



ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND



SYMBIO

A FAURECIA MICHELIN HYDROGEN COMPANY

How LLMs are revolutionizing the cybersecurity field ?

A focus on Threat Intelligence (TI)

Presented by Dr.-Ing. Natasha Alkhatib





Who am I

- ❑ Cybersecurity Lead at Symbio.
- ❑ Ex-cybersecurity engineer at ETAS Bosch.
- ❑ Holds a Ph.D. in AI for Automotive Cybersecurity from Institut Polytechnique de Paris.
- ❑ Specializes in AI-powered automotive cybersecurity solutions.



Agenda

- ❑ Threat Intelligence as a defensive application of LLMs
 - ❑ What is Threat Intelligence ?
 - ❑ The Threat Intelligence Lifecycle
 - ❑ LLM as part of the TI Lifecycle
 - ❑ Google Threat Intelligence with Gemini Pro 1.5
 - ❑ Beyond Threat Intelligence
- ❑ The offensive side of LLMs

Agenda

- ❑ **Threat Intelligence as a defensive application of LLMs**
 - ❑ What is Threat Intelligence ?
 - ❑ The Threat Intelligence Lifecycle
 - ❑ LLM as part of the TI Lifecycle
 - ❑ Google Threat Intelligence with Gemini Pro 1.5
 - ❑ Beyond Threat Intelligence
- ❑ The offensive side of LLMs

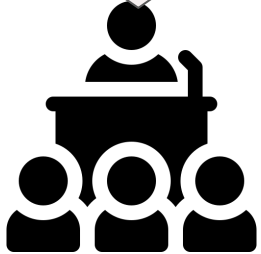
“Every battle is won before it is ever fought.”

- Sun Tzu

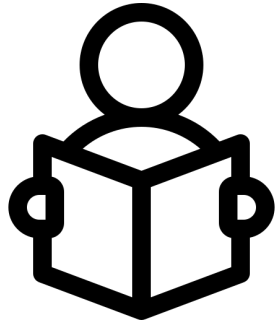
What is Threat Intelligence ?

What have you heard about **Threat Intelligence**?

Welcome to the **TI** 2024 Conference in Berlin, Germany. Today, we will discuss the following: ..



Nice report on **state-sponsored attacks**, how shall I protect my enterprise ?



TI provides external context for security decisions



Let's add **TI** to our security program!



What have you heard about **Threat Intelligence**?

Misconception



TI is just data feeds and PDF report



TI is just a research service for the incident response team



TI requires a dedicated team of high-priced, elite analysts



Then, what is Threat Intelligence ?

- ❑ Today, the cybersecurity industry faces **numerous challenges**
 - ❑ ↗ threat actors
 - ❑ ↗ false alarms
 - ❑ Shortage of skilled professionals



- ❑ Connectivity and automation revolutionizing the world
- ❑ They're also bringing ↗ **vulnerability** to cyberattacks.



Then, what is **Threat Intelligence** ?

- ❑ TI is **knowledge** that allows you to **prevent** and **mitigate** attacks on **digital systems**.
- ❑ Rooted in data, threat intelligence provides context like:
 - ❑ **Who's attacking you?**
 - ❑ What are their **motivation** and **capabilities**?
 - ❑ What **indicators of compromise** to look for in your systems?



Ok, so it helps us make **informed decisions** about our **security**.





ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND





Who can benefit from **Threat Intelligence** ?



ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND



Who can benefit from Threat Intelligence?

Team	Challenge	TI's benefits
<p>Security Operations</p> 		<p>Automatically prioritize and filter alerts and other threats.</p>
<p>Vulnerability Management</p> 	<p>Need to prioritize the most important vulnerabilities.</p>	<ul style="list-style-type: none"> • Provides access to external insights and context. • Differentiate immediate threats to their specific enterprise from merely potential threats.
<p>High-level security staff</p> 	<p>Understand the current threat landscape</p>	<p>Provides key insights on: threat actors, their intentions, targets, tactics, techniques, and procedures (TTPs).</p>

A **TI program** can produce dynamic improvements in security and operational efficiency

