



AI in CyberSecurity **Overview**

Presenter:

Alex Johnson – Senior Systems Engineer

Agenda

Spot AI-Powered Attacks Early

How to recognise the tell-tale signs of AI-driven phishing, fraud, and social engineering.

Deploy AI Defences Effectively

Practical ways AI can cut false positives, surface real threats faster, and support lean security teams.

Upskill Teams for the AI Era




The new skills security analysts need as their role shifts from manual investigation to validating AI-generated alerts.



TL;DR

AI will be Speed and Efficacy to Security

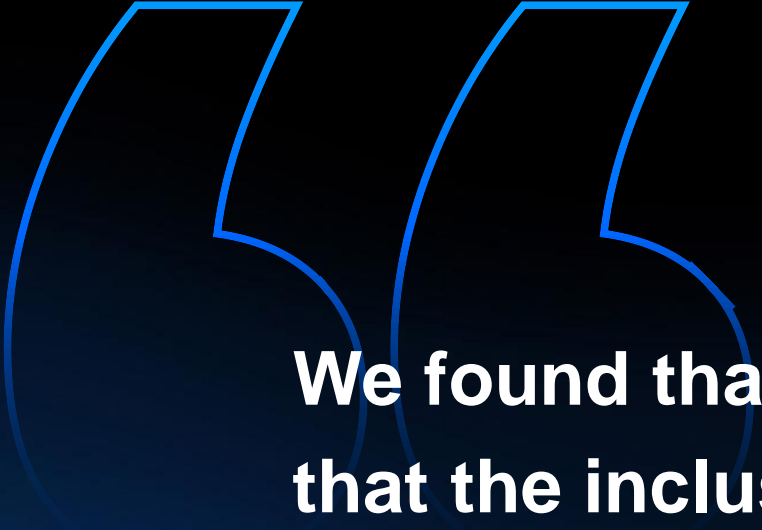


efficacy	vs	efficiency	vs	effectiveness
I can do it right.		I can do it quickly and economically.		I can do it well.
				
