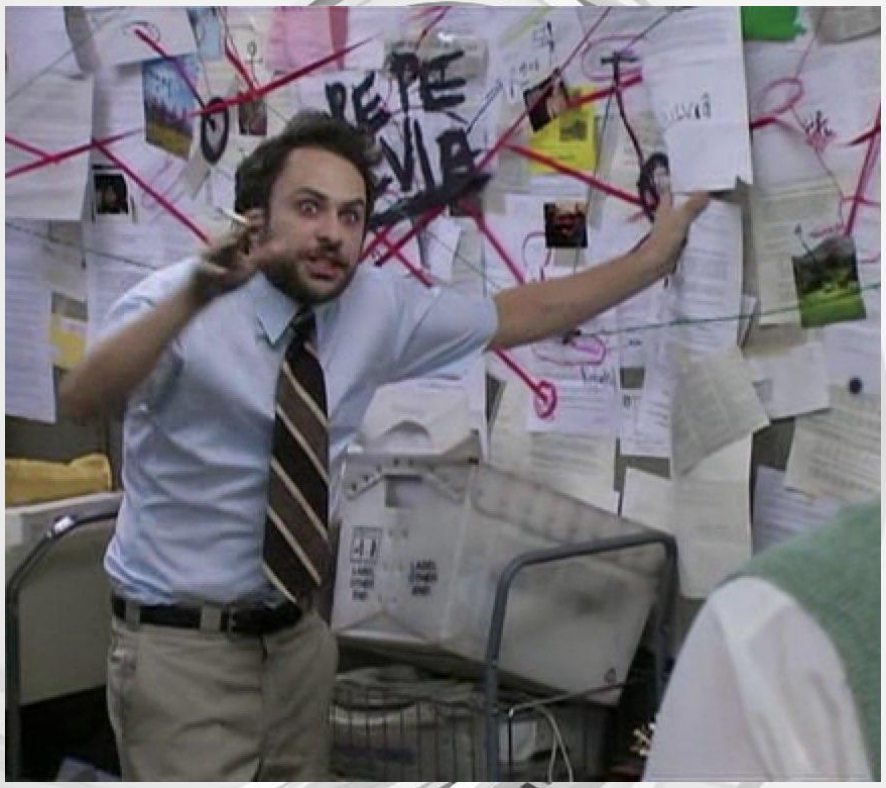
Double-Edged Sword: AI for Cyber Defense

Yet another AI Talk.. now with more memes!



Stefan Pfeiffer
Alexander Ressl

accenture

Cybersecurity is at an inflection point driven by six key trends

1
Digital transformation and expanding attack surface

The number of IoT devices worldwide is forecasted to almost **triple** from 9.7 billion in 2020 to more than **29 billion** IoT devices in **2030**.

Statista

2
Cybersecurity shift from technology risk to business risk

88% of Boards of Directors view **cybersecurity as a business risk**, as opposed to a technology risk.

Gartner

3
Responsible adoption of generative AI to fuel growth and build trust

In just one year, Accenture Cybersecurity Intelligence team saw an **815% surge** in the use of AI technologies **by dark web criminals.**

Accenture Cyber Intelligence analysis 2023

4
Cybersecurity vendor optimization across supply chain

75% of organizations state they are currently pursuing security vendor consolidation with the number rising to **90%** by **end of 2022**.

Gartner

5
Cybersecurity workforce retention and enablement

3.4 million global shortage of cybersecurity professionals

ISC² Cybersecurity Workforce Study

6
Global disruption and elevated threat landscape

93% of cybersecurity experts and **86%** of business leaders believe global geopolitical instability is likely to lead to a catastrophic cyberattack in the next two years

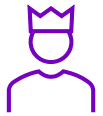
Global Cybersecurity Outlook Report 2023

AI is changing Social Engineering forever

Impersonation

	Spear phishing	Deepfakes	Misleading Images	Voice Cloning
Concern				
Example	FraudGPT appeared in July 2023 and distributed via Telegram. Similar to ChatGPT in its use but without limitations or restrictions, it **allows you to create highly targeted phishing scenarios** by specifying victims.	In 2023, several European politicians had been tricked into **arranging meetings with a person posing as a Russian politician using deepfake technology.**	Generative AI tools have been used to create a string of AI generated images which **falsely show world leaders in disparaging situations.**	In 2019, scammers used voice cloning technology to **impersonate the boss of a U.K. based energy company** and demanded $243,000 be transferred. The newest Version of ChatGPT is also able to clone voices now.