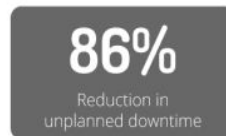
Topline Metrics



Security Operational Efficiencies



Risk Reduction



Data Source: IDC

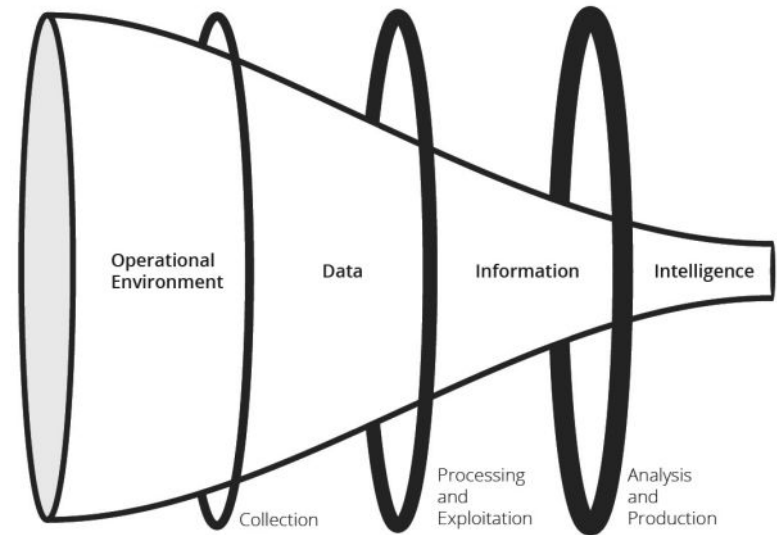


ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

Data and Information are **Not Intelligence**

Distinctions between data, information, and intelligence

- ❑ **Data** consists of discrete facts and statistics gathered as the basis for further analysis.
- ❑ **Information** is multiple data points combined to answer specific questions.
- ❑ **Intelligence** analyzes data and information to uncover patterns and stories that inform decision-making.





ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

In cybersecurity



ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND



`www.google.com`

Data



`192.168.10.10`



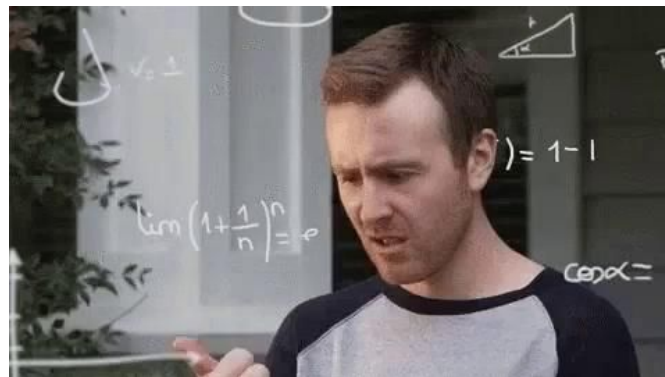
`8743b52063cd84097a65d1633f5c74f5`



ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

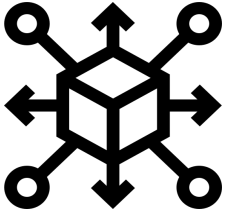
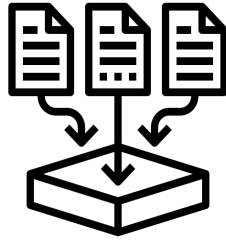
How many time has my organization been mentioned on social media this month ?

Information

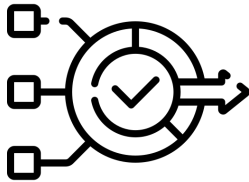
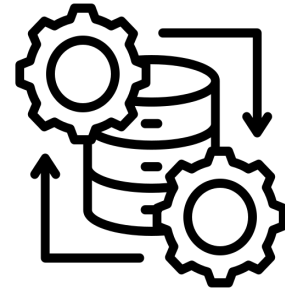




ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND



Intelligence





ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

Types of Threat Intelligence

Operational Threat Intelligence

- ❑ Also referred to as technical threat intelligence.
- ❑ Knowledge about ongoing cyber attacks, events, and campaigns.
 - ❑ Which attack vectors are being used?
 - ❑ What vulnerabilities are being exploited ?
 - ❑ What command and control domains are being employed by attackers ?
- ❑ Generally sourced from machines.
- ❑ Useful to personnel directly involved in the defense of an organization
 - ❑ System architects, administrators, and security staff.
- ❑ Source: threat data feeds
- ❑ Guides improvements to existing security controls, processes, speeds up incident response.

Strategic Threat Intelligence

- ❑ Provides a wide overview of an organization's threat landscape.
- ❑ Most helpful for informing high-level decisions
- ❑ Business-oriented
- ❑ Presented through reports or briefings
- ❑ Sources:
 - ❑ Policy documents from nation-states or nongovernmental organizations
 - ❑ News from local and national media
 - ❑ Articles in industry
 - ❑ White papers
 - ❑ Research reports

