VECTRA COGNITO

Traditional intrusion detection and prevention systems (IDPS) are struggling to cope, as cyber-criminals become ever more imaginative. The rapidly-increasing volume and effectiveness of cyber-attacks mean they must evolve to stay ahead and the way forward is artificial intelligence (AI).

Vectra Cognito changes the landscape, as this next-generation cybersecurity solution has AI and machine learning (ML) at its core. Built from the ground up on attack behavioural detection AI algorithms, Cognito analyses all network traffic, including cloud and data centre workloads, and performs automated real-time threat hunting using supervised and unsupervised ML techniques.

Cybercriminals can't avoid using specific attack techniques, and Cognito automatically recognises and exposes these to provide a complete breakdown of all attack phases, including command and control (C&C), reconnaissance, lateral movement, data exfiltration, bitcoin mining and ransomware activity. It allows security teams to respond quickly to attacks by reducing alert fatigue and presenting them with the most relevant information.

Cognito is elegantly simple, as it analyses metadata from captured packets in real-time and employs a highly scalable, distributed architecture. Deployed as a hardware appliance that Vectra calls the 'brain', this receives metadata from multiple sensors.

The sensors are small dedicated appliances that are installed in-line anywhere on the network, on a SPAN port or network TAP. Cognito's reach can be extended by deploying sensors at remote sites and Vectra also offers a VMware virtual sensor that natively integrates with vCentre to protect virtualised environments.

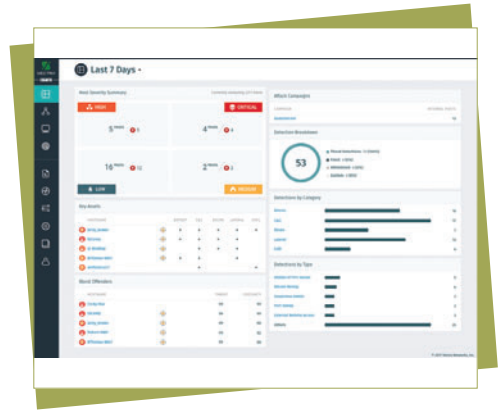
Cognito's well-designed web console opens with a dashboard showing a status overview of monitored environments. It provides executive summaries over selected time periods, clearly showing compromised hosts and their threat levels, key assets, attack categories and the types of detected attacks.

The Hosts view is Cognito's star player, as this presents a smart quadrant view based on threat severity and attack certainty axes. Hosts in the upper right sector represent the greatest threat and should be investigated immediately, whereas hosts in the bottom left sector are considered a low threat.

Cognito correlates threats over time; so, if an attack progresses, the icons of affected hosts will move across the quadrants and change colour. Selecting any host loads a pop-up window showing their threat and certainty levels, along with all the latest active detections.

You can drill down deeper and view a timeline of suspicious behaviour and when it was last seen on the selected host. The left pane shows clearly if the attack is targeting key assets and breaks it down into attack phases, or kill chains, so you can see precisely what stage it is at and if data has been exfiltrated.

This feature is worth its weight in gold, as it allows security teams to instantly identify and remediate compromised hosts, without being subjected to a barrage of uncorrelated alerts. The Campaign view provides even more valuable information by showing all hosts affected by coordinated attacks.



This presents analysts with high-level views of attack campaigns, how they are spreading and which hosts are involved. They can see suspicious activities, such as C&C or remote executions and pinpoint 'patient zero' - the first host that was compromised.

A major advantage of Cognito's AI-based threat detection is that it doesn't require predefined threat signatures. For example, Vectra didn't need to update Cognito's algorithms when WannaCry surfaced, as it already knew the attack vectors to look for, such as port sweeps and ransomware activity on SMB file shares.

Cyberattacks are getting ever more sophisticated, so new ways of thinking are needed to detect them. Vectra Cognito AI-based threat detection platform is the perfect response, and neatly fills the void perimeter and endpoint security products leave behind.

Product: Cognito
Supplier: Vectra
Telephone: +44 (0)1635 800 459
Web site: www.vectra.ai
Sales: sales-inquiries@vectra.ai