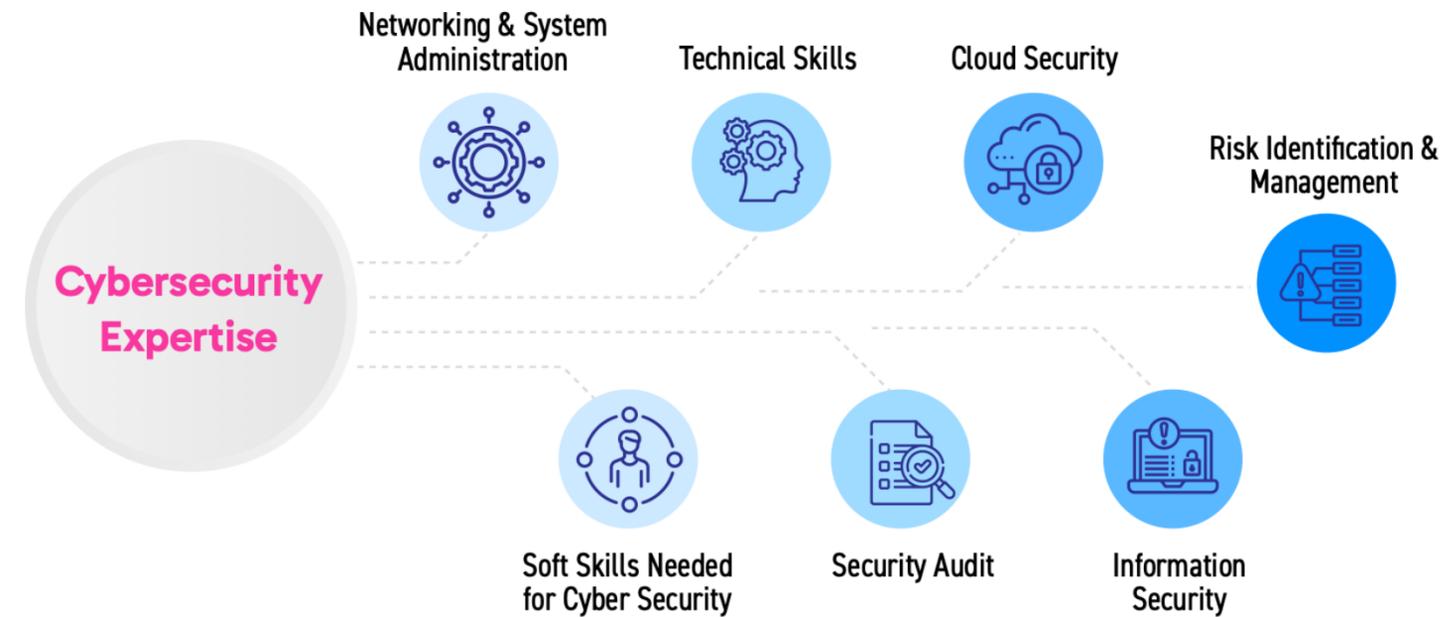- Silver ticket attack

- DC sync attack

Defense area

The weakest part of an infrastructure?

