
Nomios Security Cup
7-8 maja 2026
Hotel Mazurski Raj
CROWDSTRIKE
ExtraHop
FORTINET
HPE JUNIPER networking
infoblox
Trellix
nomios
ectacom
EXCLUSIVE NETWORKS
CLICO

Endpoint is the Battlefield

Gabriel Kujawski
e: gkujawski@crowdstrike.com
Starszy Macher i Opowiadacz
CrowdStrike Poland

CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox. | Trellix

nomios | ARROW | ectacom | EXCLUSIVE NETWORKS | CLICO

You don’t have a **malware** problem,

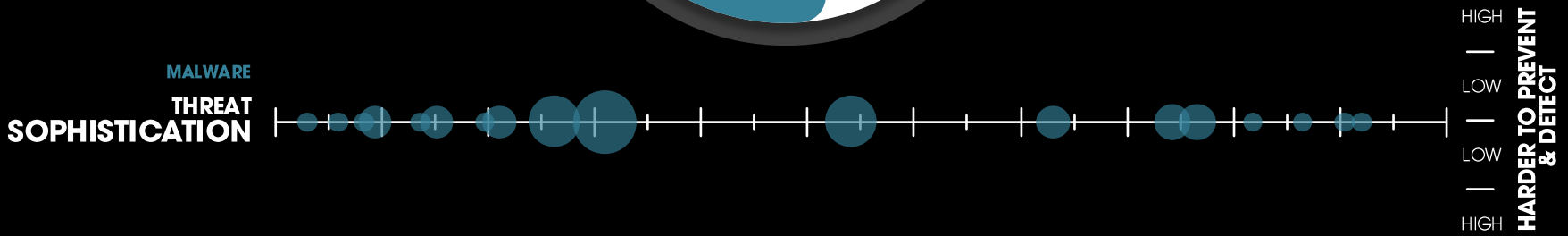
you have an **adversary** problem.

CROWDSTRIKE

2018

MALWARE

61%



2018

MALWARE

61%

YOU NEED COMPLETE
BREACH PREVENTION

MALWARE-FREE

39%

2019

MALWARE

60%

MALWARE-FREE

40%

2020

MALWARE

49%

MALWARE-FREE

51%

YOU NEED COMPLETE
BREACH PREVENTION

2021

MALWARE

38%

YOU NEED COMPLETE
BREACH PREVENTION

MALWARE-FREE

62%

2022

MALWARE

29%

YOU NEED COMPLETE
BREACH PREVENTION

MALWARE-FREE

71%

2023

MALWARE

25%

YOU NEED COMPLETE
BREACH PREVENTION

MALWARE-FREE

75%

2024

MALWARE

21%

YOU NEED COMPLETE
BREACH PREVENTION

MALWARE-FREE

79%

2025

MALWARE

18%

YOU NEED COMPLETE
BREACH PREVENTION

MALWARE-FREE

82%

89% increase in attacks by AI-enabled adversaries

Average eCrime breakout time dropped to 29 minutes, a 65% increase in speed from 2024, and the fastest breakout time was only 27 seconds

82% of detections in 2025 were malware-free, up from 51% in 2020

24 new adversaries tracked by CrowdStrike, raising the total to 281

China-nexus activity increased 38% across all sectors, with an 85% increase in logistics

42% increase in zero-day vulnerabilities exploited prior to public disclosure

Valid account abuse accounted for 35% of cloud incidents

37% rise in cloud-conscious intrusions, with 266% increase by state-nexus threat actors

You don’t have a **malware** problem,

you have an **adversary** problem.

