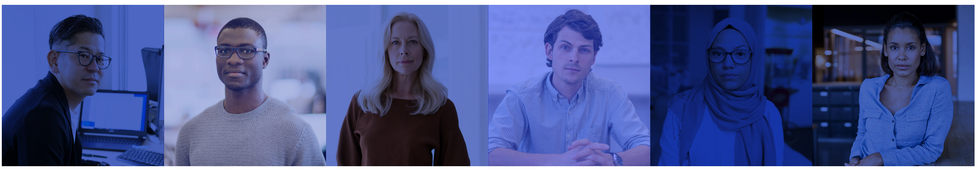

Voice of SecOps

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.

Top two concerns of **global IT professionals and CISOs**

Ransomware

Zero day attacks

U.S. respondents spent at least

11 HOURS A WEEK

dealing with alerts caused by false positives.

(significantly more time than their non-U.S. peers)

MORE THAN 70%

More than 70 percent of those surveyed think it is **likely that their company will be hit by a successful ransomware attack.**

90%

of respondents agree that **automation** allows them to **free up teams to focus** on **higher-value and/or more strategic tasks.**

90%

of U.S. respondents stated that they believe there are **tools available** in the cybersecurity market that could **improve their company's defenses.**

89%

say their security technologies require **frequent, time-consuming security patches and updates** to ensure the solutions remains effective.

61%

agree or strongly agree that threats in their company could get **missed** due to the **overwhelming volume of false positives.**

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