Cyber Threat Intelligence Trends

A survey of 338 Cyber Threat Intelligence (CTI) analysts and practitioners highlights a shocking lack of training, tools, and oversight.

"Lessons learned from this survey can be building blocks for improving operational security and collaborative efficiency on CTI teams."

- Jake Williams, SANS Institute Analyst and President of Renditions Infosec.

ABSENCE OF TRAINING
Undeveloped OPSEC and collaboration

85%
have received little or no training in OSINT techniques and risk prevention from their current employer

34%
don't have any prior experience with OSINT-related research

77%
are not receiving recurring OSINT training or certification as part of their role

INSUFFICIENT TOOLS
Exposure to counterintelligence and exploits

83%
use a web browser as their primary tool for conducting research

55%
are venturing into the dark web 10 or more times per month

38%
do not use managed attribution tools to mask or hide their online identities or personas

LACK OF OVERSIGHT
Potential compliance violations or abuse of resources

29%
report no oversight procedures to ensure that tools are not being abused by analysts

62%
report that audits are not a regular occurrence or there is no audit process

17%
implement a redundant analyst program for continuity and oversight

"Threat intelligence practitioners are at the front lines, and if they're not equipped properly, their actions can put organizations at risk."

- Scott Petry, Co-founder and CEO of Authentic8

GET THE REPORT

Silo for Research (Toolbox) is a secure and anonymous web browsing solution that enables users to conduct research, collect evidence, and analyze data across the open, deep and dark web. Silo for Research is built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

Research teams can accomplish their goals without introducing risk to the organization or revealing intent. All web activity is logged and encrypted so compliance teams can be sure that the tools are being used appropriately. Learn more at www.authentic8.com or contact info@authentic8.com to request a personalized demo.

silo By Authentic8

Google Cloud Partner

Cybersecurity INSIDERS

www.authentic8.com

www.cybersecurity-insiders.com