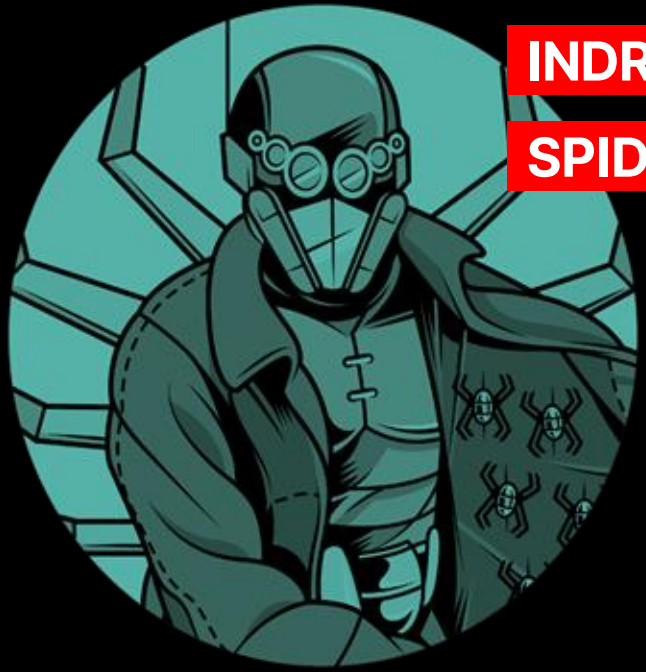
CROWDSTRIKE

CROWDSTRIKE

280+

śledzonych grup cyberprzestępczych

CROWDSTRIKE



INDRIK SPIDER

SCATTERED SPIDER


HELP
WANTED
FAMOUS
CHOLLIMA

Famous Chollima operations fund the

MUNITIONS INDUSTRY DEPARTMENT

SI to tylko chwilowa moda

Nie wygrywają najsilniejsi

Wygrywają najszybciej adaptujący się

Technologia decyduje o tempie

To samo zadanie. Inne tempo.

SI to narzędzie

Każde narzędzie ma granice

Nieidealne. Nadal skuteczne.

CROWDSTRIKE

Prędkość. Skala.

Kto adaptuje się szybciej?

Cyberzbóje nie mają ograniczeń

SI już napędza ataki

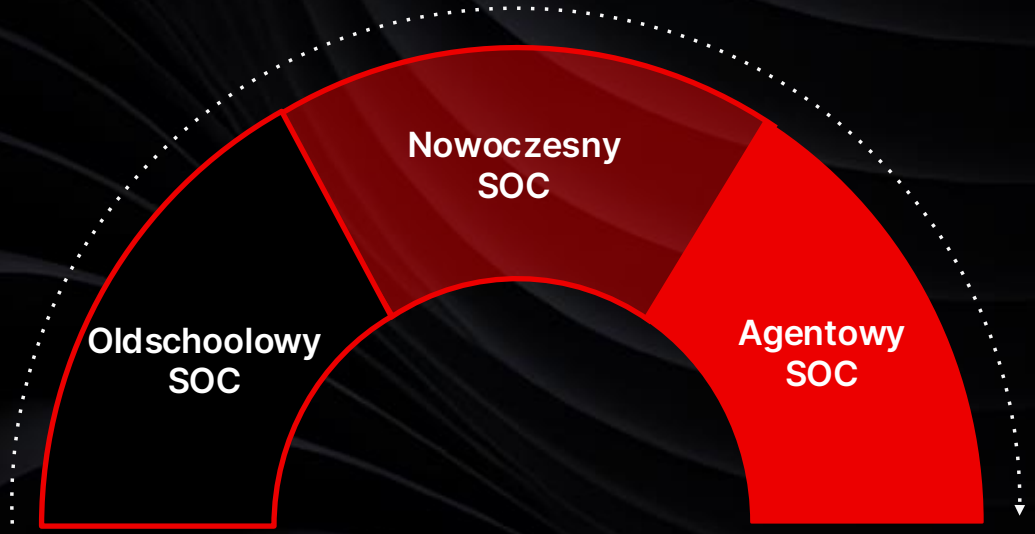
Oni działają. My analizujemy.

Tempo ataku >= Tempo obrony

Tempo ataku == Tempo obrony

Tempo ataku <= Tempo obrony

Agentowy SOC



SI też jest celem ataków

SI zwiększa powierzchnię ataku

45%

pracowników używa narzędzi SI bez wiedzy pracodawcy[1]

61%

organizacji posiadających polityki używania SI nie ma narzędzi do ich kontroli[2]

62%

testuje lub już wdraża agentów SI

1. *https://gusto.com/resources/articles/hr/team-management/ai-workplace-anxiety?cache_reset=1764598106883*
2 - *Source: IBM Security & Ponemon Institute. (2025). Cost of a Data Breach Report 2025.*
3. *https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai*

