CyberProof®
A UST Company

The road to 10x improvement in security operations with generative AI

Contents

Introduction

Cybersecurity is one arena where generative AI (GenAI) is likely to have a huge impact – with both cyber offensive and defensive implications.

On the offensive side, AI-implemented attacks are becoming more widespread and sophisticated, increasing the risk to every type of organization. AI-implemented attacks refer to the use of artificial intelligence technologies for malicious purposes, such as cyberattacks, fraud, and disinformation campaigns. While AI-implemented attacks have been in existence for a decade already, there are certain capabilities that are emerging only now.

At the same time, **on the defensive side**, GenAI is being applied to security operations in ways that will revolutionize the field of cyber defense. With its ability to create new content that is barely distinguishable from human-created content, GenAI opens up new possibilities that are having a radical impact on every aspect of security operations – people, processes, and technologies.

OFFENSE

AI is used for malicious purposes, including:

- AI-implemented cyberattacks
- Cyber fraud
- Disinformation campaigns

DEFENSE

AI is transforming SecOps, with:

- AI-powered threat hunting
- Dynamic incident response
- Security platform integration

GenAI is rapidly transforming security operations

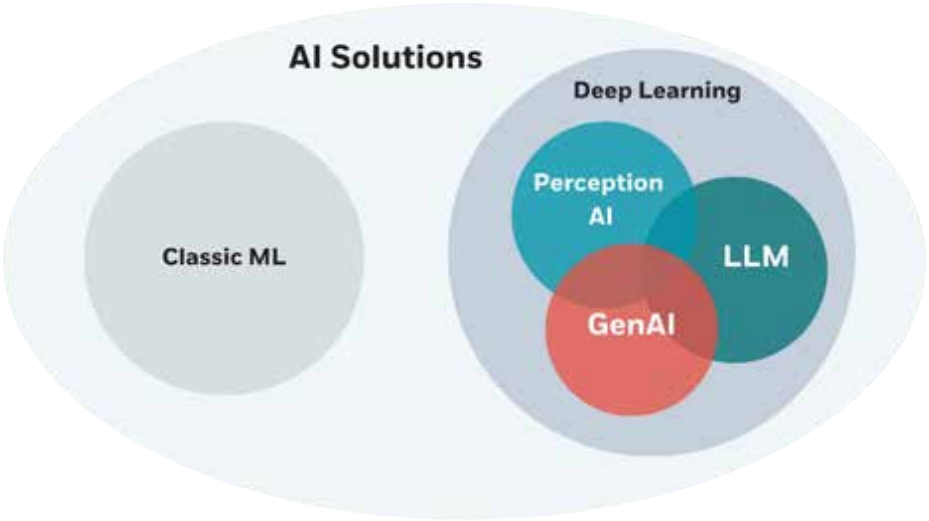
GenAI's ability to process, analyze, and learn from vast amounts of security data is quickly changing how security operations teams implement incident detection and response. Together with predictive AI, these technologies have opened the door to:

- **AI-powered threat hunting** – Hunters can use GenAI to expand their threat hunting capabilities. AI-powered tools can generate hunting queries more easily and process data at breakneck speeds. As a result, complex queries that once took hours to process can be analyzed in mere seconds, and detection time is exponentially decreased. Moreover, GenAI's summarization abilities are significant in helping threat hunters deal with the overflow of data.
- **Dynamic incident response** – GenAI has had a remarkable impact on dynamic incident response and playbook creation. GenAI can adapt each response, so that it matches the unique nature and severity of each incident.
- **Security platform integration** – GenAI has many applications in Security Orchestration, Automation & Response (SOAR) platforms. These include threat intelligence generation, anomaly detection, synthetic data generation, phishing defense, employee training, and automated security policy generation. Moreover, GenAI's impact extends beyond technology shifts to improve the human side of cybersecurity.

This eBook explores the key applications of GenAI in security operations, and how these shifts will lead to exponential benefits for organizations.

Super-charged threat hunting

A combination of Large Language Models (LLMs) and machine learning (ML) can be used to automate the adoption of a proactive approach to security operations.



RELATIONSHIP BETWEEN GENERATIVE AI AND OTHER AI SOLUTIONS

GenAI enters the picture with its capabilities in automating hunting query development. These queries can facilitate real-time threat detection, and can be fine-tuned to recognize complex cyber threat signatures that are difficult to identify manually.

Moreover, the scalability of GenAI technology enables its effective application within complex IT environments. At CyberProof, we believe GenAI will play an increasingly significant role in threat hunting as the technology continues to progress. We envision GenAI as an essential tool in malware signature recognition and malware behavior analysis.

