Snode

Active defence

Persistent engagement as the first line of defence in the digital age

20 May 2021

www.snode.com
info@snode.com
+27 12 880 0989

Table of contents

Introduction

As the hyper-dynamic digital landscape expands with emerging technology, so too does the vulnerability landscape, fuelled by the ever-evolving sophistication and complexity of cyber attackers.

The digital networks that organisations are so dependent on have become disparate during the pandemic, meaning that not only are there billions of data transfers occurring daily to keep track of, unsecured networks and shadow IT makes for a burgeoning hunting ground for hackers.

Cyber attackers have weaponised infinite mechanised resources to compromise corporate systems, the scope and sophistication of which cannot be adequately combated by the finite resources of a security team of humans. While defenders have measures in place to cover every inch of a potential attack surface, the asymmetric nature of the threat environment means that cyber security teams do not have the time, capacity or intel to match the relentless onslaught of machines.

AI technology is both the cause of sophisticated weaponised attacks, and the viable solution to combat these imminent threats (DeLisi, 2021). The only way to successfully defend against the unknown is to have an agile, resilient and innovative security posture that includes real-time, automated, countermeasure deployment.

The anatomy of cyberattacks

Prior to the development of AI cyber defence, the fundamental obstacle to achieving an autonomous response, was determining the exact action that is needed to stop an infection from spreading, while keeping the business operational (Ismail, 2017).

Traditional cyber security measures may be able to flag commonplace attack vectors, but is not equipped to contain them. A critical issue is lack of visibility into the entire threat ecosystem, and making assumptions based on legacy rules and signature-based technology. For example, if a rule or signature for a ‘known bad’ is flagged, the system could automatically block the recognised behaviour, such as a ‘bad’ IP address. This response is simplistic and does not consider the whole picture: the attack might involve connections to other IPs, or internal lateral movement; the connection to the bad IP is not the full extent of the threatening behaviour of that malware, but is just a single indicator (Ismail, 2017).

On the other side of the coin, autonomous responses could be devised to immediately deactivate a device as the earliest indication of a compromise. While this may stop the attack, automatically shutting down the device may have dire consequences for a business environment, such as shutting down an integral system within an operational technology framework.

As such, defence must be elevated by the tenacity of AI, but the key to its success lies in leveraging of the insight and intuition of the people within the defence process.

Real-time persistent engagement

A self-defending system levels the playing field by leveraging of a fully synchronised ecosystem of people, processes and technology that works together to manage, monitor, execute, automate and respond to cyberattacks in a time-intensive and cost-effective manner (Essomba, 2019).

Artificial intelligence has the ability to scale threat analysis and triage, better understand anomalies, automate responses and, most importantly, develop proactive measures (Groopman, 2020). AI algorithms learn in real time about natural patterns in a network and can detect and remediate the entire spectrum of threat, from sophisticated 'low and slow' threats and lateral movement, to brute-force, automated attacks such as ransomware (Ismail, 2017). In order to keep ahead of increasingly conniving cyber criminals, this must be taken a step further to persistent engagement and automated responses to not only relentlessly monitor adversaries, but to take swift offensive action against them and learn from their behaviour to better defend against future attacks.

An automated, self-defending system understands the tools, tradecrafts and procedures that attackers utilise to automatically deploy persistent countermeasures to disable attack vectors and degrade the attacker's capabilities. Through machine speed, this posture elevates your existing passive detection controls, giving you time to identify, respond to and remediate potential threats while focusing an analyst's energy on dealing with the most critical problems at hand.

Real-time, automated response systems allow you to:

- Consolidate all security measures in one dashboard
- Gain clear visibility across the threat landscape
- Make informed decisions through vital security metrics
- Streamline incident responses
- Empower analysts to employ intuition in critical events
- Integrate with other data sources to contextualise incidents
- Automate false security alerts

The human-machine interface

While automated techniques are better than humans at managing the volume of potential threat vectors, human analysts remain essential arbiters of controls, context, knowledge and explainability (Groopman, 2020). The nature of risk is never black and white; success depends on the integration of human and machine to combat imminent and constantly recalibrating threats.

