GATEWATCHER AIONIQ

As cyber-attacks increase in magnitude and sophistication, organisations of all sizes can no longer afford to constantly play catch-up. They need to stay one step ahead of cybercriminals, if they want to survive.

Gatewatcher's AIONIQ changes the landscape. This next-generation NDR (network detection & response) solution combines artificial intelligence (AI)-powered human insights, machine learning, statistical and dynamic analysis that allows it to conduct mapping, and behavioural analysis of all threats and provide full visibility into targeted attacks.

AIONIQ is an exciting new platform designed to detect zero-day and advanced cyber threats from day one of installation and claims extremely low false positives for fast mean time to detect (MTTD) rates. It offers a barrage of sophisticated technologies, as, along with passively mapping all organisation assets and users, it provides Shellcode and PowerShell decoding to detect advanced attacks, incorporates Cyber Threat Intelligence feeds, employs 16 anti-malware engines to reassemble and scan every file, and implements sandboxing for deeper file analysis.

Deployment options are extensive, as AIONIQ supports on-premises, hybrid and Cloud models. Central to all operations is the Gatewatcher GCenter management server, which stores and analyses all information sent to it by virtual and physical GCAP detection probes, provides configuration and reporting interfaces, and exports data to SIEM systems. Connected to a TAP, packet broker or switch mirror port, GCAP probes analyse received flows to detect, capture, reconstruct, sort and transmit files, malicious code and events to the GCenter. Multiple probes can be deployed locally and remotely. This architecture allows AIONIQ to provide a full 360-degree risk view, as it can analyse all internal, external, north-south and east-west communications, and detect lateral movement, exfiltration and compromised endpoints.

The GCenter web console opens with informative dashboards offering a curated view of all risks, allowing security operation centre teams to focus on essential tasks. Coloured blocks highlight critical, high and medium risks for 24-hour and seven-day periods, a status view shows which threat modules are in an alert state and a smart central panel provides clear specifics on detected threats.

Clicking on a risk in the list below the graphics panel presents a wealth of valuable information, such as the alert type, the risk by asset, level and user, plus the MITRE association. When used during an attack, analysts can download the Shellcode, see the number of instances, how many times it was encoded and the actual calls being made.

Zero-day attacks using ShellCode are difficult to detect and prevent, but AIONIQ has distinct advantages, as, in this reviewer's experience, it decodes Shellcode more times than any other vendor, making it more likely to discover the attack. Next, you can go hunting where AIONIQ transports you to screens showing the underlying communication data for the attack, tactical information, infected files and the number affected, file transactions, source and destination addresses, and much more.

Drilling down to the user level reveals details of user risk and a map of all interactions with other users, making it easy to spot lateral movement and track it back to patient zero. Another standout feature is AIONIQ's ability to detect C2 communication, especially using domain-generated algorithms showing which assets have been compromised.

Gatewatcher's AIONIQ takes threat detection and response to new levels, as this highly scalable platform requires no learning processes and provides high fidelity attack data from the moment it is deployed. It's a cost-effective solution for organisations of all sizes and is one of few security platforms that delivers the full spectrum of static, dynamic and AI/ML analysis, hardening, compliance, NDR, threat intel and cyber cartography functions in a single, easily managed solution.

Product: AIONIQ
Supplier: Gatewatcher
Web site: www.gatewatcher.com
Sales: +44 (0)203 743 0900
Email: contact@gatewatcher.com