

SANGFOR SECURITY GPT

Fighting AI with The Right AI



Sangfor Security GPT: Fighting AI with The Right AI

The next battleground in cybersecurity is upon us, as attackers begin weaponizing Generative AI (GenAI) to launch more sophisticated and relentless attacks than ever before. They use it to automate phishing, create deepfakes, evade detection, and discover new vulnerabilities. These GenAI-driven threats are fast, adaptive, and often invisible to traditional security tools, leaving organizations vulnerable and struggling to keep up.

This is where Sangfor Security GPT comes in. To fight Al with Al, you need the right tools—an Al that doesn't just react but anticipates and adapts. Security GPT is that tool.

As a GenAl, it detects and neutralizes threats beyond the reach of traditional and even standard Al defenses. It continuously learns and evolves, just like the threats it's designed to counter. This ensures your security operations stay ahead, safeguarding your organization in an increasingly hostile digital landscape.



How Security GPT Bridges the Gap Between Challenges and Solutions

In today's complex digital landscape, security teams face mounting challenges. They are flooded with alerts, deal with complex threat analysis, struggle with fragmented tools, and lack skilled professionals. These issues lead to slower response times and increased risk of breaches. Security GPT expertly bridges the gap between these challenges and solutions. Here is how:

Challenges

Lack of Skilled Personnel

The cybersecurity skills gap leaves teams stretched thin, making it challenging to run effective security operations.

Complex Al-Driven Attacks

Modern cyberattacks are increasingly sophisticated and Al-driven, making them difficult to detect and analyze without equally advanced tools.

How We Resolve

Security GPT automates routine tasks and enables chat-based operations, allowing less experienced personnel to navigate complex incidents easily.

Security GPT is trained on billions of data points, enabling it to detect unseen and Al-driven threats, such as zero-day attacks and highly obfuscated malware with accuracy.

Challenges

Inconvenient and Inflexible Access to Security Data

Even with a security operations platform, rigid data presentation and report formats restrict the ability to quickly retrieve specific security data or metrics and gain a deeper understanding.

·//

Overwhelming Volume of Alerts Security teams receive thousands of alerts daily, many of which are false positives. This leads to alert fatigue and missed real threats.



Time-Consuming Investigations Without advanced tools, investigations are slow and labor-intensive, delaying threat remediation.

How We Resolve

Security GPT enables users to query security data in natural language. In just 3 seconds, it can generate text and graphical summaries of key metrics, such as the organization's security posture over the past month, top 10 critical vulnerabilities, and top 10 high-risk assets, while enabling further inquiries into the data.

Security GPT automatically analyzes all security alerts and incidents. It accurately filters out false positives, allowing your team to focus on genuine incidents.

Security GPT simplifies threat analysis by providing clear, accessible explanations. This speeds up the investigation process, allowing your team to resolve incidents quickly and effectively.

Getting to Know Security GPT In-Depth

Security GPT is a GenAl model tailored for cybersecurity. Think of it as your 24/7 virtual security analyst that enhances your team's capabilities. Powered by a state-of-the-art Large Language Model (LLM) trained on over 50 billion security data points—and continuously learning from real-world data to keep evolving in real time—it automates complex tasks like threat detection, incident response, and security optimization. Whether you're a seasoned expert or new to cybersecurity, Security GPT simplifies operations while enhancing your overall security posture.





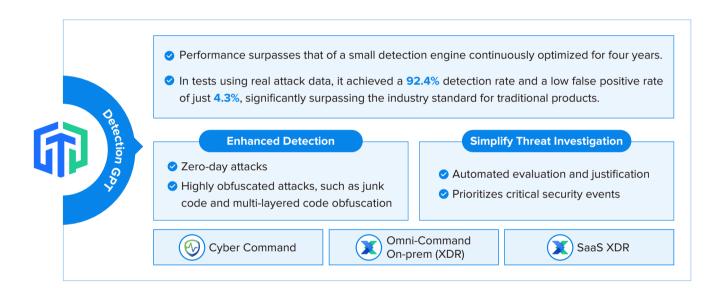
The Different Flavors of Security GPT

Detection GPT: Next-Level Precision in Threat Detection

Web Attack Detection: Trained on vast amounts of HTTP traffic, logs, and code, Detection GPT identifies web attacks with great accuracy. This makes it a critical asset in detecting advanced threats like zero-day attacks and highly obfuscated malware, which standard Al-powered tools can even miss.