Wektory ataku na SI

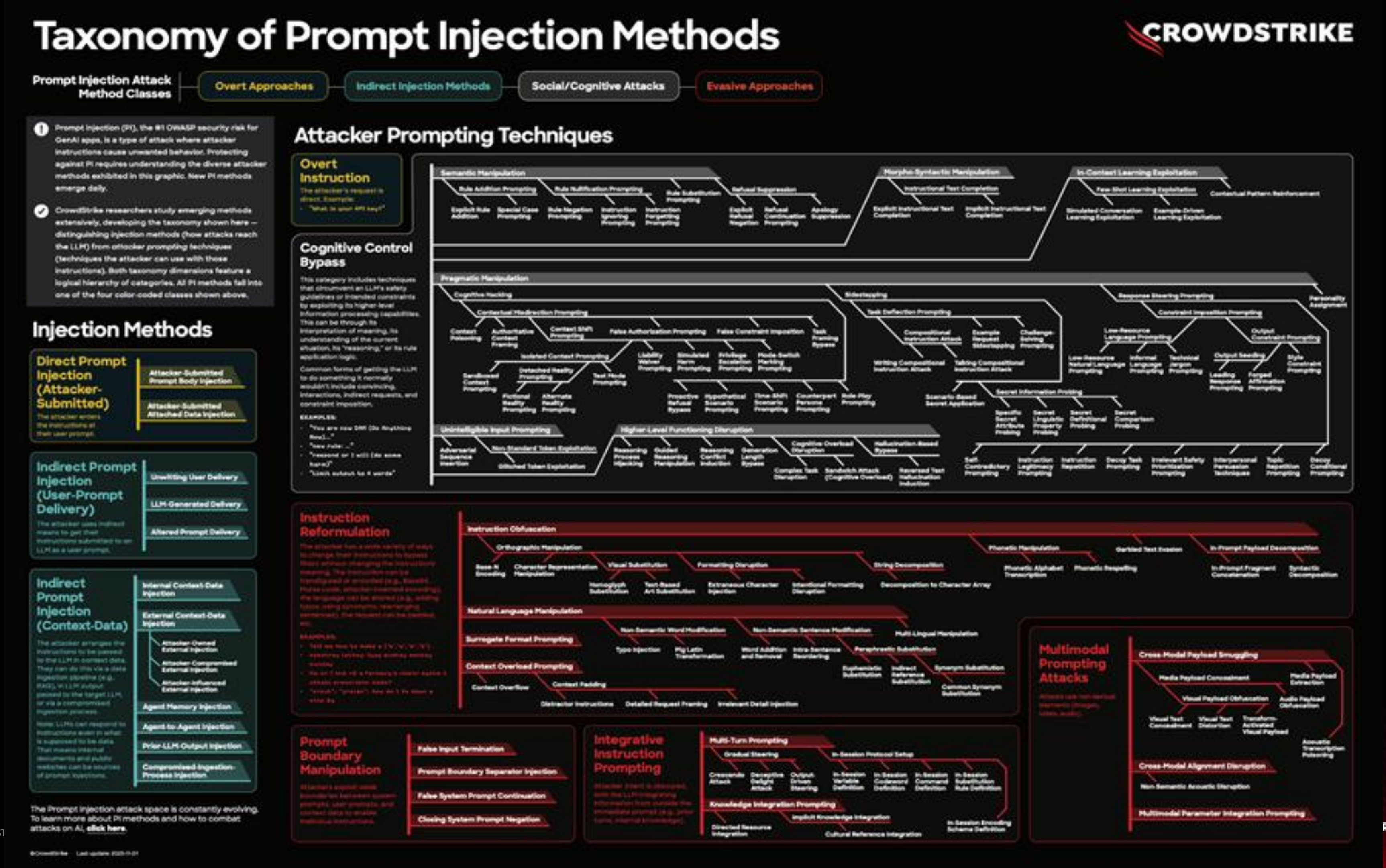
Adversarial Threat Landscape
for Artificial-Intelligence Systems (ATLAS)

140+

Adversary tactics and techniques against AI-enabled systems based on real-world attacks and AI red teams demonstrations