Dynamic incident response

Integrating GenAI into dynamic incident response and playbook creation will result in a significant improvement in efficiency, effectiveness, and personalization of security management. This will ultimately minimize the impact of security incidents on an enterprise's operations.

GenAI mitigates the gap between security specialists, who are proficient in security analysis, and developers, who have expertise in writing code. GenAI can act as a "translator" and give analysts the ability to produce code based on their own knowledge.

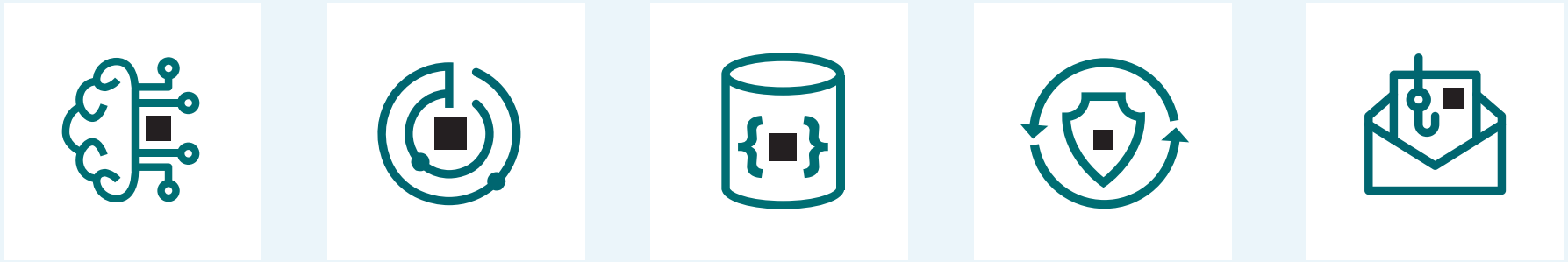
Moreover, GenAI tailors its responses based on each incident's characteristics and severity – and this allows SecOps teams to adopt more focused and successful strategies. For example, SecOps teams can leverage GenAI for:

- **Triage** – Prioritizing incidents based on their potential consequences – so that resources are utilized where they can have the greatest business impact.
- **Recommended actions** – Customizing recommendations for remediation actions that consider the specific threat, affected systems, and available resources of an organization. ML capabilities ensure that these customized recommendations evolve with each subsequent incident that is handled.
- **Red team/blue team training** – Enhancing the training of incident response teams by simulating realistic practice scenarios. This experience translates into better preparedness and helps create a more resilient organization.

Security platform integration

GenAI will integrate with Security Incident & Event Management (SIEM), Endpoint Detection & Response (EDR), and SOAR platforms, to optimize and automate security workflows, reducing the risk of false positives and human error. By automating routine tasks, GenAI allows security teams to focus on more complex and strategic tasks - leading to more efficient use of resources. In contrast to human analysts, GenAI has the advantage of performing tasks around the clock without getting alert fatigue or taking breaks.

The areas in which GenAI is expected to cause a significant disruption include:



AREAS WHERE GENAI IS EXPECTED TO CAUSE A SIGNIFICANT CHANGE

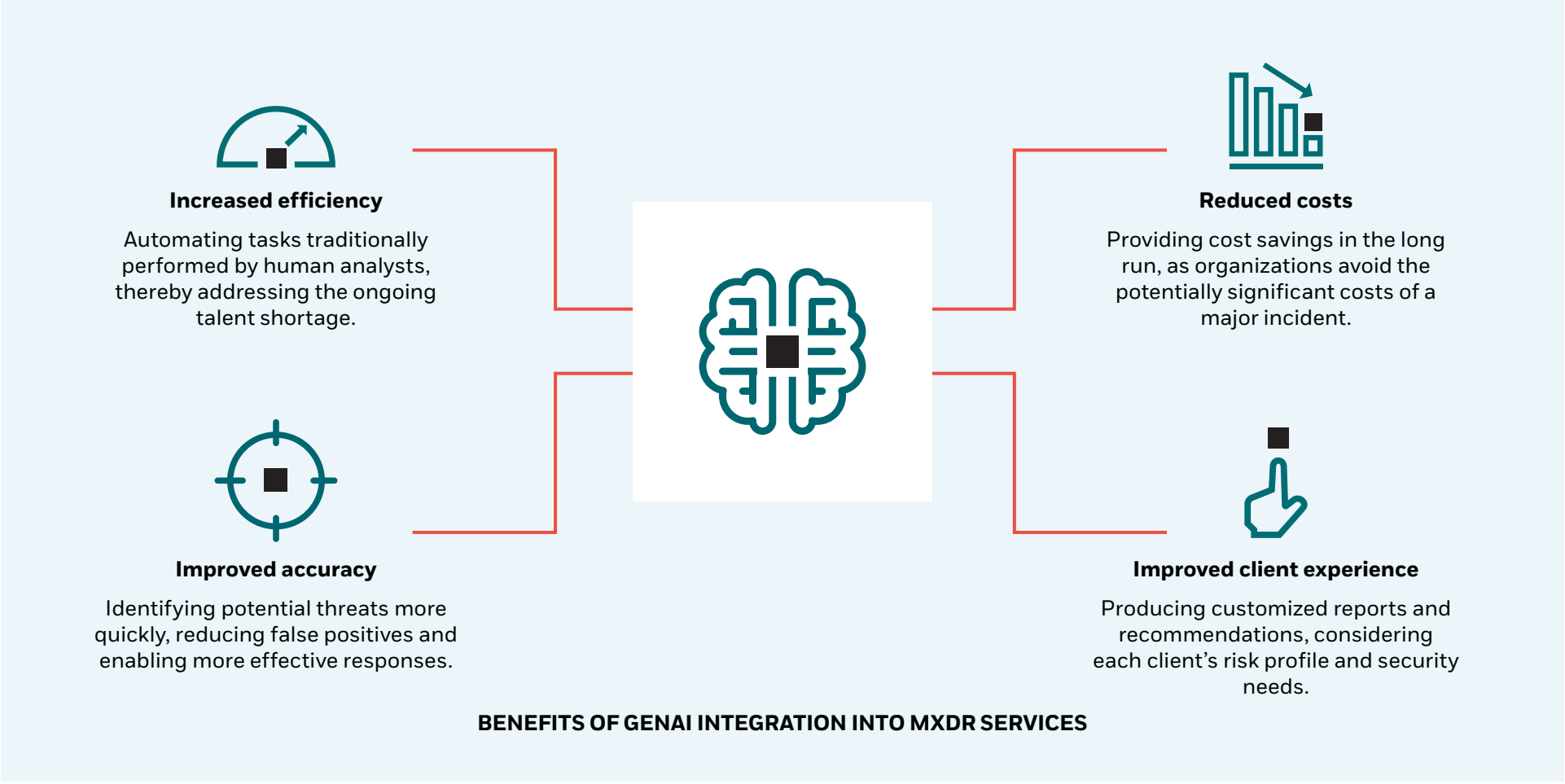
Area of activity	Impact of GenAI
Threat intelligence generation	GenAI will summarize threat data from various sources, helping analysts identify patterns and trends, and generating actionable intelligence to help enterprises pre-emptively strengthen their defenses. This proactive approach will provide a better understanding of the threat landscape and allows enterprises to be a step ahead.
Enhanced anomaly detection	GenAI can be used to facilitate better anomaly recognition - by "enriching" the pool of normal and abnormal user behaviors already available, for users, systems, and network traffic. Deviations from these models can then be quickly identified as anomalies, i.e., possibly indicating a security incident. By establishing clear baselines of what normal behavior looks like, threats can be detected faster, with fewer false positives.
Synthetic data generation	GenAI will produce synthetic data that mimics real network traffic or user behavior data. This data can be used to train ML models for threat detection without the risk of exposing sensitive information. This will be particularly useful when real data is scarce or sensitive. The synthetic data will be used to improve the accuracy of threat detection models and to test the effectiveness of different security measures.
Automated generation of internal security policy	GenAI will generate customized cybersecurity playbooks based on the unique characteristics and requirements of each enterprise that can then undergo human review and testing. Once approved, these policies will be updated in real-time (and undergo further human review and testing) to adapt to evolving threat scenarios, helping ensure that security policies will always be up-to-date and reflect the changing threat landscape. In developing policies, GenAI will consider factors such as the organization's size, industry, and risk tolerance, to create customized policies that effectively address the organization's specific needs.
Phishing training	GenAI will generate realistic phishing emails for use in security awareness programs. These simulations will serve as effective tools that expose users to the sophisticated strategies employed by scammers while ensuring a safe environment for learning. Users will familiarize themselves with subtle indications of phishing attempts, such as misleading email addresses, manipulative language usage, or unexpected attachments. The combination of advanced defense mechanisms against phishing, along with training programs, will contribute to an unyielding and dynamic approach against the widespread risk posed by phishing attacks.

Note that phishing defense can also be bolstered using LLMs. This is not directly related to GenAI. A classifier LLM can fortify defense mechanisms, automatically scrutinizing and categorizing incoming emails. The classifier LLM will acquire knowledge of linguistic patterns, structures, and other nuanced indications commonly found in phishing emails to identify suspicious messages before they reach the intended recipients. By leveraging extensive datasets that incorporate both legitimate emails and phishing attempts, the classifier LLM can accurately discern between the two categories with remarkable precision and anticipate emerging tactics employed by hackers based on observed trends.

