Anomali Lens

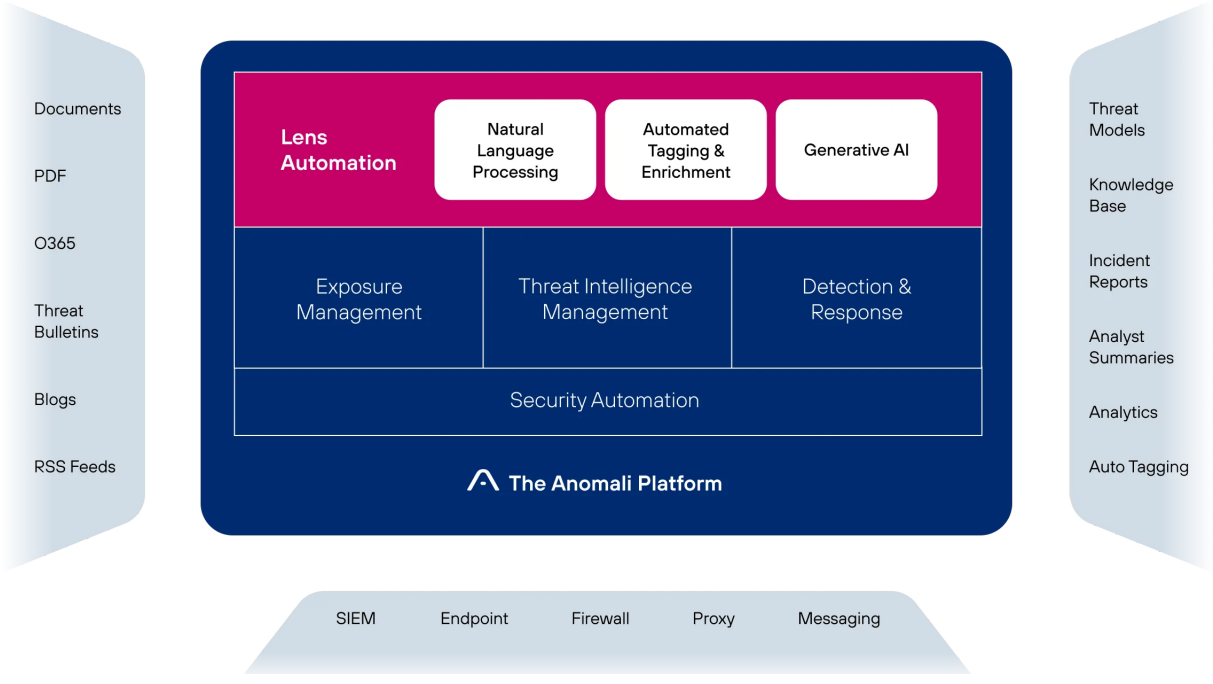
Artificial intelligence has the potential to change the way security analysts work. It can also transform the communication interface between security operations and the business. By embedding AI within The Security Operations Platform, Anomali elevates analyst experience and operational efficiency.

Anomali's use of AI extends across the human-machine interface, leveraging natural language processing (NLP) capabilities to transform human-generated data into machine readable information and converting machine generated data to human consumable insights with natural language generation (NLG). Anomali transforms and scales security operations with the power of AI embedded within The Platform.

BENEFITS

- Go from unstructured data to actionable intelligence in seconds with natural language processing.
- Automatically enrich intelligence with actors, vulnerabilities, industries, and more.
- Transform machine data into executive and analyst insights with natural language generation.
- Accelerate and simplify threat hunting with intelligence context and natural language interface.
- Automate time-consuming manual processes to increase analyst productivity.
- Improve cross-functional communication and collaboration.