Intelligence report - *GossiTheDog*

- CVE-2022-40684
- 15.000 affected devices
- 25 months of collections
- Valid VPN credentials
- Email associated with firewall configuration
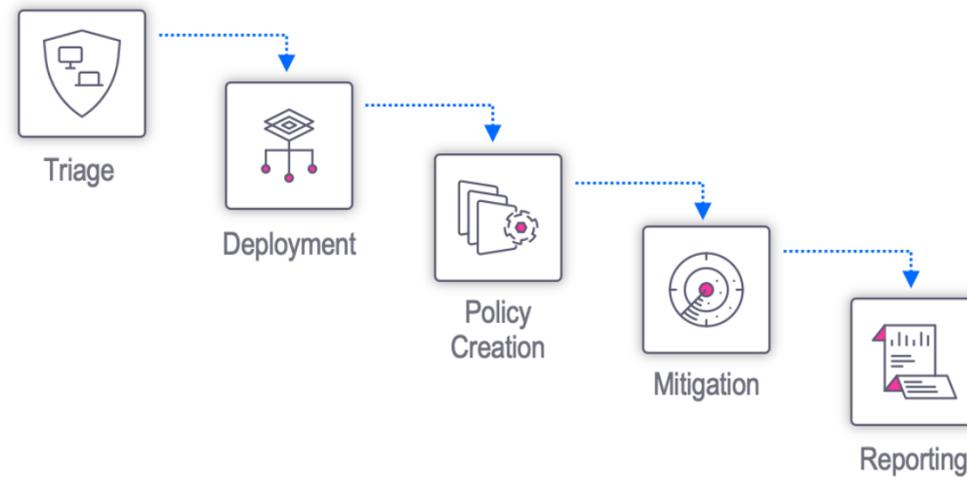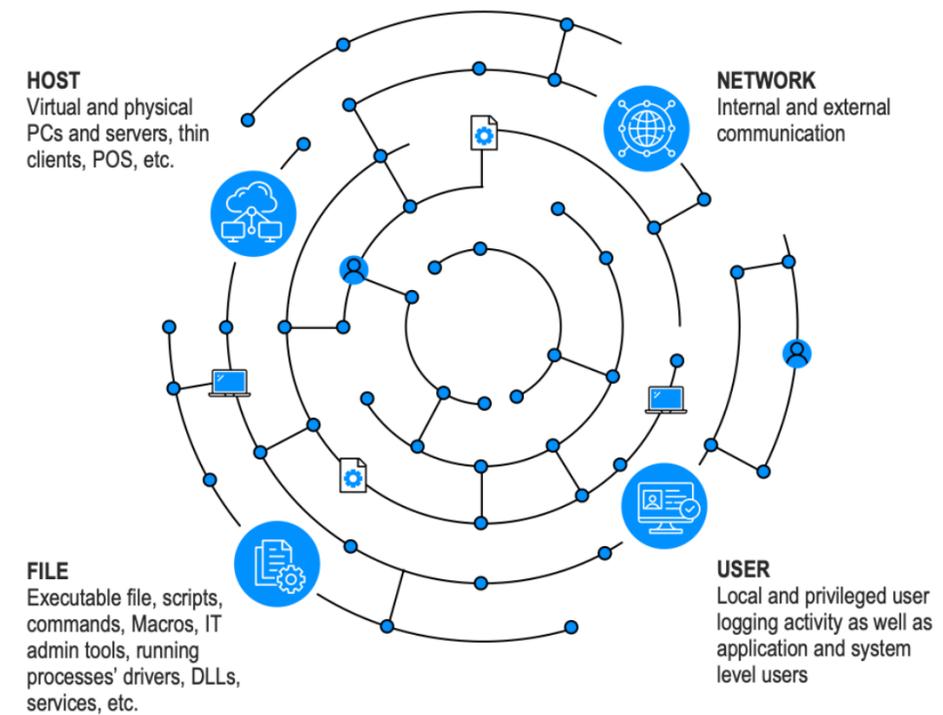- 333 Italian companies affected

Networking & System Administration

Technical Skills

Cloud Security

Risk Identification & Management

Cybersecurity Expertise

Soft Skills Needed for Cyber Security

Security Audit

Information Security

cynet

Cyber defense area

Detection and response

Incident management

Triage → Deployment → Policy Creation → Mitigation → Reporting

Monitoring the environment 24x7 and is always available for on-demand support.

HOST
Virtual and physical PCs and servers, thin clients, POS, etc.

NETWORK
Internal and external communication

FILE
Executable file, scripts, commands, Macros, IT admin tools, running processes' drivers, DLLs, services, etc.

USER
Local and privileged user logging activity as well as application and system level users
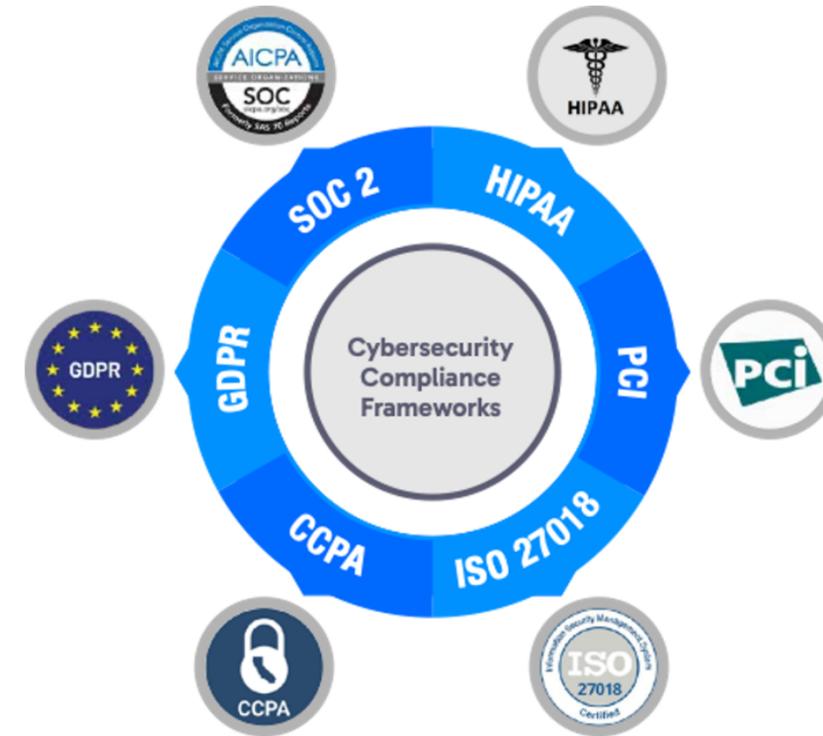
Back