				YOURDICTIONARY



**We Recently
Surveyed 2000
Organizations**



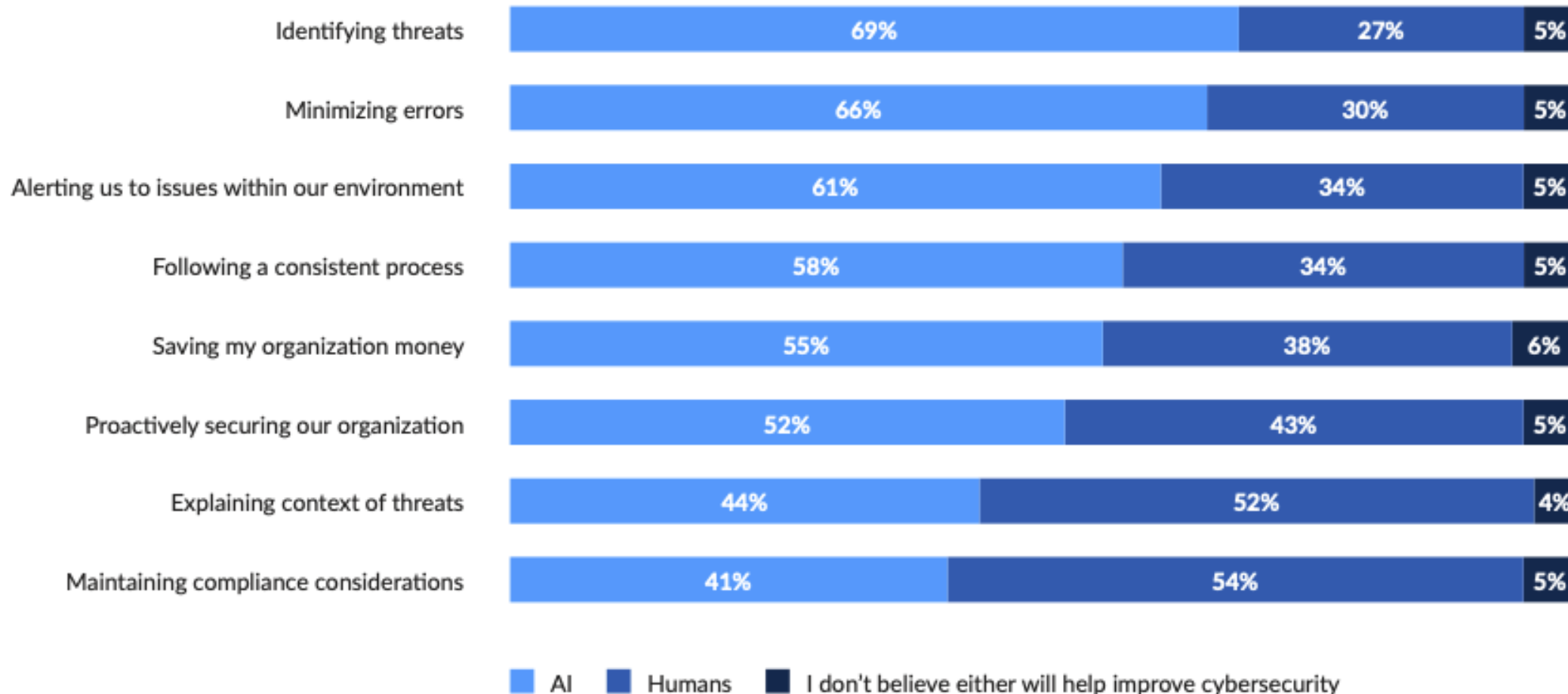



We found that 93% of organizations indicated that the inclusion of artificial intelligence will influence some portion of their cybersecurity investment decisions over the next 12 months. This shows us that, as leaders plan and budget for their future cybersecurity needs, AI will be a critical factor in their decision-making process.



Spot AI-Powered Attacks Early

Which do you think is more capable of helping to improve cybersecurity at your organization?