Real-time automated defence systems are considered a force-multiplier for your organisation's cyber security efforts, balancing AI capabilities and human capacity. These efforts are made far more efficient by allowing artificial intelligence and machine learning to analyse nuanced and high-volume data, automate repetitive and manual tasks and flag anomalies, while analysts are free to commit their efforts to higher-value decision-making and pressing issues.

Conclusion

In 2021 and beyond, cyberattackers will continue to devise ever-evolving AI and machine learning tools weaponised against organisations, governments and citizens. To remain complacent is to invite catastrophic compromise; organisations must consistently expand their technological arsenals centred around active defence to shut down persistent threats and remain resilient in the digital age.

About Snode Panthera

Snode Panthera disables attacks and defends vulnerable systems through its real-time, automated response system. This novel approach augments your cyber security team and defends targeted vulnerable systems from persistent attackers, much like a fighter jet would deploy an intense flare to attract and destroy an enemy heat-seeking missile. Snode Panthera achieves the same by automatically deploying a defensive countermeasure in real time. This precision digital defensive acts without data decryption, network interception, business interruption or human intervention.

When Snode Panthera detects a precursor to an attack, it will preemptively counter the attack and disable the attacker, preventing exploitation and system compromise. It does so by rapidly shielding vulnerable systems and simultaneously blocking the attacker without intercepting or interrupting business communications.

Benefits:

- Real-time, **24/7 automated threat detection and response** without any human intervention.
- **Protection** for vulnerable unpatched, misconfigured or unsupported operating systems and firmware.
- **Defence** against potentially compromised third-party networks, cloud-based platforms and devices.
- **Automatically reducing MTTR** (Mean Time To Respond) and **ADT** (Attacker Dwell Time) by containing threats in real time.

About Snode Technologies

Snode is a cyber defence company focused on making the unknown known. Snode is driven by excellence and the desire to tackle client challenges with bleeding-edge cyber technology.

Snode has over 100 global points of presence, protecting large industrial, agricultural, telecommunications and financial infrastructures.

Author

Nithen Naidoo

CEO and Founder of Snode Technologies

Nithen Naidoo is the CEO and founder of Snode Technologies. As a cyber security evangelist, with over 20 years of experience, Nithen provides cyber defence solutions globally, and most recently was recognised by the prestigious AfricArena tech accelerator as an Emerging Entrepreneur of 2021. Nithen is also a sought-after public speaker.

Snode Technologies, a cyber defence firm based in Centurion, South Africa, has been a finalist and winner of some of Africa's most prestigious innovation awards, most recently, an overall winner at the SA Innovation Summit 2020 and the MEST Africa Challenge 2019. Snode was also listed, by Slingshot (Singapore), as one of the (2020) Top 100 Deep Tech innovations globally.

References

DeLisi, B. 2021. Top Predictions for AI in Cybersecurity in 2021. Cyber Defense eMagazine – April 2021 Edition. Retrieved from: https://www.cyberdefensemagazine.com/e-magazines/

Essomba, M. 2019. Self-defending networks: reality or fiction? How to Strengthen Your Cyber Defence Using the Power of Automation. Cybersecurity Trends. Retrieved from: https://cybersecuritytrends.uk/2019/07/09/self-defending-networks-reality-or-fiction-how-to-strengthen-your-cyber-defence-using-the-power-of-automation/

Groopman, J. 2020. AI-driven cybersecurity teams are all about human augmentation. Techtarget. Retrieved from: https://searchsecurity.techtarget.com/tip/AI-driven-cybersecurity-teams-are-all-about-human-augmentation

Ismail, N. 2017. Autonomous response as a force multiplier for human security teams. Information Age. Retrieved from: https://www.information-age.com/autonomous-response-force-multiplier-human-security-teams-123469048/t