Agenda

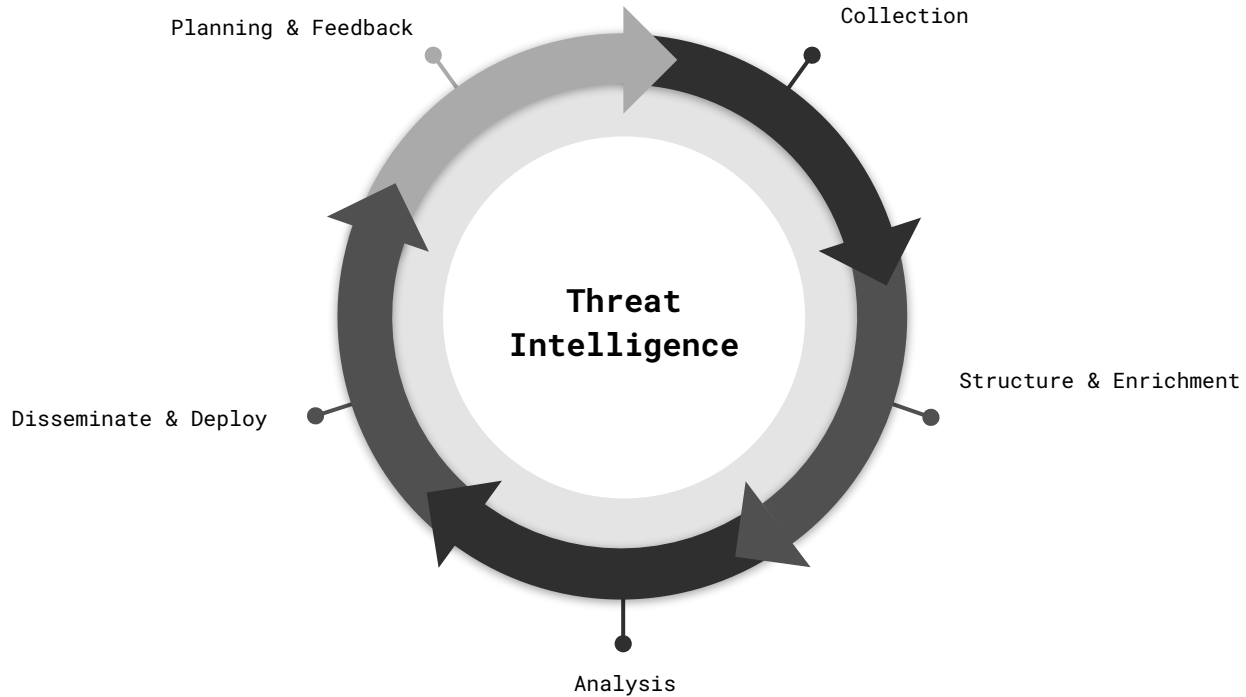
- ❑ **Threat Intelligence as a defensive application of LLMs**
 - ❑ What is Threat Intelligence ?
 - ❑ **The Threat Intelligence Lifecycle**
 - ❑ LLM as part of the TI Lifecycle
 - ❑ Google Threat Intelligence with Gemini Pro 1.5
 - ❑ Beyond Threat Intelligence
- ❑ The offensive side of LLMs

“You have to believe in your process.”