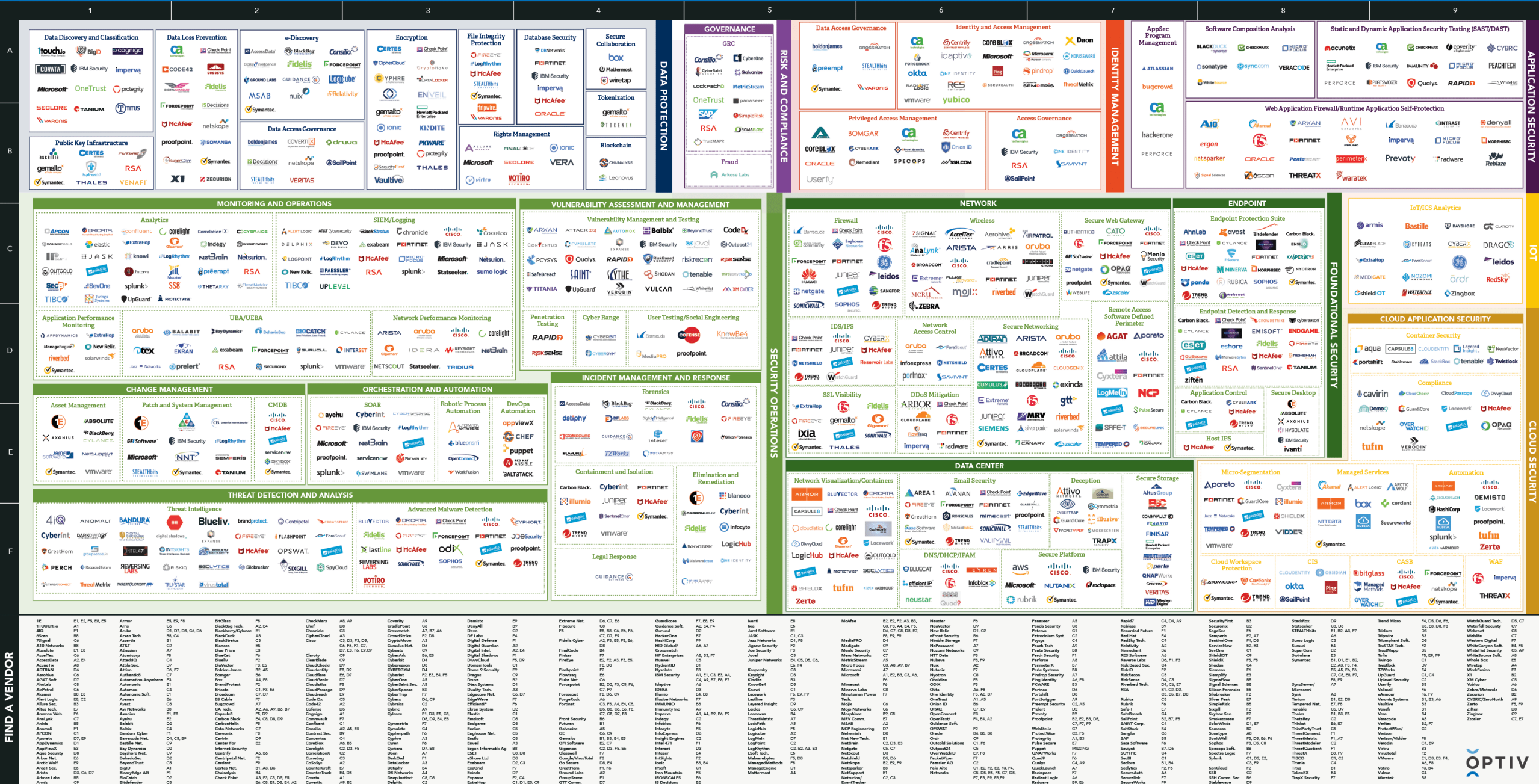


99% Of organizations we surveyed say
**Cybersecurity Purchases Will Be Influenced by AI
Capabilities**



Optiv Cybersecurity Technology Map

Navigate Cybersecurity at [Optiv.com](https://www.optiv.com)



Application Security

Application Security

WAF & Application Security

Application Security Testing

The diagram displays a comprehensive list of AppSec tools and services, categorized into three main functional areas:

- Application Security:** Includes logos for AIO, Akamai, ARXAN, Barracuda, CLOUDFLARE, CONTRAST SECURITY, DB APP SECURITY, ergon, fastly, FORTINET, FORTRA, imperva, Kaspersky, netsparker, NETSPI, onapsis, ORACLE, paloalto, Penta SECURITY, perimeterx, portshift, PROMON, Protego, Qualys, radware, RAPID7, Reblaze, riverbed, RUNDOSCHWARZ, safe-i, SEWORKS, SHIELD, sqreen, STACKPATH, SUCURI, TEMPLARBIT, THREATX, TREND MICRO, Trustwave, VERACODE, and VERNIA.
- WAF & Application Security:** This section is represented by the same set of logos as the 'Application Security' section, indicating that these tools often encompass WAF capabilities.
- Application Security Testing:** Includes logos for acunetix, ASSET SECURITY, BLACK BOX, CHECKMARK, DIGIVANTE, ERPScan, Fasoo, FORTRA, hackerone, HCL SOFTWARE, IBM, kryptowize, MICRO FOCUS, N-STALLER, NewSecure, onapsis, OX, PARASOFT, PERFORMANCE, PORTSWIGGER, Qualys, RAPID7, rezilion, SECURITY COMPASS, ShiftLeft, SiteLock, snyk, sonarsource, Synack, SYNOPSIS, tenable, Trustwave, VERACODE, WhiteHat, and WhiteSource.