Posture management
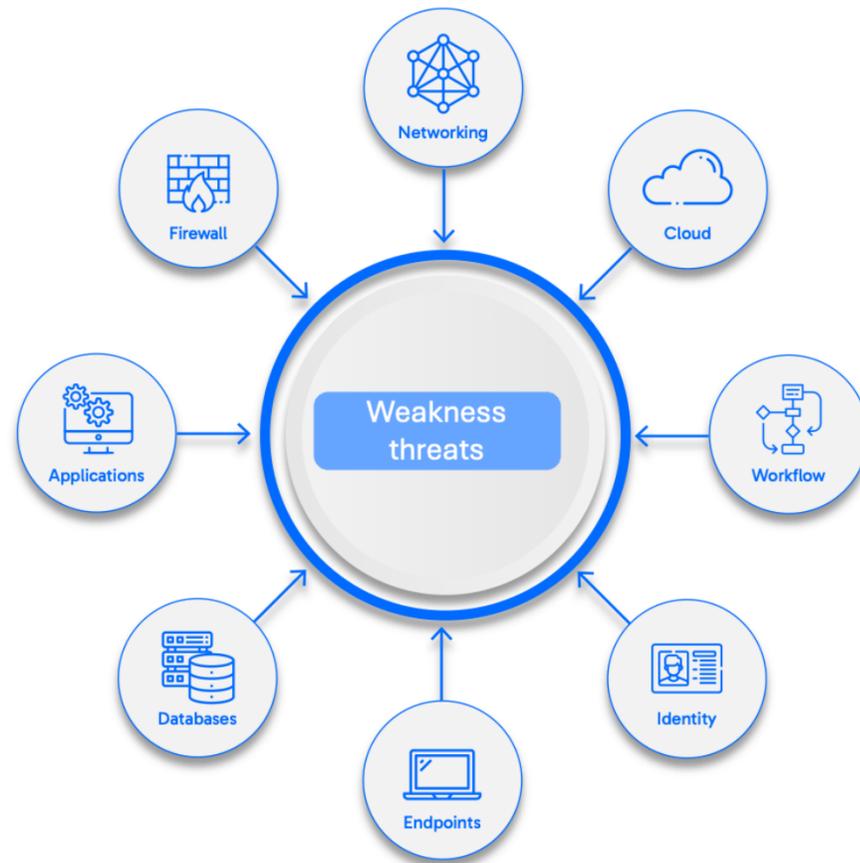
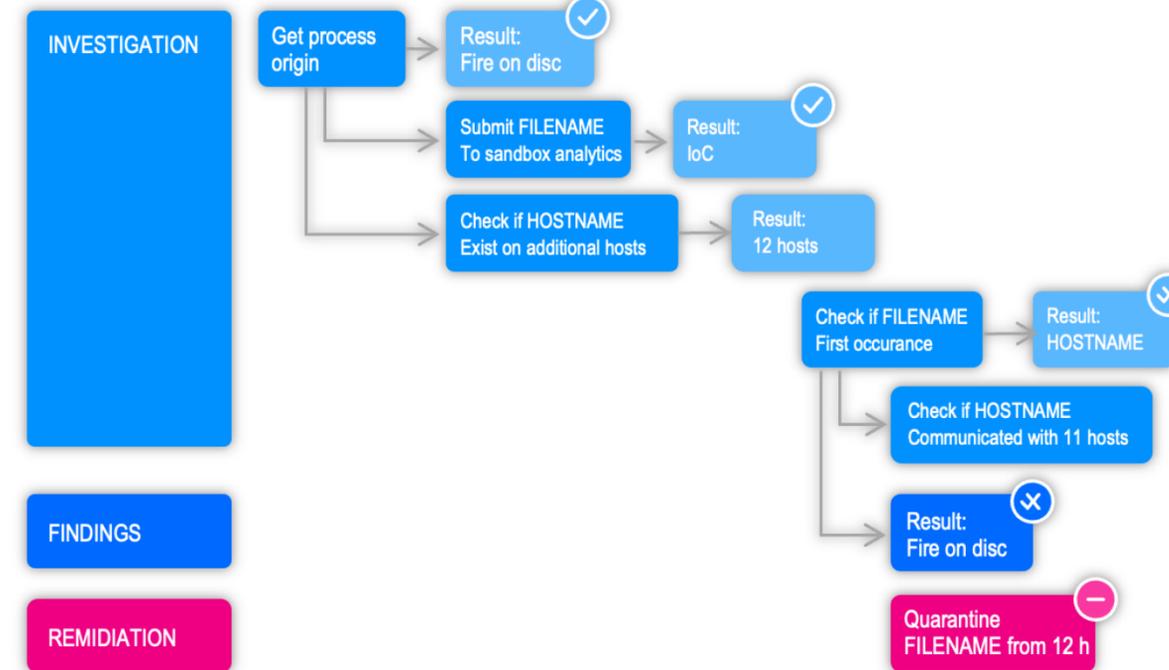Recommended settings to resolve security risks, ensure best practices & regulatory alignment with a single-click fix.