- Tom Brady

The Threat Intelligence Lifecycle

Threat Intelligence Lifecycle

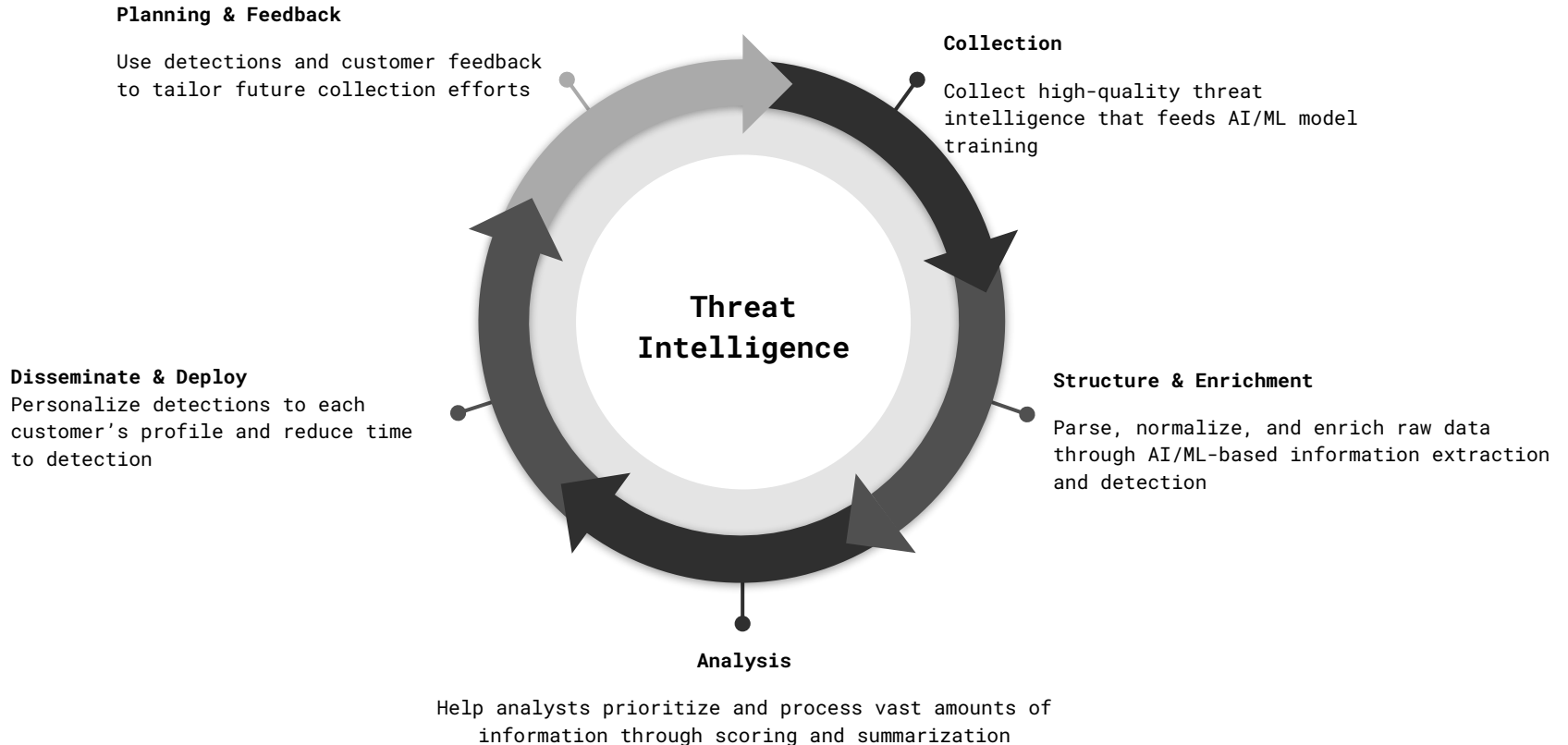


Agenda

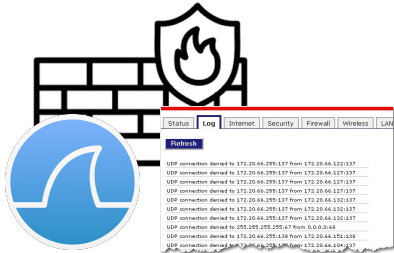
- ❑ **Threat Intelligence as a defensive application of LLMs**
 - ❑ What is Threat Intelligence ?
 - ❑ The Threat Intelligence Lifecycle
 - ❑ **LLM as part of the TI Lifecycle**
 - ❑ Google Threat Intelligence with Gemini Pro 1.5
 - ❑ Beyond Threat Intelligence
- ❑ The offensive side of LLMs



Threat Intelligence Lifecycle



- ❑ Process of gathering information to address the most important intelligence requirements
- ❑ Information gathering can occur organically through a variety of means, including:



Internal Sources



Technical Sources



Human Sources



ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

Automate more !

- ❑ **GPT-Crawler (BuilderIO):**
 - ❑ A crawler tool that integrates the capabilities of GPT-3, capable of understanding and processing complex web structures.
 - ❑ Features: Strong natural language processing capabilities, high automation, and context understanding.
 - ❑ Use Cases: Suitable for websites with complex structures and those requiring deep understanding.
 - ❑ Example: Using GPT-Crawler to scrape threat data feed blogs, automatically categorizing and summarizing content.

❑ Jina AI's reader:

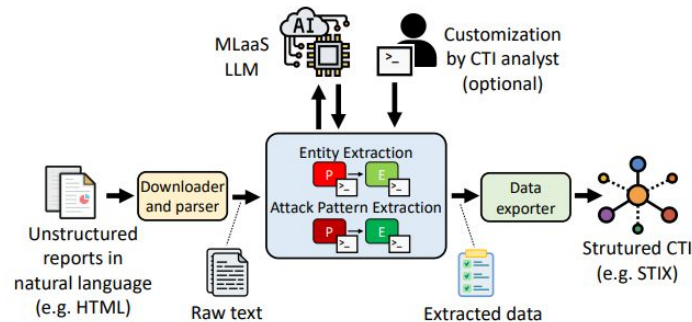
- ❑ tackles the challenges of feeding web data into language models (LLMs).
- ❑ Scraping webpages and passing raw HTML to LLMs can be complex, unreliable, and expensive due to the high volume of unwanted tokens.
- ❑ The Reader API solves this by extracting only the core content from a URL and converting it into clean, LLM-friendly text.
- ❑ This not only ensures high-quality input for your AI systems but also reduces costs by minimizing the number of tokens processed.



Structure and Enrichment

Gather Information About Threat Activity

- ❑ Processing is the transformation of collected information into a format usable by the organization.
- ❑ Different collection methods often require different means of processing.





ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

Automate more !

Prompt Extract key entities from the content of network security incidents.

