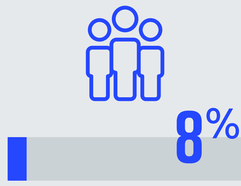
Voice of SecOps

In its first annual report, Deep Instinct set out to explore key current threat concerns and how they are impacting the cybersecurity community and those on the front lines. This global report also evaluates where the priorities need to be placed to develop a future-proof solution moving forward.

SOC staffing level adequacy



Only 8% of respondents believe their **Security Operations Centre (SOC) is "very well staffed."**

Trustworthiness of AI in cybersecurity solutions

of respondents claim to find the AI in their **AI-based cybersecurity solutions "completely trustworthy."**

Critical alert remedial times

On average it takes companies **13 hours to process a critical alert and have it remedied.**

Only 14% can process **an alert and remedy in under an hour.**

Confidence in detection of weak signals

of respondents claimed to be **"not very confident"** in their ability to **speedily and correctly detect weak (i.e. low priority) signals** in the huge alert flow that they receive.

1,247 hours

CISO Deputies surveyed stated that 1,247 hours of their working week were **taken up dealing with alerts caused by false positives.**

Number of AI cybersecurity solutions in production

of companies **have only one** AI cybersecurity solution in production.

of companies **don't have any** AI cybersecurity solution in production.

The Hayhurst Consultancy conducted research among 600 cybersecurity professionals across North America and key western European countries, including CISOs, CTOs, Global Cybersecurity leads, and Infosec analysts across a range of key verticals such as technology, financial services, healthcare, telecoms, and manufacturing.

To learn more, visit:

deepinstinct.com