Complete visibility and automation

Weakness threats

- Networking
- Cloud
- Workflow
- Identity
- Endpoints
- Databases
- Applications
- Firewall

Autonomous Responder

INVESTIGATION

Get process origin → Result: Fire on disc ✓

Submit FILENAME To sandbox analytics → Result: IoC ✓

Check if HOSTNAME Exist on additional hosts → Result: 12 hosts

Check if FILENAME First occurance → Result: HOSTNAME ✗

Check if HOSTNAME Communicated with 11 hosts

Result: Fire on disc ✗

FINDINGS

REMIDIATION

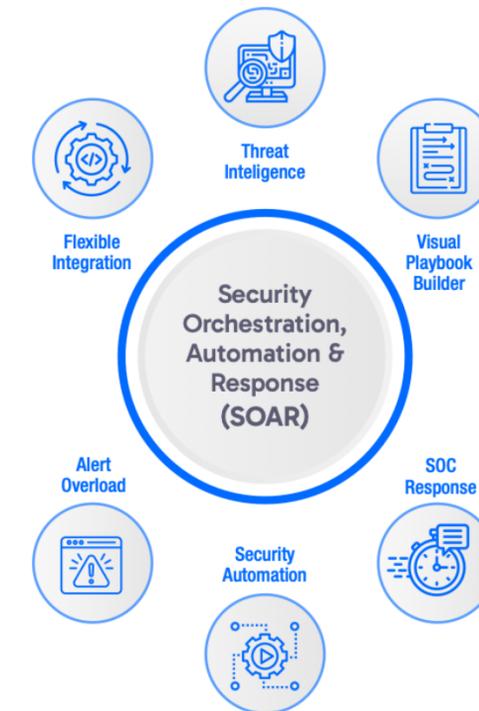Quarantine FILENAME from 12 h −

Incident response

Automatically find and resolve all attack components in seconds — not days or weeks.

Automate time-consuming manual tasks to increase team bandwidth.

Avoid the costly and resource-intensive implementation of a standalone SOAR solution.

Cybersecurity Automation

- Lower Costs
- Reduce Risks
- Product Safety
- Improve Predictability
- Superior Quality
- Enhance Process Consistency
- Greater Brand Protection
- Simplified Operations

Security Orchestration, Automation & Response (SOAR)

- Threat Inteligence
- Visual Playbook Builder
- SOC Response
- Security Automation
- Alert Overload
- Flexible Integration

Cynet made MITRE ATT&CK history again in 2024

ONLY Cynet Delivers 100% Protection and Detection Visibility in the 2024 MITRE ATT&CK Evaluations: Enterprise - without configuration changes