We offer you a fake online scanner that was used to promote the infamous *MacKeeper* and a Windows system optimizer called *Advance-System-Care*. From a compromised website we were re-directed to [systemcheckf.jclub](#) where we got this popup: Clicking "OK" offered to start an online scan - -which claimed to find a HIGH risk virus: Thankfully these helpful people knew just the tool to remove this virus from our PC and brought us to [www.jadvancepctools.jinfo](#): Here we installed *Advance-System-Care* which did not find the virus, but nevertheless had some very important tips on how to improve the system's performance. That *Advance-System-Care* did not find the alleged virus is not surprising as *Tapsnake* is an Android infection that doesn't work on Windows machines. The site hosting the fake scanner and all the next steps in the redirection chain are blocked by *Malwarebytes Premium Web Protection* module. The installer for *Advance-System-Care* is detected as PUP.Optional.AdvanceSystemCare SHA256: 164cb18150d242e88de70b9f0e35478ab9aab8e0b723472dfdc278f6ea025da.

Answer

- Malware names: MacKeeper, Advance-System-Care, Tapsnake
- Domain names: systemcheckf.jclub, www.jadvancepctools.jinfo
- Other indicators of compromise: 164cb181...78f6ea025da

(a) GPT-3.5

Answer

- Malware: Tapsnake
- Domain Names: systemcheckf.jclub, www.jadvancepctools.jinfo
- Indicators of Compromise (IoCs): SHA256: 164cb181...78f6ea025da
- Security Products: Malwarebytes Premium Web Protection
- Misleading Software: MacKeeper, Advance-System-Care

(b) SEvenLLM

SEVENLLM : Benchmarking, Eliciting, and Enhancing Abilities of Large Language Models in Cyber Threat Intelligence

Hangyuan Ji¹, Jian Yang^{1*}, Linzheng Chai¹, Chaoren Wei¹, Liqun Yang¹, Yunlong Duan¹, Yunli Wang¹, Tianzhen Sun¹, Hongcheng Guo¹, Tongliang Li¹, Changyu Ren¹, Zhoujun Li¹

¹State Key Laboratory of Complex & Critical Software Environment, Beihang University
 {jhy_1,jiaya, challenging, weichaoren, lqyang, tonyliangli, cyren, lizj}@buaa.edu.cn;

Source: <https://arxiv.org/pdf/2405.03446>

Task Name	Task Description
Key Entity Recognition	Identify the main entity information in the text, such as attacker organization, victim type, main person, the common vulnerabilities
Main Relation Extraction	Extract the relationships between major entities such as attacker, victim, attack method and so on. Through relationship extraction, connections between entities can be established to help cybersecurity experts better understand the content and context of threat intelligence.
Important Event Extraction	Key information such as the type, time, location, and impact of the event can be identified through critical event extraction
Attack Tool Identification	Tools and toolchains utilized in the attack are identified and extracted
Domain Intelligence Acquisition	Domain names often involve information about phishing sites and locations, obtaining the domain name used by the attacker to look for potential relevance.

Vul-RAG: Enhancing LLM-based Vulnerability Detection via Knowledge-level RAG

Xueying Du
Fudan University
China

Geng Zheng
Alibaba Group
China

Kaixin Wang
Fudan University
China

Jiayi Feng
Fudan University
China

Wentai Deng
Nanjing University
China

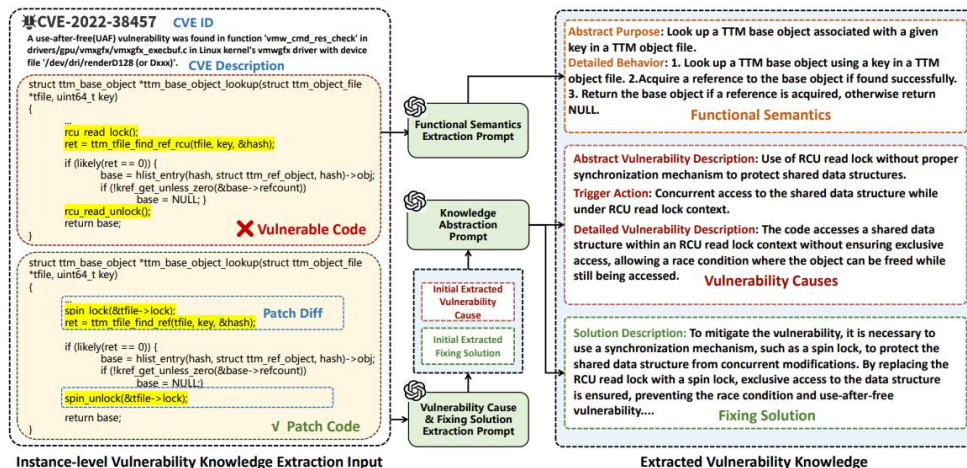
Mingwei Liu
Sun Yat-sen University
China

Bihuan Chen
Fudan University
China

Xin Peng
Fudan University
China

Tao Ma
Alibaba Group
China

Yiling Lou
Fudan University
China



Source: <https://arxiv.org/pdf/2406.11147>

- ❑ Process that turns processed information into intelligence that can inform decisions.
- ❑ Decisions might involve:
 - ❑ Investigate a potential threat?
 - ❑ What actions to take immediately to block an attack.
 - ❑ How to strengthen security controls?
 - ❑ How much investment in additional security resources is justified?
- ❑ The form in which the information is presented is especially important.
- ❑ It is useless and wasteful to collect and process and then deliver it in a form that can't be understood and used by the decision maker.



ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

Automate more !



Task Name	Task Description
Attack Means Analysis	Analyze the means and specific methods used in attacks during cybersecurity incidents
Attack Strategy Analysis	Analyze the attacker's tactics, attack plan, or usual methods in a cybersecurity incident.
Correlation Analysis	Analyze the connections and correlated evidence between different threat intelligence reports and cybersecurity incidents.
Attack Tool Identification	Tools and toolchains utilized in the attack are identified and extracted
Attack Intent Analysis	Analyze the attacker's potential motivation, intent, target industry, or target area.

Source: <https://arxiv.org/pdf/2405.03446>

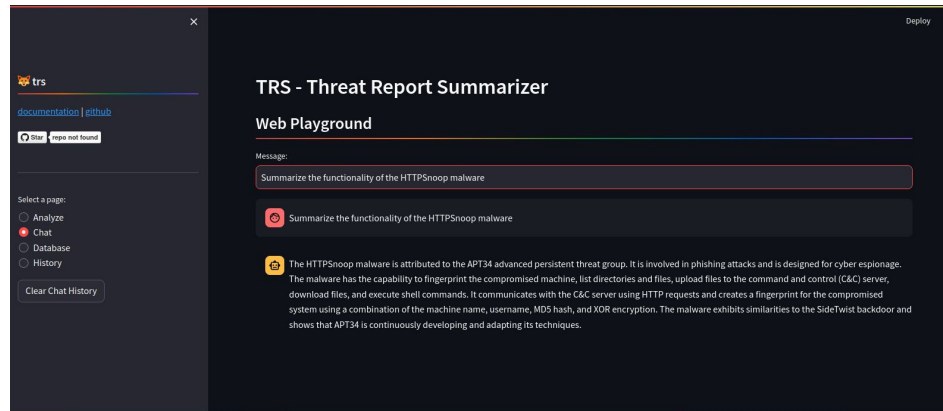
- Goal: Merge a new group either into an existing group once the link can be proven, or to graduate it to its own group if we are confident it represents a new and distinct actor set.

How similar are these groups?

UNC333		UNC501	
Known Aliases: Guccifer 4.0 Casual Bear	Methods: Spear Phishing:1 Powershell: 13 DLL Side-Loading: 3	Known Aliases: PrettyGorilla ATOD SuperSoft	Methods: Spear Phishing:15 SQL Injection:12 Sticky Keys:8
Malware: SWEETFACE: 26 FORKNIFE: 12	Target Countries: USA:12 UK:1 Germany:24	Malware: Sogu:7 XtremeRAT:13 MyDoom:10	Target Countries: USA:5 Macedonia:1 Iceland:24
Target Industries: Gov/Mil: 6 Crafting: 14 Aviation: 7	Infrastructure: TK: 8 CA: 2 UG: 23	Target Industries: Tech:6 Crafting:20 Nuclear Power:4	Infrastructure: FR:8 DE:2 TK:23

Source: <https://cloud.google.com/blog/topics/threat-intelligence/clustering-and-associating-attacker-activity-at-scale>

- ❑ trs leverages OpenAI and ChromaDB to analyze and chat with cyber threat intelligence reports and blogs.
- ❑ Supply a threat report URL to pre-built commands for summarization, MITRE TTP extraction, mindmap creation, and identification of detection opportunities, or run your own custom prompts against the URLs text content.



Source: <https://github.com/deadbites/trs>

- ❑ Dissemination involves getting the finished intelligence output to the places it needs to go.
- ❑ Strategic threat intelligence via analyst-curated reports and threat graph insights
- ❑ Tactical intelligence is converted to machine-readable data (MRTI) and signatures for immediate use by customers and partners.
- ❑ Personalize the threat intelligence to the needs of each customer by recommending relevant intelligence and customize scoring based on each customer's threat profile (e.g., industry, geographic region, vulnerabilities).

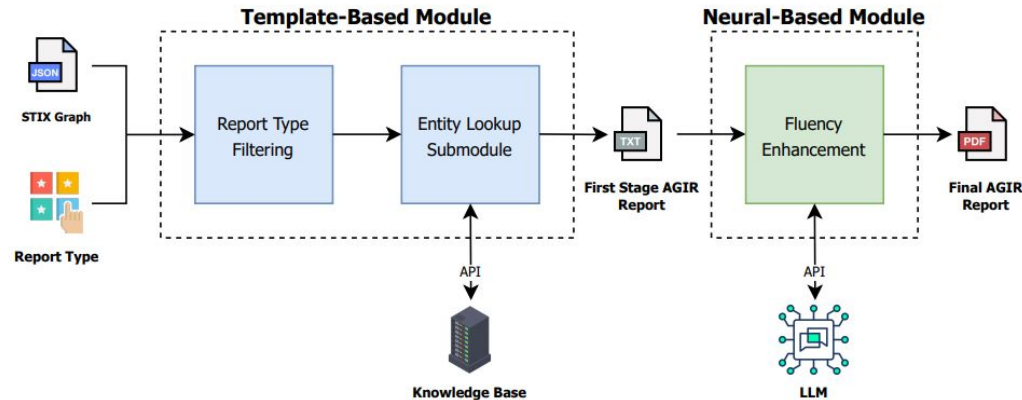


ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

Automate more !

