CHECK POINT™

PREVENTING NEXT-GENERATION THREATS
THROUGH AI AND INNOVATION

Cyber threat prevention has always been tough. Now that the threats are increasing in volume and sophistication, it's more challenging than ever before. Enter AI.

Although Artificial Intelligence (AI) went mainstream amidst the emergence of ChatGPT, Check Point has always been an industry leader when it comes to leveraging artificial intelligence to support cyber security solutions. Across the past 30 years, Check Point has developed more than 70 engines, 40+ of which are based on purpose-built LLM approaches, that provide industry best threat prevention.

By integrating AI into security technologies, organizations can not only enhance threat prevention, but they can also improve automation of processes, threat hunting and Security Operations Center (SOC) event correlation. And that's not all. Further, AI-based tools can inherently improve and evolve themselves, helping organization future-proof against next-generation threats.

Innovation, as through AI, is central to creating an agile and flexible environment through which you and your teams can meet new challenges.

> "The nature of cyber security threats is one of constant change."
>
> Dr. Dorit Dor
> Check Point CTO

AI and Automation

For cyber security professionals, the automation of security processes is an imperative. AI-powered cyber security automation increases efficiency, promotes resource maximization, and prevents subtle threats from escalating. Here's a breakdown of how that works...

Streamlining of Security Operations

Cyber security technologies powered by artificial intelligence engines can streamline routine security tasks that are time-consuming for human employees. For instance, these kinds of tools can assist with data correlation, log analysis, incident prioritization and incident reporting. As a result, humans can spend time on higher-level and more complex security-related tasks, like optimizing risk governance and enabling the business.

Adaptive Threat Detection

Cyber security technologies powered by AI can also parse through historical data and current security activities, helping to speed and scale detection. And in contrast with rule-based systems that need continual manual updates, AI models can independently shift detection strategies; without human intervention. In essence, because of solution autonomy, enterprises can significantly reduce the probability of cyber threats and cyber attack damage.

Rapid Incident Response

Security technologies with AI engines embedded within them can sift through extensive volumes of data, quickly uncovering anomalies and potential threats. Upon identification of a threat, AI can trigger predefined response actions; from isolating affected systems, to stopping malicious maneuvers, to patching of application. This saves time, maximizes resources, leads to cost-efficiencies, and simplifies the situation for cyber security professionals.

Threat Hunting

Threat hunting that's powered by AI enables fast threat detection and interception, which can minimize the magnitude and ripple effect of a threat. AI-driven threat hunting can also help cyber security staff allocate resources optimally and develop comprehensive plans around attack prevention that are based on attack attribution, further mitigating risk.

Proactive Threat Hunting

There's no question—AI has transformed threat hunting. Cyber security used to be a reactive discipline, where IT experts would wait until alerts arrived or incidents occurred before taking action. AI-powered tools mean that unknown malware is seen before it causes harm. Proactive AI-based threat hunting enables cyber security staff to take act fast, before risk leads to damages.

Resource Allocation and Risk Management

AI-driven threat hunting can also provide cyber security teams with clarification around security gaps, security weaknesses, and emerging vulnerabilities. This information enables staff to then allocate resources optimally, ensuring that the most critical areas of risk are addressed. And because information is typically available in real-time, staff can then make resource allocation adjustments, and risk management improvements as threats evolve.

Complex Threat Analysis and Attribution

AI has the capacity to correlate disparate data points across vectors in order to identify connections between seemingly unrelated cyber security events. As a result, AI not only assists organizations in halting sophisticated 'sleeper' attack campaigns, but it also enables organizations to attribute attacks to specific groups or nation-states. Thus, organizations then objectively develop a clearer sense of what (or more accurately, 'who') they're up against and how to (re)build prevention and defense strategies.

Distillation of SOC Events

Artificial intelligence has significantly transformed the ways in which Security Operations Centers (SOCs) manage workflows and drive value. AI renders Security Operations Center management easier, more accurate and more successful.

Automated Event Triage

Because SOC teams can't necessarily expand as quickly as their responsibilities expand, SOC teams need to maximize efficiency. Cyber security tools, like Horizon SOC, deploy AI to accurately identify real attacks across millions of daily logs and alerts.

These kinds of tools empower security staff to respond effectively to the most severe cyber security threats (via automated triage and single-click remediation) and help teams avoid wasting time on trivial alerts and false-positives.

AI-generated Verdict

SOC teams can run AI-based incident analysis on top of other security layers to accurately assess whether or not a given event pertains to malicious activity. Some AI-based engines, like Check Point's Horizon SOC, allow for searches on any Indicators Of Compromise (IOC), enabling security staff to obtain rich, contextualized threat intelligence that can help determine the significance of divergent IOC activities.

Minimization of Breach Impact

The triaging of alerts and ability to access in-depth live intelligence on any IOC (attack timelines, patterns, malware DNA...etc) empowers SOC teams to overcome regular security challenges and to achieve the certainty required to carry out responsibilities successfully. Oftentimes, the SOC is all that stands between an organization and a potentially devastating cyber breach.

Future-Proofing Against Next-Generation Attacks

Artificial intelligence and machine learning-based cyber security technologies can augment their capabilities over time. They can learn from previously observed patterns across vectors and become better attuned to suspicious activity across lifespans.

These are "...engines that learn and improve themselves against the kind of attacks we don't yet know will happen," says Check Point CTO Dr. Dorit Dor.