MITRE ATT&CK 2024 EVALUATIONS RESULTS
VISIBILITY VS. PREVENTION RATE
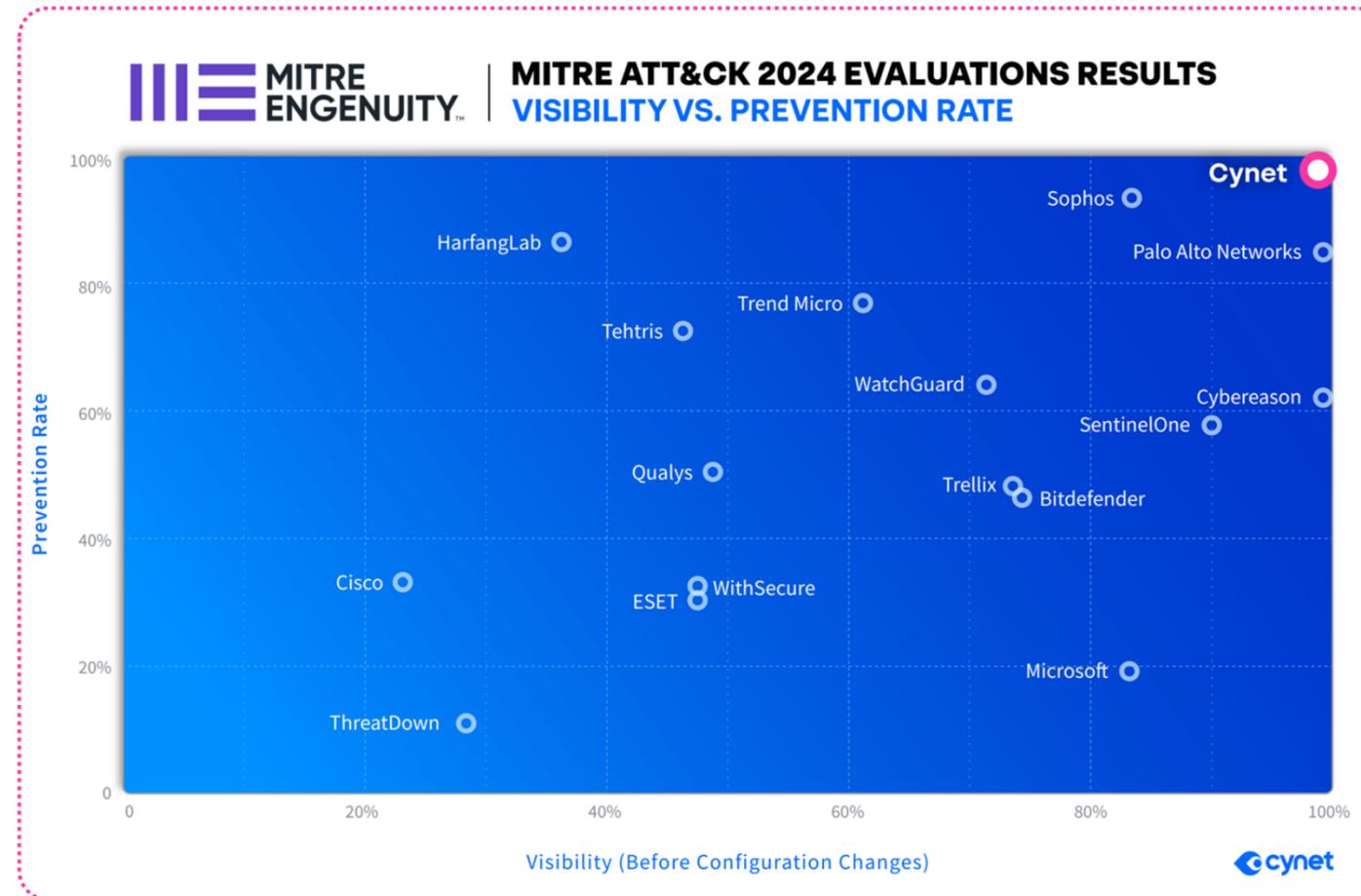
Better protection, better visibility, better coverage
No false positives

MITRE ATT&CK 2024 EVALUATIONS RESULTS
CYNET PERFORMANCE HIGHLIGHTS

100%
Detection Visibility

77 of 77 Attack Sub-Steps with NO CONFIGURATION CHANGES

100%
Protection

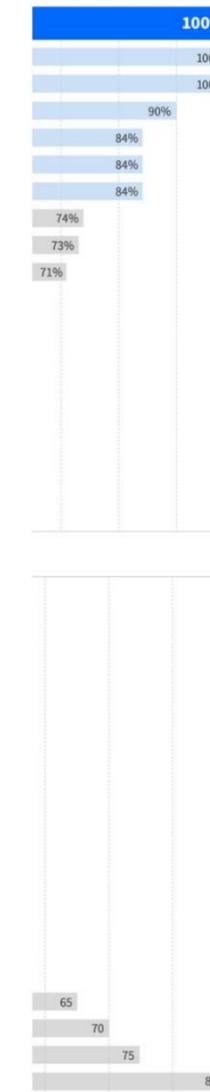21 of 21 Malicious Sub-Steps Blocked

100%
Technique Coverage

77 of 77 Technique level Detections with NO CONFIGURATION CHANGES

0 False
Positive Detections

0 of 20 Legitimate Sub-Steps Flagged as Malicious

A picture, please!

Q&A

Contatti:

marcol@cynet.com

Vieni a trovarci al nostro stand!