ARCTIC WOLF

THE LEADER IN **SECURITY OPERATIONS**

Beyond Threat Detection

Leveraging Artificial Intelligence in the Modern Security Landscape

Christopher Fielder
Field CTO

The Human - AI Partnership

The interest in Artificial Intelligence in cybersecurity remains high, but humans continue to play a critical role.

Arctic Wolf research into how organizations are planning to utilize AI within their security programs found that leadership is not prepared to fully embrace and trust AI as a solution independent of human expertise.

Security decision makers want AI powered solutions that empower their humans rather than replacing them

01

Nearly 1 in 3 consider AI to be a primary driver for their cybersecurity strategy moving forward.

02

Respondents show huge appetite for AI, believing it has potential to **enhance SOC capabilities.**

03

Leaders are not prepared to turn the keys over to AI. **Humans play a pivotal role** in contextualizing threats and data.

04

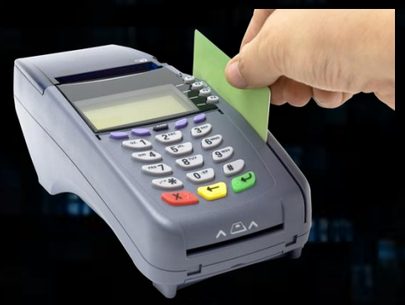
AI and human engineers could make a formidable team, but **lack of skilled experts presents obstacles** to managing AI.

Technological Advances: “Can We” *not* “Should We”

Every Advancement made in modern technology has ultimately been used by criminals

The Printing Press

- Mass production of Information
- Counterfeiting and Propaganda



Credit Card & PCI

- Cashless immediate transactions
- CC Fraud and Card Skimmers

Telephones

- Instant Global Communication
- Telephone Fraud and “Phone Phreaking”

Encryption

- Data security in motion and at rest
- Ransomware!

The Future: An AI Arms Race?

The worst potential future:

"Is your AI better than their AI"

Threat actors are actively leveraging Artificial Intelligence to facilitate cybercrime

Why should be concerned? Can't we just build better AI?

- You have to eliminate all vulnerabilities; They must only find one
- You are utilizing the baseline of normal, what is normal?
- Whose AI is better trained? "Junk in = Junk out"
- Defenders are bound to AI Ethics, Cybercriminals are not

We are not the only ones investing in AI

Cybercriminals are actively developing malicious Artificial Intelligence to facilitate sophisticated cybercrime

New Variants of Polymorphic Malware

AI Powered Bots and Botnets

Enhancing Social Engineering via AI

AI Analysis to monetize large data sets

We are not the only ones investing in AI

Cybercriminals are actively developing malicious Artificial Intelligence to facilitate sophisticated cybercrime

Anomaly Avoidance

(Reverse Baselining)

LLM Poisoning

(Evil ChatGPT)