A Game Changer For Attackers

	Exploitation	Authentication	Image reputation / Influence	
Concern	 **Polymorphic Malware**	 **Credential Hacking**	 **Public people**	 **Fake News, Spam**
Example	BlackMamba is a **“trial” polymorphic malware** that relies on AI. What's new? Its **self-generation** is renewed each time, making it possible to fool protection and detection processes.	Using PassGan, 51 percent of passwords from the RockYou dataset, which comprises 15.68 million common passwords, were cracked in under one minute, with an additional 20 percent cracked in under a day.	 An X (Twitter) user shared photos of ‘Donald Trump getting arrested’. The **hyper-realistic eerie images went viral, creating shock and delight**. Next step videos..	 Meta’s AI bot Galactica was heavily criticized and ultimately pulled back for generating what experts called ‘statistical nonsense’ and ‘deep scientific fakes’.

AI-enhanced Cyber Defense

Because we are defenders aren’t we ;)

Key AI Use Cases

01

Prevent threats

More efficiently utilize threat intelligence to reduce an organization's exposure and improved response mechanisms to prevent incidents from expanding into large-scale breaches.

02

Decrease toil

Decrease manual, repetitive and automatable tasks to free up valuable time and resources of security analysts to focus on valuable security work.

03

Scale talent

Use AI to automate mundane and repetitive tasks and create an attractive work environment for security professionals. AI can also enable staff with fewer technical skills to interpret complex problems.

AI Use Case Examples

AI-enabled Security Operations

Simplify search (i.e., through natural language), complex data analysis (i.e., through summaries), threat detection engineering (i.e., use cases, playbooks creation) and Gen AI-based security assistant (i.e., code analysis)

AI-enabled Threat Intelligence

Summarize industry-leading, frontline threat intelligence into an easy-to-comprehend format. Security teams can quickly understand how the latest threats may be targeting their organization, and how they can make threat intelligence actionable across their organization.

Improved Threat Detection

Through machine learning, AI systems can identify patterns and trends in data that may be overlooked by humans. This contributes to improved detection accuracy, especially for complex and rapidly evolving threats.

Automated Vulnerability Management

AI can perform security scans, identify vulnerabilities, and in some cases, even suggest automated actions to remediate them.

Preventive Security Exposure Management

In addition to pure vulnerability management, AI-enabled Preventive Exposure management can solve complex attack vectors. Analyse, evaluate, prioritize attack patterns and attack vectors and develop appropriate defense strategies.

Automated Compliance

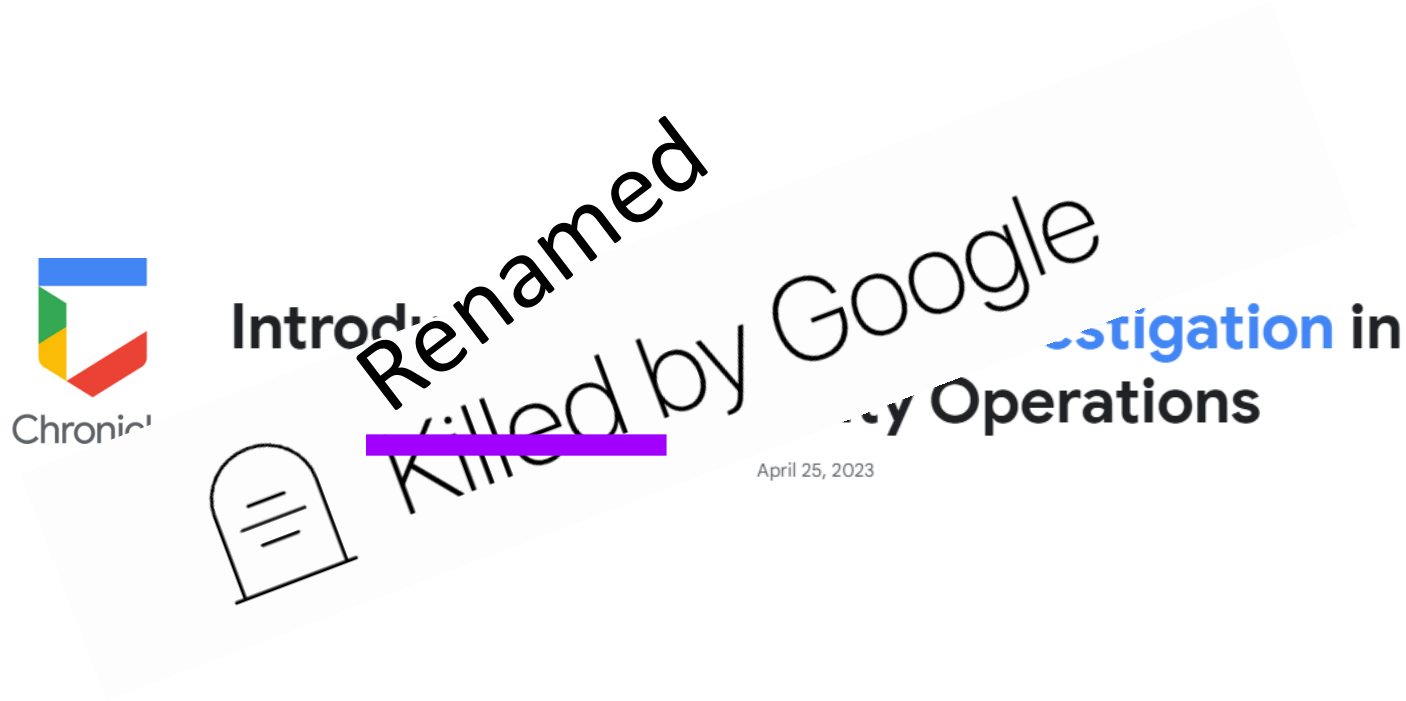
AI can help automate compliance with security policies and standards by continuously monitoring security configurations and responding to deviations.