Empowering Security Professionals: Explains complex threats in accessible language, reducing reliance on expert knowledge and enabling informed decision-making.

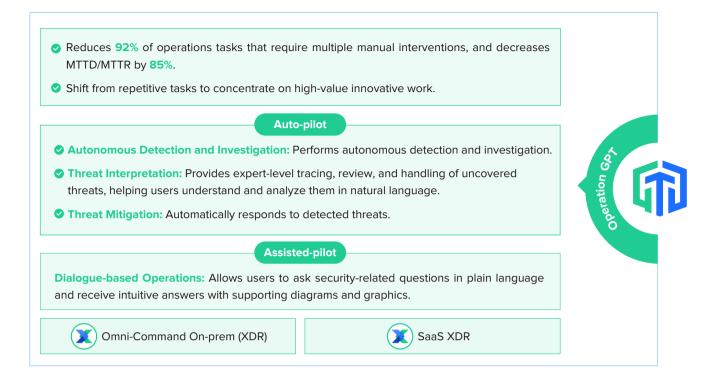


Operation GPT: Simplifying and Automating Your SecOps

Operation GPT offers two main functionalities: Assisted-Pilot GPT and Auto-Pilot GPT.

Auto-Pilot GPT: Takes over routine security tasks, autonomously detecting and investigating potential threats and providing logical explanations and evidence. Maps the entire attack path in a visual topology diagram with expert-level analysis.

Assisted-Pilot GPT: Allows interaction with the Al using natural language, simplifying the operation of security tasks. It helps interpret events, analyze alerts, and provide guidance through an intuitive, conversational interface.



Why Security GPT is The Right Al For Your Cybersecurity Needs



Enhanced Intelligence: Security GPT acts as a force multiplier for your security team, providing them with expert-level insights and recommendations that enhance decision-making. By automating routine tasks and simplifying complex analyses, it enables even less experienced team members to perform at a higher level.

24/7 Availability: Unlike human analysts, Security GPT operates around the clock, ensuring your organization's defenses are always active, even during off-hours or when your team is unavailable. This constant vigilance is crucial in today's always-on digital environment.





Proactive Defense Against Al-Driven Attacks

Advanced Threat Anticipation: As cybercriminals weaponize GenAl to develop more sophisticated and adaptive threats, Security GPT equips your organization to anticipate and counteract these attacks. Unlike reactive traditional security tools, its Al-driven capabilities enable real-time monitoring and proactive defense, detecting threats before they escalate.

Adaptive Learning: Security GPT continuously learns from new data and emerging threats, ensuring that its capabilities evolve with adversarial tactics. This keeps your organization's defenses up to date, reducing the risk of being blindsided by new attack vectors.





Streamlined Security Operations

Automation of Complex Processes: Security GPT automates labor-intensive security tasks such as threat correlation, incident management, and root cause analysis. By doing so, it frees up valuable time for your security team, allowing them to focus on more strategic initiatives like refining security policies or planning for future threats.

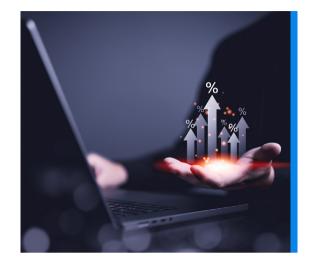
Efficiency and Speed: With Security GPT, incidents that once took hours or even days to investigate can now be resolved in minutes. Its ability to quickly analyze vast amounts of data and provide actionable insights cuts response times and improves security operations efficiency.



Long-Term Value and ROI

Cost-Effective Security Enhancement: By automating routine tasks, Security GPT lowers the operational costs associated with manual incident response and threat management. This cost efficiency, combined with its ability to enhance existing security tools, results in a strong return on investment.