How enterprises can benefit from GenAI

Enterprises working with GenAI-driven service providers will benefit from new types of Managed Extended Detection & Response (MXDR) services. A few examples might include more personalized reports that are tailored to the client's risk profile, highly customized security training leading to greater employee preparedness, and new security tools and solutions that leverage GenAI's ability to generate new security content and make predictions.

More broadly speaking, GenAI integration into MXDR services will provide a range of benefits that can be summarized as follows:



BENEFITS OF GENAI INTEGRATION INTO MXDR SERVICES

Leveraging Microsoft and Google AI innovation

The most significant players in the cybersecurity industry are leveraging advances in AI and LLMs to provide new, practical applications for security teams – addressing challenges such as threat overload and the talent gap. MXDR vendors are starting to leverage the AI-powered capabilities of Microsoft Security Copilot and Google Chronicle Security Operations to enhance their MXDR offerings.

Microsoft Security Copilot – which is integrated with the end-to-end Microsoft Security portfolio – uses a natural language-based investigation experience that provides step-by-step guidance and context to accelerate incident investigation and response. Using GenAI capabilities, which facilitate continuous improvement as the LLM continues to be trained, Copilot summarizes processes or events and tunes reporting – freeing up the analysts to focus on types of work that require human thought and expertise. Security Copilot runs on Azure's hyperscale infrastructure, delivering enterprise-grade security and privacy-compliant experience.

Google Chronicle uses AI-powered capabilities in threat detection, investigation, and response – simplifying complex data analysis and security engineering. Chronicle AI can generate the query, present initial information, and make it possible to modify and iterate results. Chronicle AI also speeds up investigations by pulling together and analyzing data from security events, entity insights, and behavior anomalies.

Automating digital playbooks

With the current explosion of GenAI tools, new development directions for making security operations more customized, automated, and efficient are seemingly endless. At CyberProof, for example, we are finding new ways to leverage GenAI to provide client-specific digital playbooks that can be generated automatically.

We are extending CyberProof's Use Case Factory, integrating it with new GenAI capabilities. The use case process will include customization of what each use case accomplishes for each client - and automation of triage, remediation, and recovery.

These capabilities will mean that a cybersecurity analyst who handles a threat will be able to automatically tailor the incident response process. By leveraging GenAI solutions, analysts will be able to:

- **Input English-language text,** and have it converted automatically to programming language
- **Adapt and transform generic digital playbooks,** in real time, to match the specific requirements and IT ecosystem of each client

The development of these new capabilities involves working with multiple GenAI models: integrating them as necessary, and training the models by leveraging data gleaned in our work with our own clients. CyberProof's team of AI data scientists and automation experts are involved in integrating, developing, and training the various GenAI models to automate what, until now, has been a manual and labor-intensive process.

MXDR on steroids with GenAI

Gartner views GenAI as becoming a general-purpose technology with an impact not unlike that of the steam engine, electricity, and the internet. While the hype around GenAI is likely to subside, Gartner predicts, its impact is expected to grow as people and enterprises discover more innovative applications for the technology.

MDR providers implementing GenAI into their portfolio roadmaps obtain a deeper understanding – both of cybersecurity, and of the associated benefits and risks of generative artificial intelligence. Their knowledge and experience can help organizations navigate the complexities of today's cyber threat landscape.

Outsourcing to an MXDR provider that leverages GenAI provides enterprise organizations with faster threat detection, reduced dwell time, and quicker, more effective response. Moreover, utilizing GenAI ensures that the organization's cybersecurity needs continue to be met while, at the same time, allowing internal resources to be freed up and to stay focused on their core business activities.

At CyberProof, our commitment to being GenAI-driven is inherently connected to our ongoing dedication to being at the forefront of our industry – ensuring our clients benefit from the latest and most effective security measures. By adopting GenAI-driven security practices, we also have the advantage of offering our clients customized services that are tailored to each organization's specific needs and risk profiles. These combined capabilities lead to faster, more effective threat detection & response and help mitigate the potential business risk to the enterprise.

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com.

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum

About UST

For more than 23 years, UST has worked side by side with the world's best companies to make a real impact through transformation. Powered by technology, inspired by people, and led by our purpose, we partner with our clients from design to operation. Through our nimble approach, we identify their core challenges, and craft disruptive solutions that bring their vision to life. With deep domain expertise and a future-proof philosophy, we embed innovation and agility into our clients' organizations—delivering measurable value and lasting change across industries, and around the world. Together, with over 30,000 employees in 30+ countries, we build for boundless impact—touching billions of lives in the process.

Visit us at www.UST.com

cyberproof.com