Nyotron brings disruptive PARANOID security solution to the UK

Submitted by: Newshound Communications
Tuesday, 30 May 2017

Nyotron (https://nyotron.com), the creator of threat agnostic cybersecurity solutions, today announced its expansion into the UK and Europe and its debut at Infosecurity Europe 2017 where it will be exhibiting PARANOID, the flagship new-generation endpoint security platform. PARANOID whitelists normal behaviour patterns and permissible actions at the operating system level as opposed to blacklisting attacks and takes a 'threat-agnostic' approach. This enables PARANOID to detect, prevent, respond to and analyse any attack – even unknown unknown threats such as Advanced Persistent Threats (APTs) and Zero-hour attacks – because it requires no prior knowledge of the threat. The technology is disruptive in that it challenges the accepted wisdom that point solutions or advanced threat intelligence are the best way to deal with unknown unknowns, instead using legitimate user behaviour patterns to verify activity to provide a single form of future-proof defence.

Nyotron's launch into the UK market marks the latest move in an aggressive expansion strategy. Originally founded in Israel in 2012, the company CEO, Nir Gaist has spent the past five years developing the Behaviour Pattern Map (BPM) programming language on which the PARANOID solution is based. Following the successful patenting of BPM, and with a number of high profile customer wins including El Al Airways, a major US law enforcement agency and the largest bank in Israel, the company opened its US headquarters in Silicon Valley in late 2016 and is now turning its sights on EMEA, opening offices in the Leadenhall Building in Central London.

The Nyotron PARANOID new-generation endpoint security platform is the brainchild of Nir Gaist, a cybersecurity prodigy from Israel who realised that while attacks may vary, their end objectives were finite and typically limited to file deletion, data exfiltration, and malicious encryption. Rather than focus on attacks he decided to look at how to capture legitimate user behaviour in the form of a programming language (BPM) which enables PARANOID to classify system calls that are normal, suspicious or malicious.

"Today's advanced malware is able to bypass traditional and so-called next-generation endpoint products to avoid detection. Even advanced threat intelligence solutions are reliant upon machine learning, artificial intelligence or mathematical-based techniques which use some element or attribute of a known attack to predict threats as opposed to the deterministic nature of PARANOID. We take the opposite approach and focus on the damage stage. Our unique threat-agnostic approach assumes threats WILL get into the network. The attack then becomes irrelevant, a red herring, with legitimate activity the focus. By whitelisting normal behaviour patterns at the operating system level we don't need to have any knowledge of the threat's characteristics."
Nir Gaist, CEO Nyotron

How it works

PARANOID addresses communication at the operating system level unlike other whitelisting technologies which typically focus on applications. Agents are located on endpoints in a server based architecture and monitor the system calls sent via the operating system, data, communications, registry and process management systems to the kernel space. These are monitored and compared against acceptable behaviours

using BPM to distinguish between “good” and “bad" actions. Numerous indicators such as how the long the user takes to respond, their keystrokes and mouse movements are used to verify the legitimacy of the system call request, detecting and preventing any malicious activity irrespective of the threat type, structure, attack vector, method or technique used. PARANOID then captures the threat, enabling analysis and response to determine who generated it and how, and where or when the attack penetrated the organisation.

“At the current time, there is no filter between the user space and the kernel space. It’s a void. It simply allows any instruction from the operating system to be actioned whether it’s legitimate or malicious. It’s here where PARANOID sits and why it is so different to any other solution, embodying a new approach to whitelisting. We are able to differentiate between these system calls because we filter the kernel space. By comparing activity against the BPM we are then able to either allow or block requests making the system impervious to attack.”
Nir Gaist, CEO Nyotron

Nyotron War Room. High-profile enterprises that have invested in a Security Operations Center (SOC) or similar in order to deal with targeted attacks can benefit from the real-time visibility of the Nyotron War Room. This delivers a unique 3D representation of the security status of all endpoints, providing a visual interface to help security analysts conduct digital forensics, gather intelligence and analyse attacks that infiltrate the network.

Nyotron Managed Defense Services. The current shortage in cyber skills is seeing many enterprises seek external expertise. Nyotron’s Managed Defense Services for end users and MSSPs provides endpoint security via the Nyotron War Room facilities manned 24/7 by Nyotron’s top analysts and research teams. The Nyotron War Room offers proactive and actionable alerts, supported by forensics and mitigation services.

PARANOID is unique in that it is:
A kernel filter: PARANOID carries out filtering between the operating system and the kernel, applying a method of defence through the application of user behaviour indicators.
Threat-agnostic: PARANOID assumes a position of compromise ie that the attacker is already in the network or will circumvent existing controls at some point. This makes the method or mode of attack irrelevant with the primary mode of defence being legitimate behavioural analysis. This approach futureproofs the organisation against any threat even those ‘in the wild’ or ‘unknown unknown’ attacks.
Zero-hour: Machine learning solutions take time to build up a picture of threats or predictive intelligence. PARANOID actively protects the organisation and assets inside or outside the network from the moment it is deployed.
Subliminal: PARANOID’s light footprint client does not rely on any database frequent updates. Setting its own industry record of less than 1% footprint and no reboot deployment, PARANOID performs silent installation. A special covert mode implementation is also available.
Universal: PARANOID complements other security solutions such as SIEM or SOC cyber centres but equally can operate as a standalone solution. Unlike other point based solutions, PARANOID can stop any threat, eradicating the need for point solution security measures.

About Nir Gaist

Nir Gaist, the company CEO and founder, started programing at the age of six. Three years later, he and his brother Ofer Gaist, now COO, started Nyotron as a penetration testing company. Nir hacked an Israeli service provider when he was nine, which was so impressed with his skills it ended up hiring him. From there, he went on to test telephone systems, online banking protocols, ATMs and more for the largest banks in Israel. When he was 10, Nir began his studies at the Israeli Technion University and wrote a curriculum for the Israeli Ministry of Education on offensive security that he taught in high schools throughout Israel. He has also worked on a number of security projects with Microsoft, winning an organizational best practice award from Bill Gates when he was 12.

Notes for editors
Nir Gaist will be in the UK on 5 June and conducting interviews at the company HQ in the Leadenhall Building and attending Infosecurity Europe on 6 June where Nyotron wil be exhibiting on stand L120. Please contact us to arrange a one-to-one briefing on either date.

About Nyotron
Nyotron is a privately held cyber-security company that has developed a disruptive threat-agnostic defense technology to cope with the biggest challenge of today's digital era — the unknown threat. PARANOID is designed to prevent targeted and advanced national-level cyber-attacks on high-profile enterprises, and it does so without any previous knowledge about the threat or its methodologies. Based on a unique last-line-of-defense approach, the company's technology is designed to protect enterprise data and critical assets by mitigating threats that were able to outsmart all security layers.
Nyotron's customer base includes all major industries, such as transportation, government, banking, healthcare and the public sector. The company's headquarters are in Santa Clara, California, and R&D is in Israel. To learn more, visit www.nyotron.com.

Media contact:
Sarah Bark
SHConsulting
E: sarah.bark@shconsult.co.uk
T: 01420 587978
M: 07912 012321

Marketing contact:
Donna St John
Vice President of Marketing, Nyotron
E: dstjohn@nyotron.com
T: +1 408-780-0752