Automated Response

AI can initiate automated responses to specific security events or attacks. This results in a faster response time, minimize damage and implement countermeasures in real time.

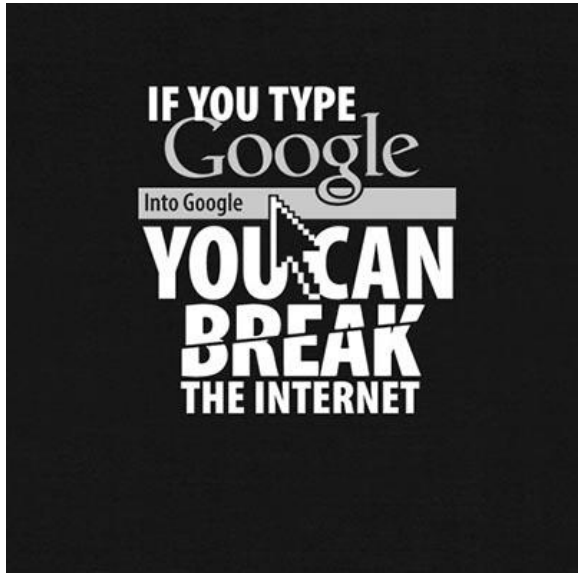
Introducing AI-powered investigation in Chronicle Security Operations

April 25, 2023



Google SecOps

Introducing AI-powered investigation



Security AI Assistant for SOC Analysts

Context

In the current landscape, Security Operations Centers are experiencing significant challenges that affect the performance of Level 1 SOC analysts. There is a pressing need for solutions that boost operational efficiency, automate mundane tasks, and improve threat escalation decision-making processes.

Challenges:

- High volume of security alerts
- High rate of false positives
- Complexity in managing a variety of security tools
- High turnover rates among Level 1 analysts
- Prevailing skills gap in the cybersecurity industry
- Routine tasks diverting focus from critical security issues
- Difficulty in accurate threat escalation decision-making

Solution

To address these issues, it is critical to find a solution that enhances operational efficiency, minimizes false positives, automates routine tasks, and supports more effective decision-making for threat escalation in SOCs.

The "Security AI Assistant for SOC Analysts" is an AI-driven tool designed to transform the efficiency and effectiveness of your SOC operations, significantly addressing key challenges experienced by Level 1 analysts.