For example, Check Point's leading industry web and API protection product, which is powered by AI, was able to immediately prevent the Log4j problem without any signature or update because of the way in which engineers structured the AI-engine's learning—it looked out for future-forward types of threat characteristics.

"One of the reasons we moved our engines at Check Point to be AI-based is because it serves as future-proofing" says Dr. Dor.

AI and Human Collaboration

Errors can be costly. When it comes to leveraging AI across a business, in most cases, using the "keep-the-human-in-the-loop" approach works best. As the name implies, Human In The Loop (HITL) hands tactical (and perhaps some strategic) decision-making over to algorithms and machines, while advocating for humans to maintain managerial control over systems.

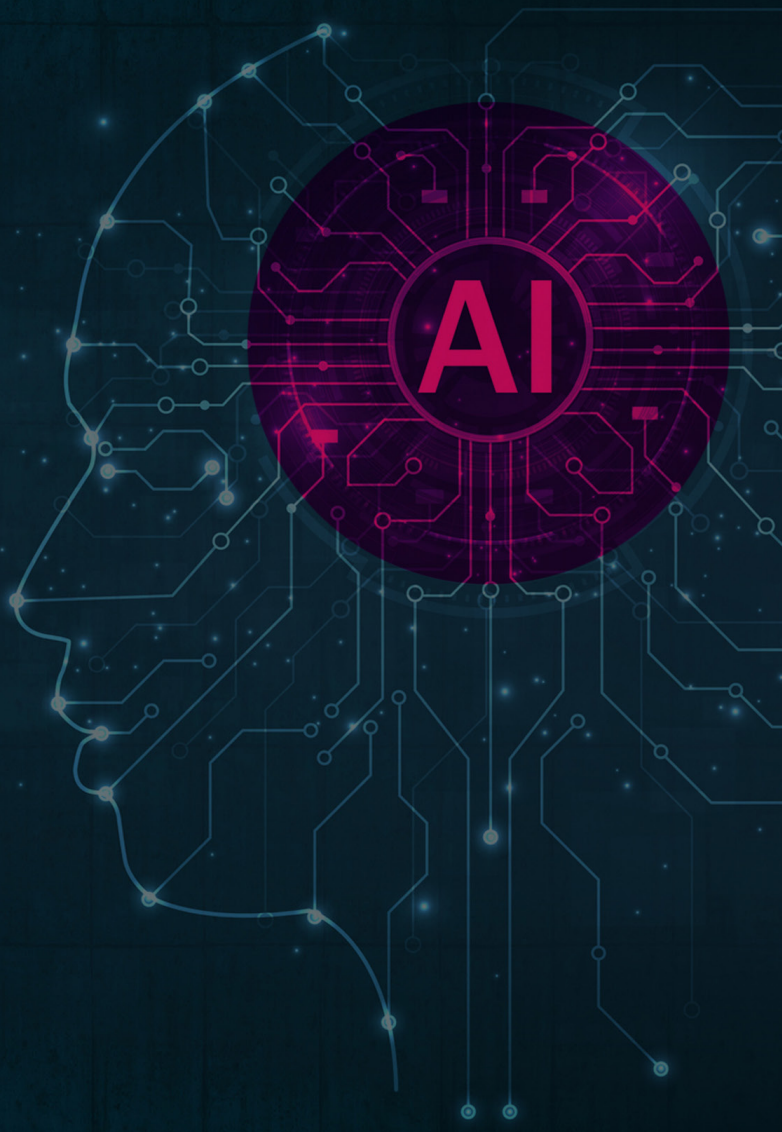
Across AI and ML-based decision-making processes, humans need to remain in-the-loop and able to provide oversight, guidance and intervention where appropriate. This helps to ensure intended, ethical and value-add outcomes.

AI and the Economic Dimension

If they can afford it, cyber criminals will use AI in the context of cyber attacks. AI relies on compute resources, which have a monetary cost. But cyber attackers, like cyber defenders, have finite financial capabilities.

"There will be an inevitable arms race and stacking up of AI capabilities against one another," anticipates Check Point CISO Marco Eggerling. This is a key reason as to why Check Point began integrating AI capabilities into its products many years ago.

Defenders shouldn't need to worry about the exponential added cost of AI-based prevention mechanisms. "We help defenders mitigate attacks by AI tools and, in many cases, remove the economic burden of the utilization of AI, as it's an integral part of our products already," says Eggerling.



Conclusion

It nearly goes without saying—Advanced, next-generation cyber threats are proliferating at an unprecedented rate. The enterprise attack surface is continuing to expand and cyber security teams are inundated by alerts that they can't keep up with.

The automation, threat hunting, SOC and independent learning abilities that AI-driven cyber security solutions offer is unrivaled by the capabilities of even the most talented group of enterprise security professionals. AI-based solutions are no longer simply a nice-to-have, but a core element of the modern tech stack.

While humans need to remain 'in-the-loop,' strategic innovation—as exemplified by intelligence-based solutions—can lead to a more secure IT and workplace environment.

If you have a random collection of AI-powered cyber security solutions, you might be leaving value on the table. Reinvent your current cyber security architecture. Please visit the Security in Action webpage or talk to a Check Point sales representative to get started.

You also might be interested in A CISO's Guide to AI. To discover AI and cyber security technologies that can benefit your business, learn more here.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com