Threat Intelligence Reporting with LLM

AGIR: Automating Cyber Threat Intelligence Reporting with Natural Language Generation



Source: <https://arxiv.org/pdf/2310.02655>

- ❑ The high-quality data about threat actors and their TTPs is used directly to train the AI technologies used throughout the Threat Intelligence Lifecycle, which leads
 - ❑ Improved detections
 - ❑ Better intelligence collection over time.

- ❑ Feedback from customers, both from explicit and implicit feedback mechanisms ensures that the intelligence collections are aimed at those threats that matter most to the customers.

Agenda

- ❑ **Threat Intelligence as a defensive application of LLMs**
 - ❑ What is Threat Intelligence ?
 - ❑ The Threat Intelligence Lifecycle
 - ❑ LLM as part of the TI Lifecycle
 - ❑ **Google Threat Intelligence with Gemini Pro 1.5**
 - ❑ Beyond Threat Intelligence
- ❑ The offensive side of LLMs



The screenshot shows the Google Threat Intelligence search interface. At the top, the Google Threat Intelligence logo is displayed. Below it, the text "Examine CVEs and stay ahead of cyber threats" is shown, with "TTPs" written below "CVEs". A search input field contains the hash "55d8b1951e1ce8b3aea07ee3a3fb9f0e8f0cd345d08096806ddad9a6691510ec". To the right of the input field are "Choose file" and "Search" buttons. Below the search bar are three buttons: "My Threat Profiles", "IoC Collections", and "Mandiant Reports". At the bottom, a link is provided: "Do you want to learn more about GTI search capabilities? Check our [Documentation](#), or automate submissions using the [API](#)".



- ❑ Gemini 1.5 Pro offers the world's longest context window, with support for up to [1 million tokens](#).
- ❑ It was able to process the entire decompiled code of the malware file for [WannaCry in a single pass](#), taking 34 seconds to deliver its analysis and identify the killswitch.
- ❑ Gemini-driven entity extraction tool :
 - ❑ It can automatically crawl the web for relevant open source intelligence (OSINT)
 - ❑ It can classify online industry threat reporting.
 - ❑ It then converts this information to knowledge collections, with corresponding hunting and response packs pulled from motivations, targets, tactics, techniques, and procedures (TTPs), actors, toolkits, and Indicators of Compromise (IoCs).



Agenda

- ❑ **Threat Intelligence as a defensive application of LLMs**
 - ❑ What is Threat Intelligence ?
 - ❑ The Threat Intelligence Lifecycle
 - ❑ LLM as part of the TI Lifecycle
 - ❑ Google Threat Intelligence with Gemini Pro 1.5
 - ❑ **Beyond Threat Intelligence**
- ❑ The offensive side of LLMs



Beyond Threat Intelligence

- ❑ Audit:
 - ❑ [chatgpt-code-analyzer](#) - ChatGPT Code Analyzer for Visual Studio Code

- ❑ Offensive:
 - ❑ [PentestGPT](#) - A GPT-empowered penetration testing tool
(Source:)

- ❑ Reverse Engineering:
 - ❑ [LLM4Decompile](#) - Reverse Engineering: Decompiling Binary Code with Large Language Models

Agenda

- ❑ Threat Intelligence as a defensive application of LLMs
 - ❑ What is Threat Intelligence ?
 - ❑ The Threat Intelligence Lifecycle
 - ❑ LLM as part of the TI Lifecycle
 - ❑ Google Threat Intelligence with Gemini Pro 1.5
 - ❑ Beyond Threat Intelligence
- ❑ **The offensive side of LLMs**