Mobile Security

[illegible]

Messaging Security

AREA 1

- BlackBerry
- CYREN
- FORTINET
- GreatHorn
- IRONSCALE
- MICRO FOCUS
- HortonLife.COM
- SONICWALL
- TREND MICRO
- VALIANTMAIL

B2B SYSTEMS

- CISCO
- PIREYE
- FORTRA
- malguard
- Microsoft
- proofpoint
- SOPHOS
- Trustwave
- votiro

Other vendors shown:

- Barracuda
- CYBERO
- Forcepoint
- GoSecure
- INKY
- Material
- mimicast
- Susa Software
- Trellix
- Vode Secure
- WEBROOT

Security Consulting & Services

A collage of various technology and security company logos, including Deloitte, Cisco, Oracle, Microsoft, and others.

Deploy AI Defences Effectively

Regions considering adding AI-informed technology for breach response readiness are:

↑ The top three

01. The U.S. ~56%
02. U.K. and Ireland ~54%
03. Austria, Switzerland, and Germany ~51%

↓ The bottom three

01. South Africa, Australia, and **New Zealand** ~49%
02. Belgium and the Netherlands ~44%
03. Denmark, Sweden, Norway, and Finland ~38%



The Network Is No Longer The Perimeter

How and where do your users connect today?

- ✓ Zero Trust is becoming the new norm.
- ✓ AI should be on the workstation and server to identify attacks pre-execution
- ✓ Security operations should be the catchall safe pair of hands
- ✓ SOC should be using AI to ensure fast and accurate time to response



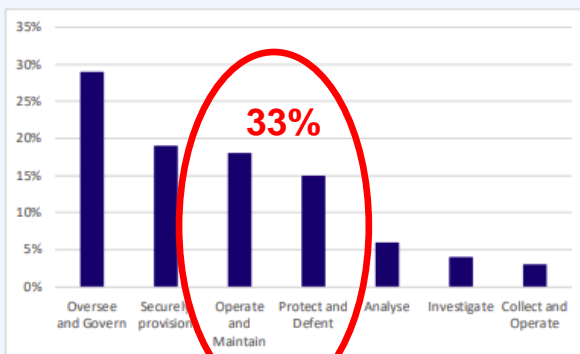
Upskill Teams for the AI Era

How are you going to upskill your security teams if you cant find them?

- **10,818** cyber security professionals (ABS Census 2021 – 7xANZCO categories)
- **4,356** cyber operations specialists (ABS Census 2021 - ANZCO 262116/18)
- AISA membership ~12,000 members
- ~**30,000** per Austcyber
- **3305** CISSPs per ISC2 (2022)

- ISC2 : **25,000** short today
- National Skills Commission : **30,000** short over 4 years
- Austcyber :
 - **7000** short in 2023
 - **16000** short by 2026

Figure 1: Distribution of cyber security workers across role focus (Australia)



Source: (ISC)2* (2021)

4,356 cyber operations specialists.
~850 in NZ



Hiring top-tier cybersecurity talent remains a widespread challenge that organizations face as part of developing security programs. Now, many leaders are looking for alternatives to hiring as a way of overcoming this “security skills gap.” One possibility being considered is the adoption of AI to maximize the talent of the staff they are able to hire:

73%

Believe in the promise of AI in cybersecurity and are already implementing AI-driven solutions; with 79% taking this approach because they believe AI will improve their ability to detect new threats.

54%

Recognize that maximizing AI’s potential may require changes, namely upskilling their teams to manage AI.



Organizations recognize changes are needed to accommodate the increase in AI-powered cybersecurity systems, with almost half (49%) expecting AI adoption to mean their analysts will waste less time on low-level or repetitive tasks. These analysts are then expected by a similar percentage (46%) to transition into acting more as alert validators, reviewing and verifying AI outputs as the technology focuses on the repetitive, granular work at increased speeds.

More than half of respondents though, or 52%, expect in-house teams will need to upskill to better manage AI technology.

96%

of organizations expect AI adoption to change their team's workflow or responsibilities.



Thank You

END
CYBER
RISK