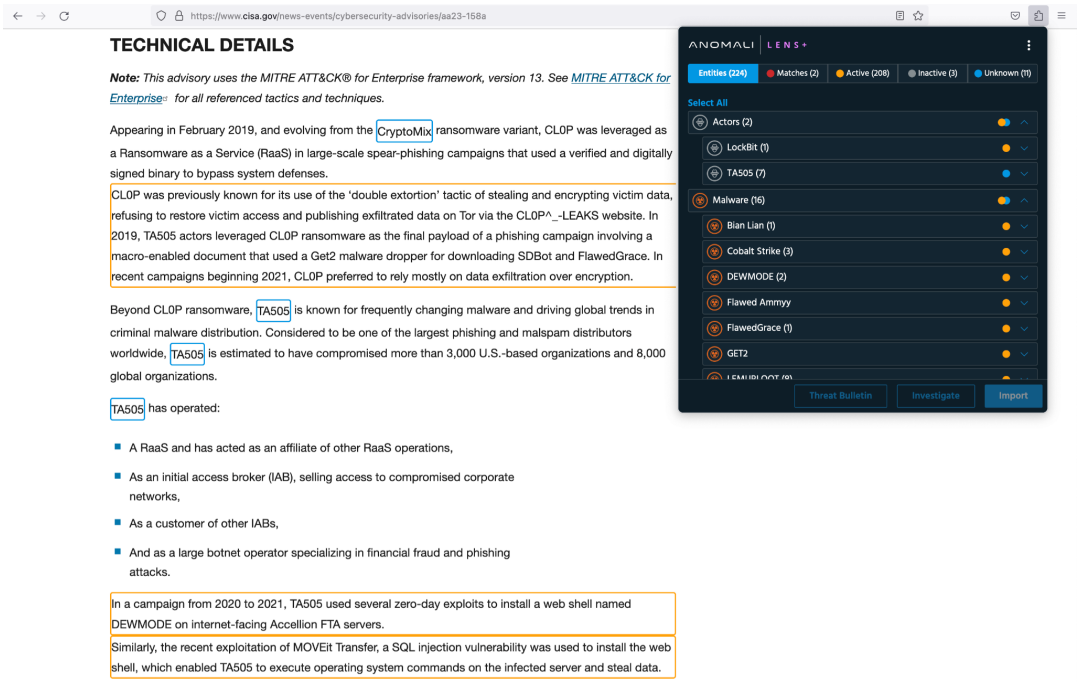
Anomali's architecture automatically correlates telemetry with external threat data at AI speeds



Natural Language Processing

Unstructured threat intelligence is a vital resource for analysts and executives. However, ingesting and interpreting this data at volume for relevant information can be arduous and time-consuming. This is especially important during significant events, such as a new cyberattack or data breach.

Anomali Lens includes a powerful Natural Language Processing engine that helps operationalize threat intelligence by automatically scanning digital content (PDF, HTML, Office 365 - Word, Excel, Outlook) to identify relevant threats and streamline the lifecycle of researching and reporting. Available as a browser extension or Office 365 plug in, Lens automatically highlights information that matters in news articles, threat bulletins, social media, research papers, blogs, coding repositories, and internal content sources, then helps analysts quickly capture the full significance and context of a threat, and action it across the organization to reduce risk. Executives can gain immediate context for online cyberattack reports with one-click visibility into their organizations current posture.

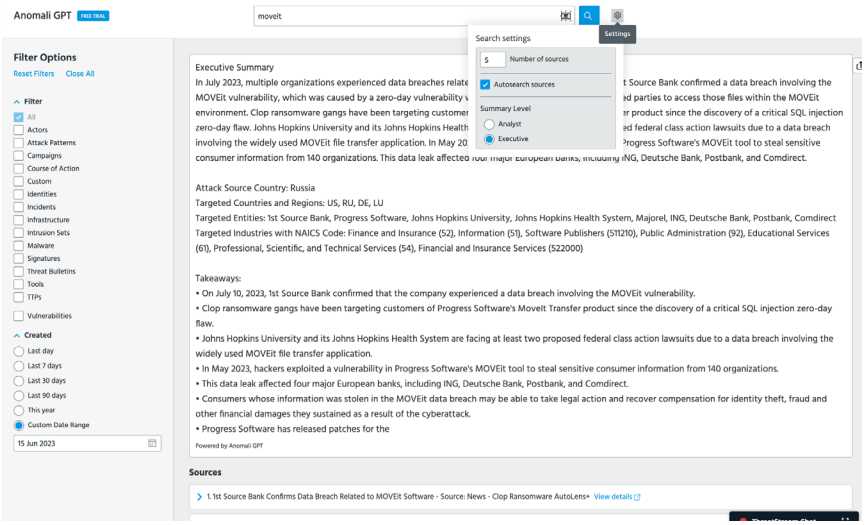


Automatically scans digital (PDF, HTML, OFFICE 365. etc.) content to identify relevant threats and streamline researching and reporting on them.

Natural Language Generation

Data is the essence of modern security, and includes logs from various security sources, threat intelligence, incidents, vulnerabilities, and more. Most security initiatives are overwhelmed with data and often lack context for real-time decisioning. Anomali leverages Generative Pretrained Transformer (GPT) to convert the troves of data into human consumable actionable insights.

The Anomali GPT capability is a private model of GPT, built on the world's largest repository of curated threat intelligence. It automatically summarizes critical events across multiple sources of information, enriching it with Anomali curated intelligence to inform executives and analysts of the key takeaways and business risks associated with threat events. It also automatically enriches intelligence with tags and associations for actors, malware, MITRE TTPs, countries, industries, vulnerabilities, and more. Summarize threat models, search the knowledge-base, hunt for threats, generate executive summaries of news, and more using natural language with Anomali GPT.