Future-Proofing Your Security Posture: As cyber threats continue to evolve, adaptable and scalable security solutions have become a pressing need. Security GPT's continuous learning and integration capabilities ensure that your security posture remains strong, protecting your organization not just today, but well into the future.



SANGFOR SECURITY GPT

INTERNATIONAL OFFICES

SANGFOR SINGAPORE

10 Ubi Crescent, #04-26 Ubi Techpark (Lobby B), Singapore 408564 Tel: (+65) 6276-9133

SANGFOR HONG KONG (CHINA)

Unit 1612-16, 16/F, The Metropolis Tower, 10 Metropolis Drive, Hung Hom, Kowloon, Hong Kong Tel: (+852) 3845-5410

SANGFOR INDONESIA

Atrium Mulia 3rd Floor, Jl. H.R. Rasuna Said Kav. B 10-11 Kuningan, Setia Budi, Kecamatan Setiabudi, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12910, Indonesia Tel: (+62) 21-2168-4132

SANGFOR MALAYSIA

No. 45-10 The Boulevard Offices, Mid Valley City, Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia Tel: (+60) 3-2702-3645

SANGFOR THAILAND

141 Major Tower Thonglor (Thonglor10) Floor 11 Sukhumvit Road, Kholngtan Nuea Wattana BKK, Thailand 10110 Tel: (+66) 02-002-0118

SANGFOR PHILIPPINES

Unit 14B 14th Floor, Rufino Pacific Tower, 6784 Ayala Avenue, Makati City, Metro Manila, Philippines Tel: (+63) 916-267-7322

SANGFOR VIETNAM

210 Bùi Văn Ba, Tân Thuận Đông, Quận 7, Thành phố Hồ Chí Minh 700000, Vietnam Tel: (+84) 903-631-488

SANGFOR SOUTH KOREA

Floor 17, Room 1703, Yuwon bldg. 116, Seosomunro, Jung-gu, Seoul, Republic of Korea Tel: (+82) 2-6261-0999

SANGFOR UAE

D-81 (D-Wing), Dubai Silicon Oasis HQ Building, Dubai, UAE Tel: (+971) 52855-2520

SANGFOR ITALY

Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia Tel: (+39) 0331-6487-73

SANGFOR PAKISTAN

Office No.210, 2nd Floor, "The Forum", Plot No. G-20, Block 9, Khayaban-e-Jami, Clifton, Karachi, Pakistan South Region: +92 321 2373991 North Region: +92 345 2869434 Central Region: +92 321 4654743

SANGFOR TÜRKIYE

A Blok. Kat 51. D 643, Atatürk Mh, Ertuğrul Gazi Sk, Metropol İstanbul Sitesi. 34758 Ataşehir/İstanbul Tel: (+90) 216-5156969

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway Secure User Internet Access Behaviour

Network Secure - Next Generation Firewall Smarter Al-Powered Perimeter Defence

Endpoint Secure - Endpoint Security The Future of Endpoint Security

Cyber Command - Network Detection and Response Smart Efficient Detection and Response

Omni-Command - Extended Detection and Response Revolutionize Your Cyber Defense with Intelligent XDR

TIARA - Threat Identification, Analysis and Risk Assessment Smart Threat Analysis and Assessment

IR - Incident Response Sangfor Incident Response – One Call Away Cyber Guardian - Managed Threat Detection & Response Service Faster Response Through Human/Al Collaboration

HCI - Hyper-Converged Infrastructure Fully Converge Your Data Center

MCS - Managed Cloud Services Your Exclusive Digital Infrastructure

VDI - aDesk Virtual Desktop Infrastructure Seamless Experience, Secure and Efficient

Access Secure - Secure Access Service Edge Secure, Agile, and Everywhere

EDS - Enterprise Distributed Storage The Only Secured Data Storage You Need

SD-WAN Boost Your Branch with Sangfor



Sales: sales@sangfor.com Marketing: marketing@sangfor.com

Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com