A NEW CYBER SECURITY PARADIGM TO GET AHEAD OF THREATS

Sponsored by Cyber Talk

Since its inception, cyber security has focused on how products can effectively react to threats. Traditionally, security engineers have developed methods to stop the attack once detected, even after the exploit has caused damage to organizations and individuals. In response, attackers have diversified their attack methods to evade detection.

> The Creeper Worm, an experimental replicating program developed in 1971, was the first computer virus. It infected DEC PDP-10 computers running the TENEX operating system using the ARPANET. It copied itself to the remote system where the message, "I'm the creeper, catch me if you can!" was displayed. The Reaper program was created to move across the ARPANET to delete the self-replicating Creeper.[1]

Despite the invasion of Gen V or large-scale, multi-vector attacks armed with advanced attack tools over the past five years, many cyber security technologies remain in reactive mode. Mitigating damage is a goal, but with recent sophisticated attacks, shutting down network services has been common.

Traditional security strategies and methods are no longer enough to thwart advanced attacks. The Log4J vulnerability[2], SolarWinds attack[3] and supply chain attacks are noteworthy examples of how attack methods have outpaced conventional reactive security strategies.

Now, there is a new paradigm to help your organization stay ahead of these sophisticated attacks.

Enter AI and Machine Learning

The introduction of AI and Machine Learning is changing the cyber security landscape, incorporating predictive prevention to stop cyberattacks.

The importance of AI cannot be overstated. For example, 69% of senior executives[4] across all industries stated that they believe their organization would not be able to respond to cyberattacks without AI. Furthermore, as the number of cyberattacks increases by over 50% per year,[5] it's simply not possible for humans to scale at that level.

---

[1] https://en.wikipedia.org/wiki/Creeper_(program)

[2] What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake, The Conversation, December 22, 2021.

[3] Saheed Oladimeji, Sean Michael Kerner, SolarWinds hack explained: Everything you need to know, TechTarget, June 16, 2021. https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[4] Respond to Cyber Attacks by Industry https://www.statista.com/statistics/1028762/worldwide-reliance-ai-respond-to-cyber-attacks-by-industry/

[5] Human and machine: Working together to solve the cyber security problem. March 8, 2022. https://www.cybertalk.org/2022/03/08/man-machine-working-together-to-solve-the-cyber-security-problem/

AI can look at billions of alert and log data records arriving each second, and it can continuously evolve predictive threat models. With AI and big-threat data, it's time for the cyber security industry to replace reactive security with a new paradigm that gets out in front of threats to stop attacks outside of information environments before they inflict damage and spread globally.

What do the elements of MACS mean?

Multi-Action Cyber Security (MACS) is a new paradigm that is predictive, comprehensive, process oriented, consolidated, and accelerated to deliver proactive security, while optimizing service levels.

Prevention and Process Orientation

Detection means identifying threats after they have entered an information environment. In contrast, prevention means stopping cyber threats outside an organization's information environment before attacks can cause extensive damage such as extortion by ransomware, or theft of intellectual property as well as secondary damage like productivity loss due to shutting down services during remediation.

To become preventative, AI and Machine Learning engines examine data to recognize known threats and evolve their threat models to recognize novel threats and predict emerging threats. Chip-level threat recognition and massive intelligence of known threats are 2 ways to feed threat data into security engines that use machine-learning.

> DevOps is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes.[6]

The MACS prevention process also extends to the entire software cycle. It does this by preventing compromises to DevOps that can cause supply-chain attacks and by finding software vulnerabilities from Dev-Ops through to production environments. Along with the process focus, MACS extends predictive security to whole information environments irrespective of where users and assets are located.

[6] "What is DevOps?"
https://aws.amazon.com/devops/what-is-devops/

Spatial Agnosticism

Today's organizations are approaching total spatial distribution. On-premises data centers and LANs join one or more off-site cloud deployments as well as SaaS workloads and an increasingly work-at-home and mobile workforce. Add smartphone users as well as remote offices, integrated supply-chain partners and customers, and IoT devices and you have anywhere - everywhere computing.

MACS security uses AI to protect workloads, users, networks and computing assets with consistent policies regardless of their spatial distribution. With all this diversity, it helps to replace fragmented thinking about networking and security with a holistic perspective.

Holistic View of Information Environments and Security

Due to technical diversity and the variety of threats in the landscape, especially multivector attacks, IT and security professionals should look at their information environments not as a collection of individual components to be protected separately by point solutions, but as a single entity to be protected through a consolidated security architecture. There are several reasons for this. A consolidated security architecture permits the automated sharing of threat information and policies with all enforcement points throughout the environment regardless of location or technology.

> Since every chain is as strong as its weakest link, it's absolutely necessary to make sure all links in the chain become resilient and operate under the same security levels. The best way to achieve this is through having a consolidated security framework.

Perhaps even more importantly, looking at an information environment as a single unit is necessary to effectively micro-segment the environment to create policy-driven zero-trust in which each person, device and type of data can only communicate with specified resources. As it takes AI to predict and prevent threats, it also takes AI to automatically push changing policies to all enforcement points in a data center, LAN, cloud, SaaS as well for remote users and remote offices connected by WAN.

In addition, a holistic view of the environment through a consolidated security architecture streamlines monitoring, management and administration especially when aided by AI-assisted automation. As if ubiquitous, preventative security isn't enough, the MACS paradigm also insists on optimizing service levels and performance.

Conclusion:

The meaningful introduction of AI and its subcategory Machine Learning underpin the Multi-Action Cyber Security paradigm to offer security professionals the extraordinary opportunity to fix the basic problem of reactive security that has plagued cyber security since the beginning. The era of preventative security is here.

To learn more about DevSecOps, click here. To understand the benefits of a consolidated security architecture, go this page.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com