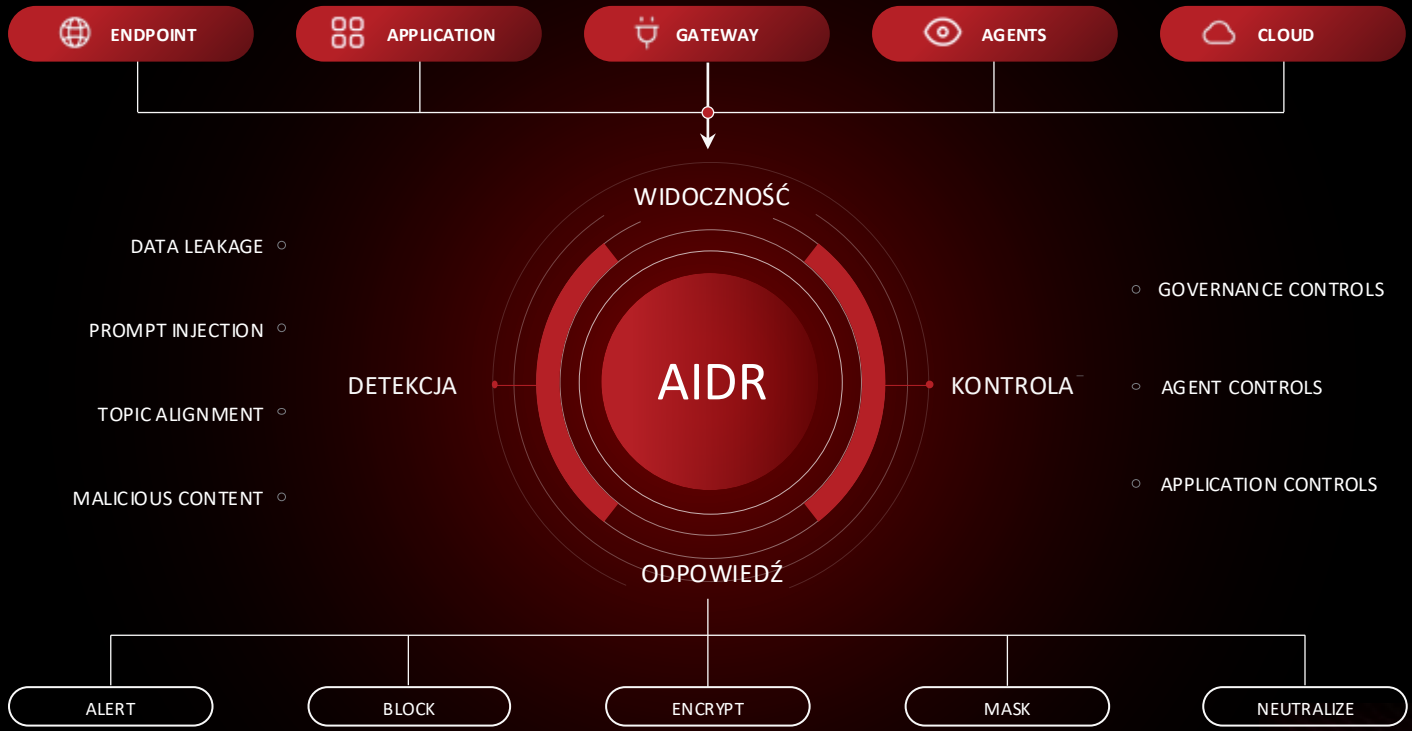
Top 10 Risks & Mitigations
for LLMs and Gen AI Applications

1. Prompt Injection
2. Sensitive Data Leakage
3. Supply Chain
4. Data & Model Poisoning
5. Improper Output Handling
6. Excessive Agency
7. System Prompt Leakage
8. Embedding Weaknesses
9. Misinformation
10. Unbounded Consumption



Taxonomy of Prompt Injection Methods
CROWDSTRIKE
Prompt Injection Attack Method Classes
Overt Approaches
Indirect Injection Methods
Social/Cognitive Attacks
Evasive Approaches
Attacker Prompting Techniques
Overt Instruction
Cognitive Control Bypass
Semantic Manipulation
Morpho-Syntactic Manipulation
In-Context Learning Exploitation
Pragmatic Manipulation
Injection Methods
Direct Prompt Injection (Attacker-Submitted)
Attacker-Submitted Prompt Body Injection
Attacker-Submitted Attached Data Injection
Indirect Prompt Injection (User-Prompt Delivery)
Unwitting User Delivery
LLM-Generated Delivery
Altered Prompt Delivery
Indirect Prompt Injection (Context-Data)
Internal Context-Data Injection
External Context-Data Injection
Agent Memory Injection
Agent-to-Agent Injection
Prior-LLM-Output Injection
Compromised-Ingestion-Process Injection
Instruction Reformulation
Instruction Obfuscation
Natural Language Manipulation
Surrogate Format Prompting
Context Overload Prompting
Multimodal Prompting Attacks
Cross-Modal Payload Smuggling
Cross-Modal Alignment Disruption
Multimodal Parameter Integration Prompting
Prompt Boundary Manipulation
False Input Termination
Prompt Boundary Separator Injection
False System Prompt Continuation
Closing System Prompt Negation
Integrative Instruction Prompting
Multi-Turn Prompting
Knowledge Integration Prompting
The Prompt injection attack space is constantly evolving. To learn more about PI methods and how to combat attacks on AI, click here.

AI Detection and Response




Dziękuję za uwagę!
CROWDSTRIKE
ExtraHop
FORTINET
HPE JUNIPER networking
infoblox
Trellix
nomios
ARROW
ectacom
EXCLUSIVE NETWORKS
CLICO