Automatically generate executive and analyst summaries to improve cross-team communications and accelerate analyst workflows

KEY CAPABILITIES

- **Extract intelligence:** Transform unstructured data from different - sources blogs, threat bulletins, Office 365, etc. into intelligence in seconds with natural language processing. Recognize and tag MITRE ATT&CK TTPs to identify and associate actor insights.
- **Curated intelligence:** Go from traditional RSS feeds into curated and enriched high-quality RSS feeds with GPT-generated executive summaries and takeaways with AutoLens+. Feeds include Bleeping Computer, CISA Advisories, InfoSecurity Magazine and many more.
- **Automate enrichment:** Automatically add tags and associations to the intelligence for actors, countries, industries, vulnerabilities and more with AutoLens+, translating technical indicators into business risk.
- **Operationalize intelligence**: Automate IOC import into Threat Bulletins, Investigations, and Sandbox detonation, as well as report creation to export investigations as finished intel.
- **Derive insights:** Deliver customizable dashboards for identified news on trending malware, CVEs, actors, and more.
- **Summarize & collaborate:** Quickly summarize information for critical events from multiple sources using GPT / Generative AI to inform the executives and drive quick action.
- **Accelerate the hunt:** Go from bulletins to hunt for adversary footprints in your environment in one click. Hunt years of data in seconds.
- **Search with natural language:** Store petabytes of data inexpensively in a cloud-native scalable data lake and search it in seconds with ease using natural language.

Key Use Cases

GAIN ACCESS TO INTELLIGENCE FROM UNSTRUCTURED DATA SOURCES

Scan phishing emails, malicious email addresses, URLs, and hashes from a source threat bulletin, blog, Office 365, pdf, or a website.

OPERATIONALIZE MITRE ATT&CK

Automatically associate ingested intelligence with scanned and imported techniques with MITRE ATT&CK IDs, then export to an investigation at the click of a button.

DERIVE BUSINESS RISK INSIGHTS FROM INTELLIGENCE

Automatically tag and associate new intelligence with actors, countries, industries, vulnerabilities, etc. to identify business risk and prioritize response actions.

HUNT FOR ACTIVE THREATS

One-click to determine whether a scanned threat indicator or TTP is seen in your environment, scanning years of data in seconds.

GENERATE INCIDENT REPORTS

Create professional-quality reports to inform threat detection, response, and remediation efforts as well as management.

CROSS-FUNCTIONAL COLLABORATION AND DECISIONING

Quickly condense information from multiple sources of intelligence into shareable summaries to inform.

REDUCE ANALYST FATIGUE

Automate repetitive tasks, including intelligence extraction and analysis, incident investigations, report generation, and executive communications.

	LENS	LENS+	AUTOLENS+	GPT
THREAT ENTITY SCANNING AND IDENTIFICATION				
Scan web pages to identify threat entities	✔	✔		
Scan web product consoles and reports	✔	✔		
Scan MS O365 documents (Outlook, Word, Excel)		✔		
Scan PDF documents		✔		
Auto-scan web pages		✔		
Scan and auto curates RSS feeds for intelligence				✔
THREAT ENTITY STATUS, RELEVANCE AND TAGGING				
Highlight and tooltip entities within scanned assets	✔	✔		
One-click pivot to hunt for threat entities with Security Analytics	✔	✔		
One-click pivot to view threat entity details in ThreatStream	✔	✔		
MITRE ATT&CK TTP highlighting		✔		
Automate tagging countries, industries, actors, vulns, MITRE TTP, etc.			✔	
ANALYSIS AND USE				
Provide GPT summaries for RSS feeds			✔	
Condense multiple news articles into exec and analyst smmaries				✔
Import threat entities into ThreatStream		✔		

	LENS	LENS+	AUTOLENS+	GPT
Create or update investigations		✔		
Detonate URLs in a sandbox		✔		
Create threat models from intelligence sources*				✔
Hunt with natural language				✔
Knowledge-base search				✔
USAGE				
Page Scans	100	Unlimited		
Users	Unlimited	Unlimited	Unlimited	Unlimited
Ingestion	None	Unlimited	??	??
DEPLOYMENT				
Browser extension (Chrome, Firefox, MS Edge)	✔	✔		
IT deployed plugin (Chrome, Firefox, MS Edge) Microsoft O365 plugin	✔	✔		
Anomali Platform UI		✔	✔	✔

ANOMALI