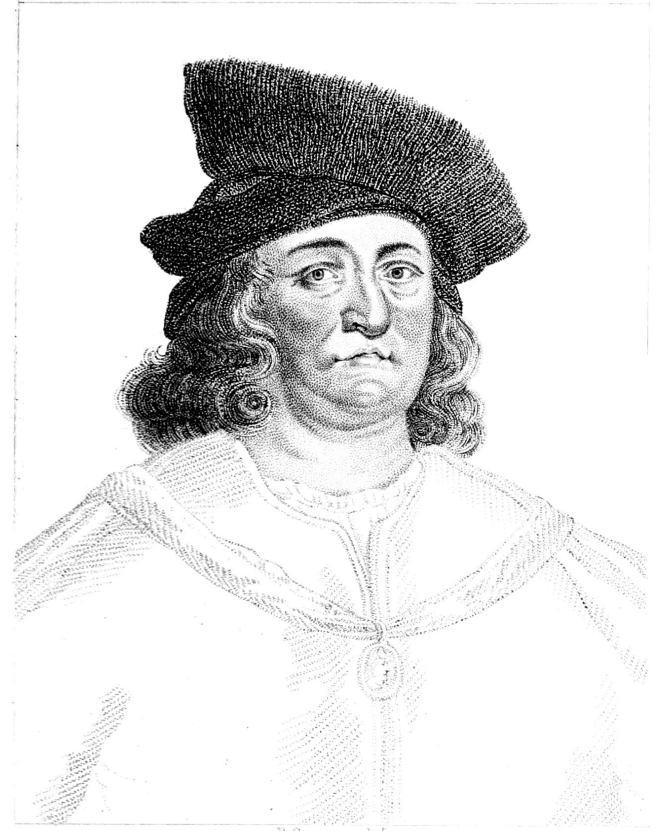


ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

Poison is in everything, and nothing is without poison.

The **dosage** makes it either a **poison** or a **remedy**.

- PARACELSUS



Adversarial application of LLMs

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (3)	Abuse Elevation Control Mechanism (3)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (3)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (3)	Compromise Infrastructure (3)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Hijacking (2)	Automated Collection	Content Infiltration	Data Manipulation (2)	Data Removal
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (3)	Deobfuscate/Deocode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (3)	Browser Session Hijacking	Data Encoding (2)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (4)	Establish Accounts (2)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Boot or Logon Initialization Scripts (3)	Deploy Container	Forge Web Credentials (2)	Cloud Service Object Discovery	Replication Through Removable Media	Clipboard Data	Data Obfuscation (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (3)	Direct Volume Access	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Dynamic Resolution (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)	Stage Capabilities (3)	Supply Chain Compromise (3)	Scheduled Task/Job (3)	Create or Modify System Process (3)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Modify Authentication Process (2)	Debugger Evasion	Taint Shared Content	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Financial Theft	Firmware Corruption
Search Open Websites/Domains (3)	Valid Accounts (4)	Trusted Relationship	Serverless Execution	Event Triggered Execution (17)	Escape to Host	Execution Guardrails (2)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (4)	Fallback Channels	Exfiltration Over Web Service (4)	Inhibit System Recovery	Network Denial of Service (2)
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Event Triggered Execution (17)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Hide Infrastructure	Ingress Tool Transfer	Scheduled Transfer	Resource Hijacking (4)
			Software Deployment Tools	Hijack Execution Flow (13)	Exploitation for Privilege Escalation	Hijack Execution Flow (13)	Network Sniffing	File and Directory Discovery	Group Policy Discovery	Data from Local System	Multi-Stage Channels	Transfer Data to Cloud Account	Service Stop
			System Services (2)	Implant Internal Image	Hijack Execution Flow (13)	Impair Defenses (11)	OS Credential Dumping (3)	Log Enumeration	Log Enumeration	Data from Network Shared Drive	Non-Application Layer Protocol	System Shutdown/Reboot	
			User Execution (3)	Modify Authentication Process (2)	Process Injection (12)	Impersonation	Steal Application Access Token	Network Service Discovery	Network Service Discovery	Data from Removable Media	Non-Standard Port		
			Windows Management Instrumentation	Office Application Startup (3)	Indirect Command Execution	Indicator Removal (13)	Steal or Forge Authentication Certificates	Network Share Discovery	Network Sniffing	Data Staged (2)	Protocol Tunneling		
				Power Settings	Pre-OS Boot (3)	Modify Authentication Process (2)	Steal Web Session Cookie	Password Policy Discovery	OS Credential Dumping (3)	Email Collection (3)	Proxy (4)		
				Scheduled Task/Job (3)	Scheduled Task/Job (3)	Modify Cloud Compute Infrastructure (2)	Unsecured Credentials (3)	Peripheral Device Discovery	Steal or Forge Kerberos Tickets (5)	Input Capture (4)	Remote Access Software		
				Server Software Component (3)	Traffic Signaling (2)	Modify Cloud Resource Hierarchy		Permission Groups Discovery (3)	Steal Web Session Cookie	Screen Capture	Traffic Signaling (2)		
								Process Discovery	Unsecured Credentials (3)	Video Capture	Web Service (3)		
								Query Registry					
								Remote System Discovery					
								Software Discovery (1)					

<https://attack.mitre.org/matrices/enterprise/#>

How LLMs are revolutionizing the cybersecurity field - Dr.-Ing. Natasha Alkhatib



ML in PL
CONFERENCE 2024
7 - 10 NOVEMBER / WARSAW, POLAND

Thank you