Key Capabilities:

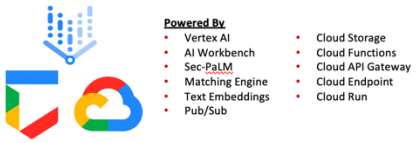
- **Streamlined Alert Management**: Intelligent prioritization and reduction of false positives
- **Continual Adaptation**: Counters high turnover rates with its ability to learn and adapt
- **Skills Gap Compensation**: Fills the talent void with advanced AI capabilities
- **Automated Routine Tasks**: Frees analysts to focus on critical security issues

Impact

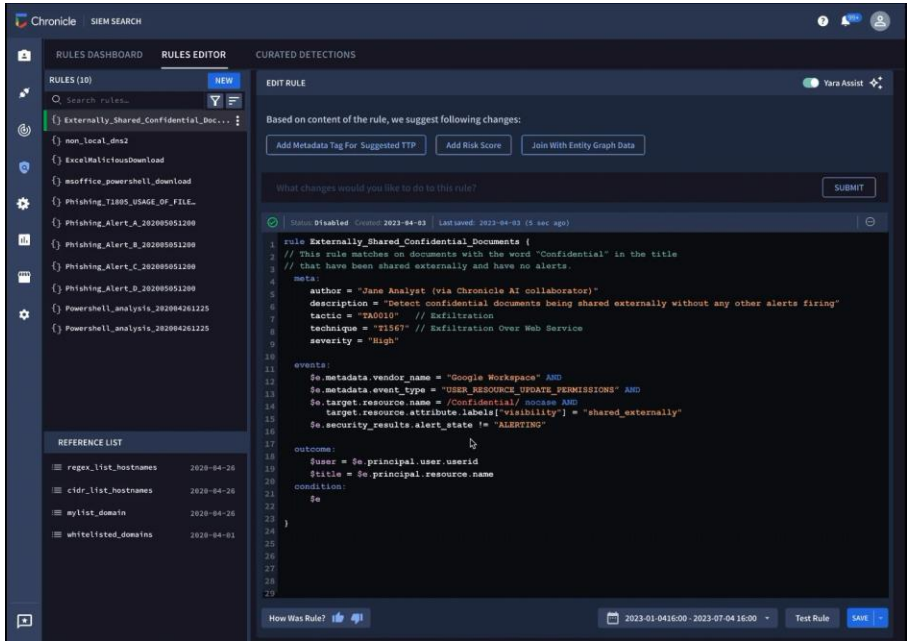
The "Security AI Assistant for SOC Analysts," with capabilities like streamlined alert management, continual adaptation, skills gap compensation, and automation of routine tasks, has the potential to significantly transform the global security industry. It promises to enhance efficiency and accuracy, adapt to rapid changes, bridge the existing skills gap, reduce operational costs, and expand the reach of advanced security services. By focusing on intelligent prioritization and automation, it frees analysts to address critical issues, democratizes access to high-level security, and improves overall response to threats.

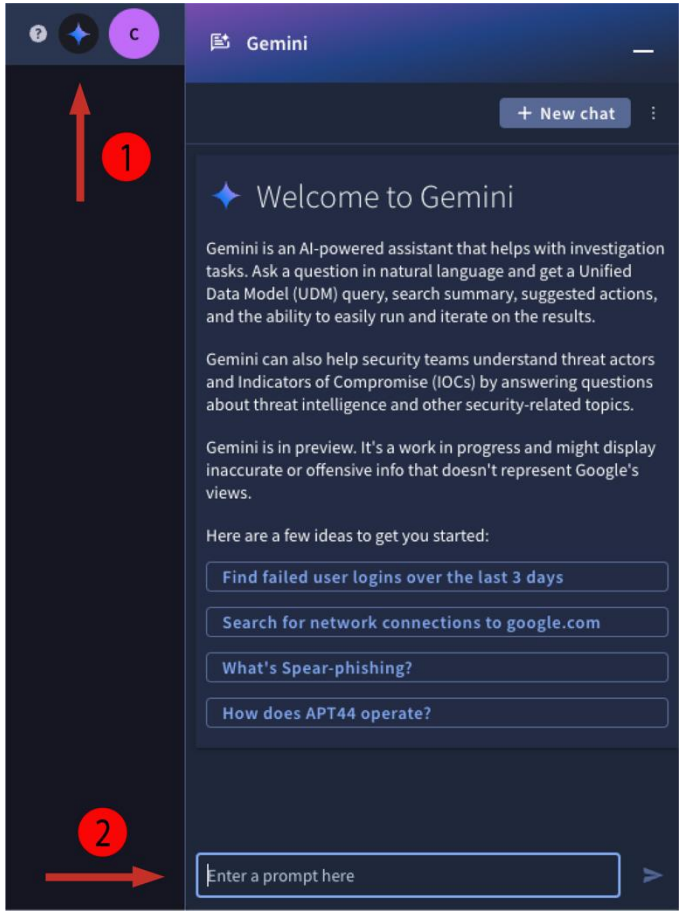
Empowering SOC analysts with:

- Knowledge expansion
- Streamlined decision-making
- Optimized efficiency through automation rapid response mechanisms



Gemini features working *today*





Key Facts

- Gemini can be used to **generate Queries, Detection Rules and SOAR Automations**
- **Investigations** are enriched via Gemini

Risks associated with utilization of Generative AI

Sensitive Data Exposure
Gen AI models trained on sensitive data creates additional risk of exposure of sensitive information

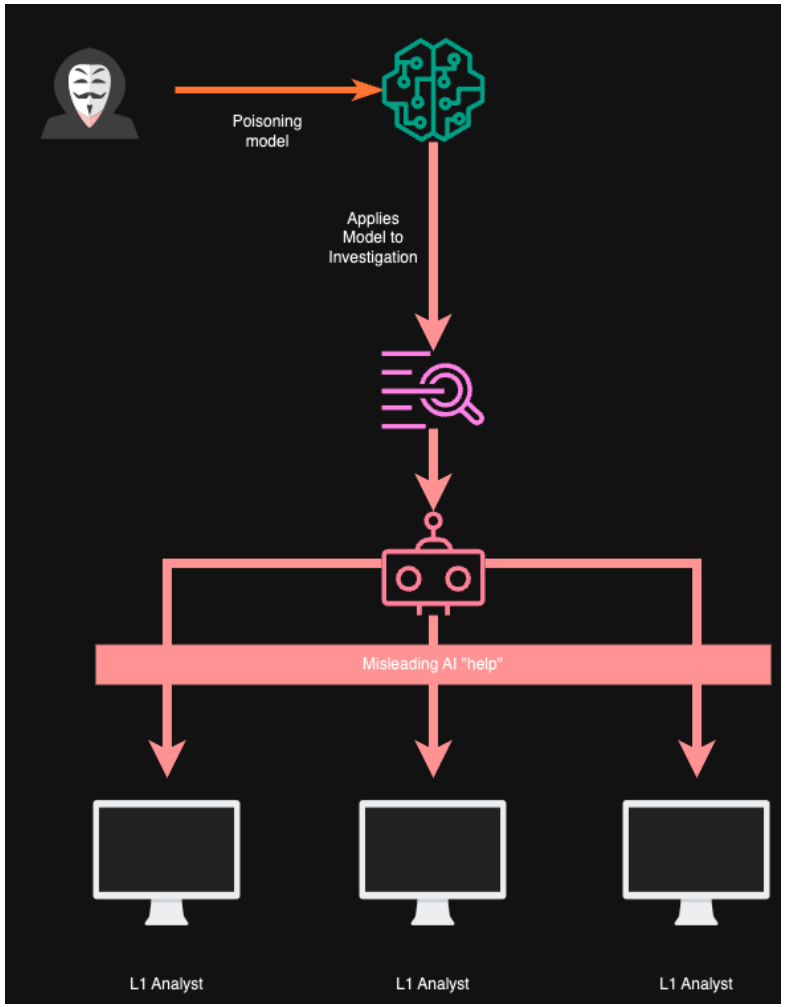
Gen AI Model Disruption
Attacks on AI infrastructure expose risks to disruption of AI models and dependent business operations

Gen AI Bias
Unconscious biases in training data can lead to unfair outcomes, resulting in reputational and legal implications

Reverse Engineering
Exposed AI models create a gap for reverse engineering that can result in stolen or attacked critical systems

Data Manipulation
Manipulation of training data can lead to distorted AI results, outcome biases, and damaged business insights