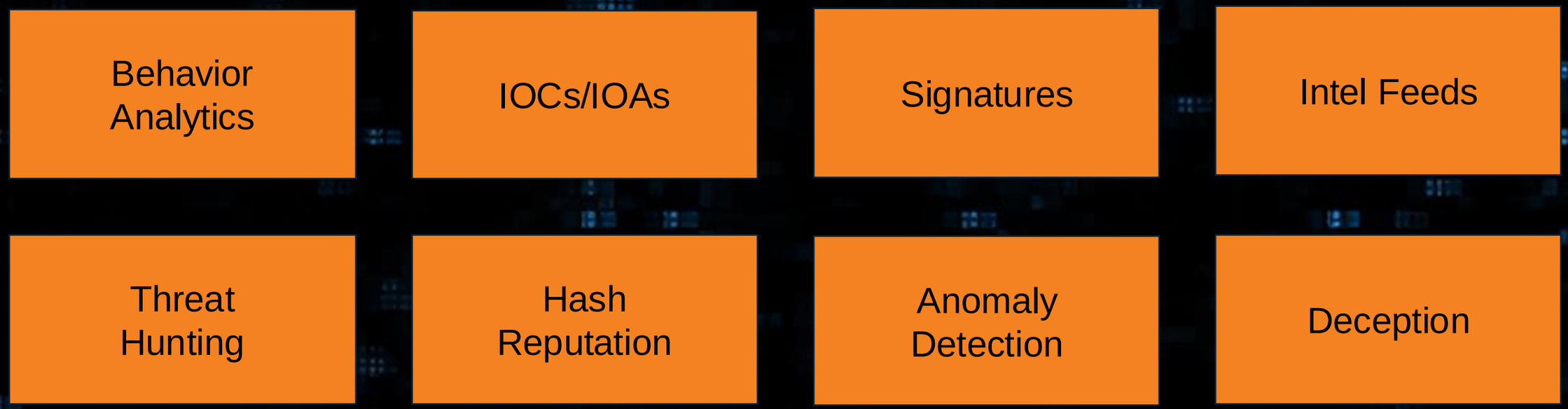
Self Directing Phishing Campaigns

Threat Detection is no longer our root concern

More threat detection methods exist today than ever before, and almost every detection method is either powered by or aided with some form of artificial intelligence or machine learning.

Yet despite the numerous ways in which we can detect threats and the more we invest in AI, the problem seems to grow.

- 48% of organizations were breached in 2023
- 48% of companies fell victim to at least one ransomware attack in the last 12 months
- Ransom demands have increased by 20% of a median of $600,000



“Put AI in it!”

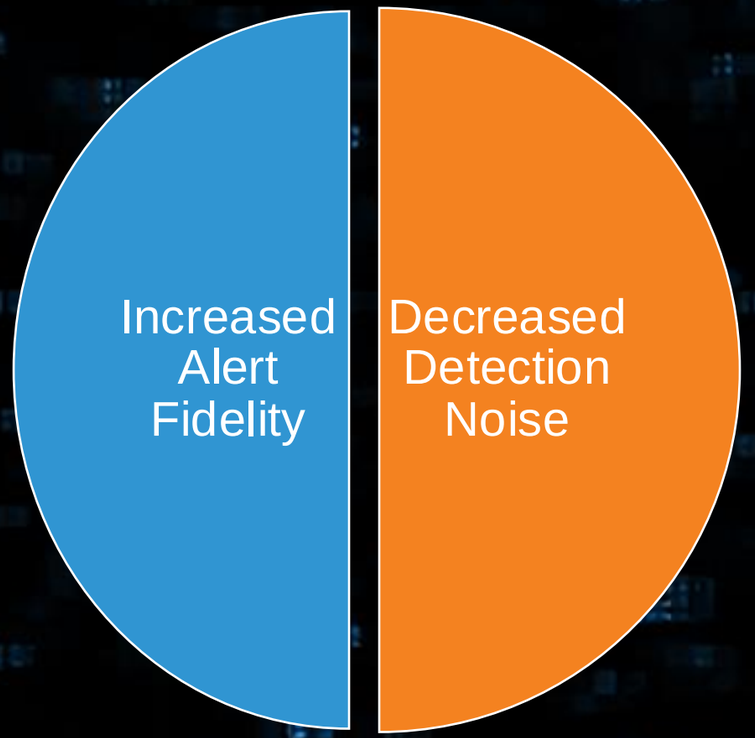
But, what problems are we trying to solve?

Detection alone is no longer the focal point

Every security device you have invested in can detect and alert (and most use “AI”)

- EDR, XDR, NGAV
- SIEM
- NDR
- ETC

- **Yet Attacks Increase YOY, with the Median ransom demand increasing 20% in the last year to $600,000**



If we hope to minimize the impact of modern threats, we must decrease detection noise and increase efficacy

- Increase Time to Response (TTR) rather than focusing solely on TTD
- Increasing alert fidelity (Quality over Quantity)

Beyond Threat Detection

2022

Noise Suppression and False Positive Reduction

Automated Cross-surface Evidence Collection

Stronger Threat Intelligence

Future

The Results of AI Enhanced Security Operations

DWELL TIME

0:23

Industry average time to identify an intrusion is 206 days.
Arctic Wolf does it on average in 23 minutes.

ADVANCED THREATS

62%

of customers had advanced threat activity being missed by security tools but caught by Arctic Wolf.

ARCTIC WOLF

SYSTEMS engineering

THE LEADER IN **SECURITY OPERATIONS**

Thank You