SENSEON

Sensory AI for cyber defence

Benefits

- Real-time, accurate threat detection
- Dramatically reduces false positives
- Unparalleled visibility across digital estate
- Contextual and actionable alerts
- Automates threat investigation
- Replaces the need for multiple solutions
- Intuitive UI simplifies threat investigation
- Fully scalable, versatile deployment

> We are impressed by the breadth and diversity of the activity that Senseon is able to detect. This strengthens my confidence that our organisation is well protected.

Paul Grant, IT Solutions Lead

Harbottle & Lewis

Security failures will cost an estimated **$8 trillion by 2022**

'A game-changer'

The Senseon platform is a unique and innovative AI-led approach to cyber threat detection. Senseon offers security teams unparalleled visibility across their organisations, allowing for the detection of even the most subtle and complex of cyber attacks. By alerting accurately on genuine threats, Senseon dramatically reduces false positive alerts.

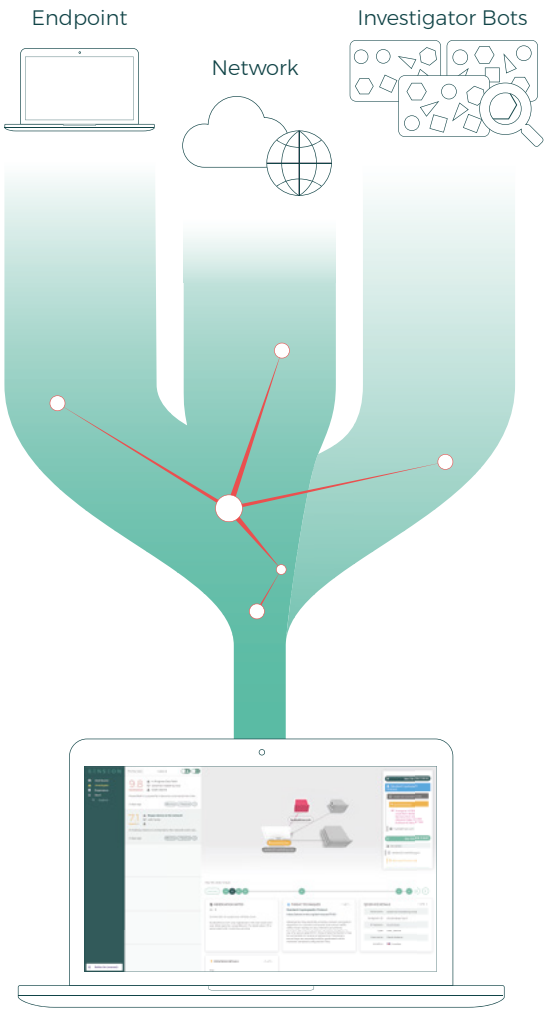
Senseon's ability to think like a human analyst allows it to not only automate many of the repetitive investigative tasks, but to go beyond the capabilities of traditional tools by detecting advanced threats that bypass their systems. In this way, Senseon helps organisations retain their invaluable people, who find real purpose in the work they do.

The Senseon platform's all-in-one cyber defence approach replaces the need for multiple tools, meaning companies can simplify their security stacks, saving them time and money. By replacing multiple tools with the Senseon platform, organisations expose malicious actors hiding in the gaps, and are better able to focus on delivering their business objectives.

The evolving threat landscape

Traditional single-point cyber security tools attempt to detect threats from just one point of view. This limited approach allows attackers to hide in the gaps created by these various single-point tools, and means threat detectors must err on the side of caution, resulting in a flood of false positives being escalated for the attention of security teams. The problem is further exacerbated by the increasing velocity of attacks and growing attacker innovation.

All of this puts a great burden on security teams to manually sift through a large number of false positives alerts, wasting their time and money, and drastically decreasing job satisfaction. Attackers are presented with an advantage, and by slipping through the gaps between single point tools can hide amongst the sheer volume of false positives alerts created by these tools.



The technology

Senseon deploys its senses across endpoints, networks, and Investigator Bots - which look at potential threats from an outside point of view - to detect unusual activity anywhere in the organisation. Senseon's unique AI Triangulation technology thinks like a human analyst. By observing threats from multiple perspectives, pausing for thought, and learning from experience, Senseon automates the process of investigation. In this way, Senseon detects even the most subtle and complex of cyber attacks, increases the accuracy of threat detection, and dramatically reduces the number of false positive alerts.

Benefit for all

Senseon was designed with all users in mind from CISOs to non-security professionals. The 'Dashboard' view offers CISOs and board executives a holistic overview across their entire organisation, helping them to manage risks that would otherwise go unnoticed. The 'Investigate' view has been designed to help analysts simplify the process of investigation and to prioritise genuine threats. More seasoned analysts enjoy using the 'Hunt' view, where they can access the raw data to carry out manual investigations. Senseon is also accessible for non-security professionals, as its step-by-step narrative of 'Cases' presents an easy and intuitive way of visualising the threats within their organisations.

Exponential value from day one

Senseon's extensive visibility across its senses, its use of AI Triangulation, and its narrative-based interface are capable of simulating how the analyst thinks, enabling the technology to augment their role. The platform raises genuine alerts, and provides security teams with the necessary context to thoroughly understand and remediate threats. This unique approach to cyber security saves organisations time and money, allowing them to better focus on delivering their business objectives and to remain ahead of the evolving cyber threat landscape.

> Real time machine learning technologies, like Senseon, are critical in helping organizations cut through the noise of their busy networks to identify the real threats.

Dr Ken Urquhart, Former Senior Director, Microsoft Alchemie Ventures

Find out how Senseon's free four-week Value Assessment can help your organisation.

Call **+44 (0)20 7692 5178** email **demo@senseon.io**
or visit **www.senseon.io/value-assessment**

About Senseon

Senseon is the next phase of AI for cyber defence, moving beyond rules-based systems that are too rigid to keep pace with emerging cyber-attacks or ineffective AI systems which cannot differentiate between unusual behaviour and malicious threats. Unique to Senseon, 'AI Triangulation' understands and correlates threats across an organisation's entire digital estate, providing much needed context and clarity in an increasingly noisy landscape. Founded in 2017, Senseon brings together cyber security experts, former government cyber operatives and applied machine learning specialists. Headquartered in London, UK and Chicago, USA, Senseon also has a presence in the Middle East and Australia.

Contact Us

info@senseon.io
+44 (0) 20 7692 5178
senseon.io
@SenseonTech
100 Pall Mall, London, SW1Y 5NQ