Risks associated with Incident Response Tools using GenAI



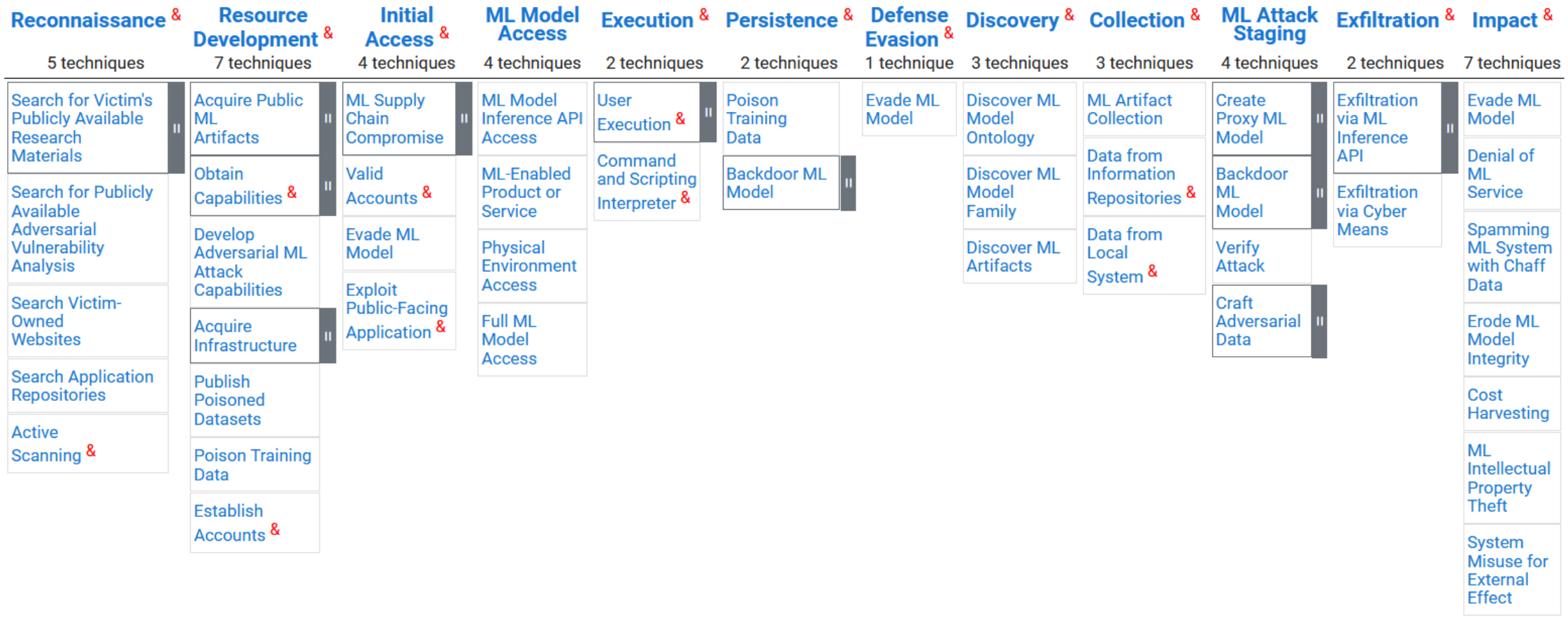
Misleading “help”
Overlooking certain attack patterns or prioritize benign activities that seem like past attacks, creating blind spots in threat detection.

Dependence on AI without Human Oversight
Over-reliance on AI in SIEM solutions may reduce the role of human analysts, potentially leading to critical security issues being missed.

Missing Company Context
AI models can make mistakes or fail to understand complex attack patterns, and without proper human oversight, attackers could exploit this to their advantage.

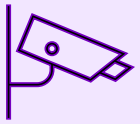
MITRE ATLAS

- **Adversarial Threat Landscape for Artificial-Intelligence Systems**



Source: https://atlas.mitre.org/

Concerns And Mitigations Summary

Theme	Mitigation strategies
 **Impersonation**	• **Strengthen your threat protection/detection systems** on messaging, workplaces and IM tools • Modify your **awareness programs to integrate a focus around AI** capabilities • Adapt your **attack simulation exercises by taking into account AI** in scenarios
 **Exploitation**	• Make sure you can **cover the evolution of malware with polymorphisms** (EDR/XDR, probes/NDR, proxies, mail, etc.) • Expertise your **cyber defense teams with AI skills** (SOC analysts, incident responders, reversers, etc.) • Adjust your **qualification and analysis playbooks** with specific tools
 **Authentication**	• Activate **User Behavior Analysis** (UBA) capabilities to detect abnormal behavior (impossible location, authentication rate by applications…) • Make sure to **use strong authentications** (MFA typically) • Integrate **SOC detection scenarios based on authentication** mechanisms
 **Image reputation / Influence**	• Develop your **Cyber Threat Intelligence (CTI) capabilities** to prevent attacking attempts & targeted campaigns • Perform **table-top exercises** integrating crisis management, fact qualification, legal interactions and communication with public relations

Thank You

Any Questions?