brigantia

Welcome to the

Insider Threat Roadshow

brigantia

York
Birmingham
London

Insider Threat Roadshow

brigantia

Welcome to the

Insider Threat Roadshow

Ed Knox
Senior Product Specialist

Trusted cybersecurity distributor

Why Brigantia?

Traditional distribution is broken.

- **Quality products**
- **Trusted advisors**
- **Strong partnerships**

Why Brigantia?

Quality Products

- **Quality over reputation**
- **Rigorously tested**
- **Quality over quantity**

Why Brigantia?

Trusted Advisors

- Peerless knowledge
- Dedicated product specialists
- Tailored support

Why Brigantia?

Trusted Advisors

- **Meaningful relationships**
- **Flexible**
- **Adding value**

Technology Partners

CONCEAL

CyberSmart

Heimdal®

HORNETSECURITY

ITagree

KEEPER®

KnowBe4
Human error. Conquered.

next

OCTIGA
Office365 Security

redstor™

Rootshell
Security

SENDMARC

Action1

ARISTA
Edge Threat Management

eSENTIRE

IronVest
The freedom of protection

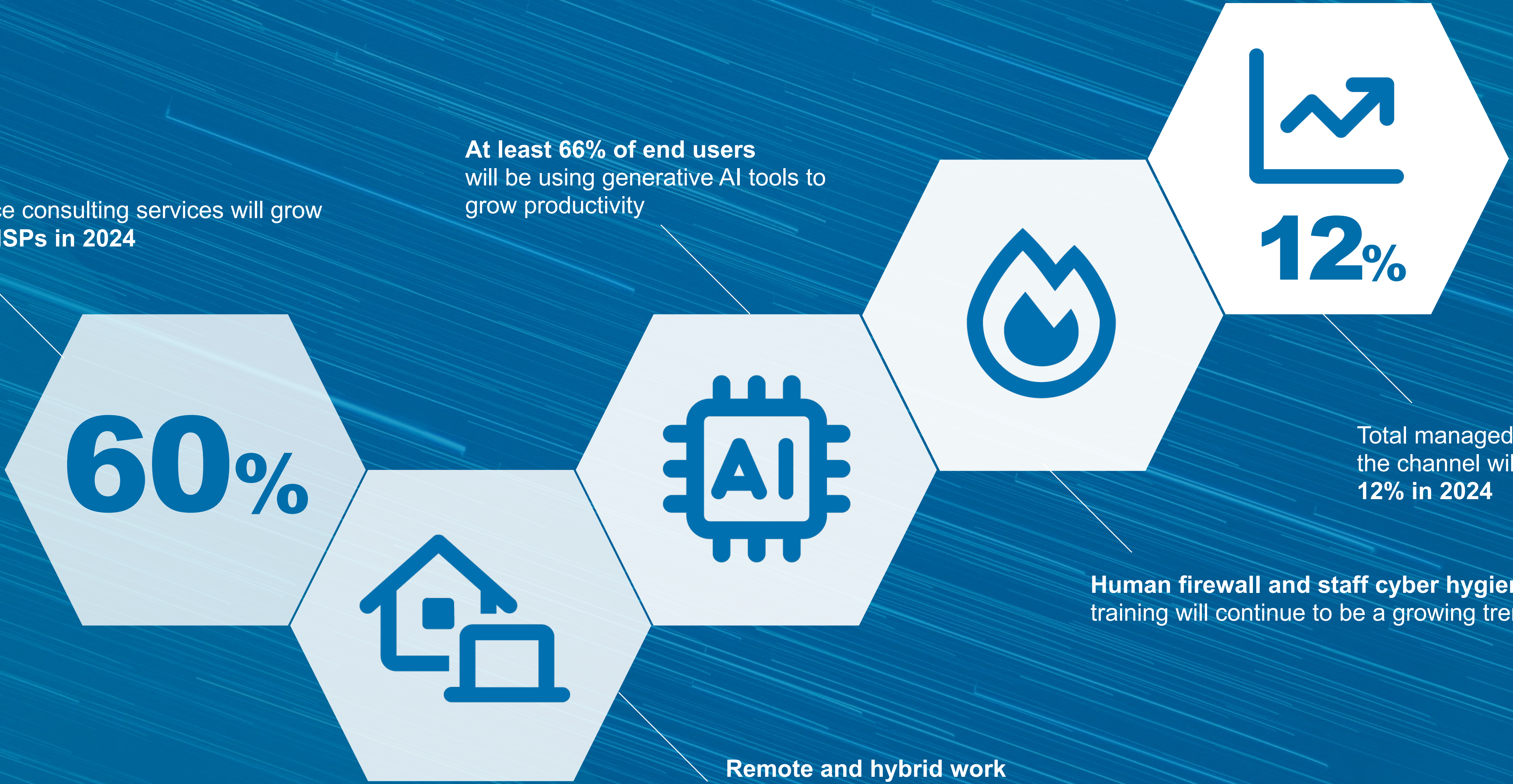
Parallels®

TRILLION
Powered by Crossword Cybersecurity

Agenda for the day

09:00 – 09:30	Registration & coffee
09:30 – 09:45	**Welcome and update from Brigantia**
09:45 – 10:00	**Brigantia** “Protecting from the inside out ”
10:00 – 10:30	**Hornetsecurity** "The importance of Microsoft 365 and how to protect against insider risk"
10:30 – 11:00	**Next DLP** “The dangers of unintentional insiders”
11:00 – 11:30	Break for coffee & networking
11:30 – 12:00	**Guest Speaker**
12:00 – 12:30	**Conceal** “Detecting insider threats within the browser”
12.30 –1300	**Sendmarc** "Bulletproofing Business Email: DMARC Solutions for MSP Clients"
13:00 – 14:00	Lunch & networking

Why have we put this event on?



Compliance consulting services will grow **60% for MSPs in 2024**

At least 66% of end users will be using generative AI tools to grow productivity

Remote and hybrid work will continue to be offered by employers

Human firewall and staff cyber hygiene training will continue to be a growing trend in 2024

Total managed services revenue in the channel will grow at least **12% in 2024**

What is Insider Threat?

- An insider threat is a risk posed by those who have access to an organisation's physical or digital assets.

- These insiders can be anyone who has or had authorised access to an organisation's network and computer systems.

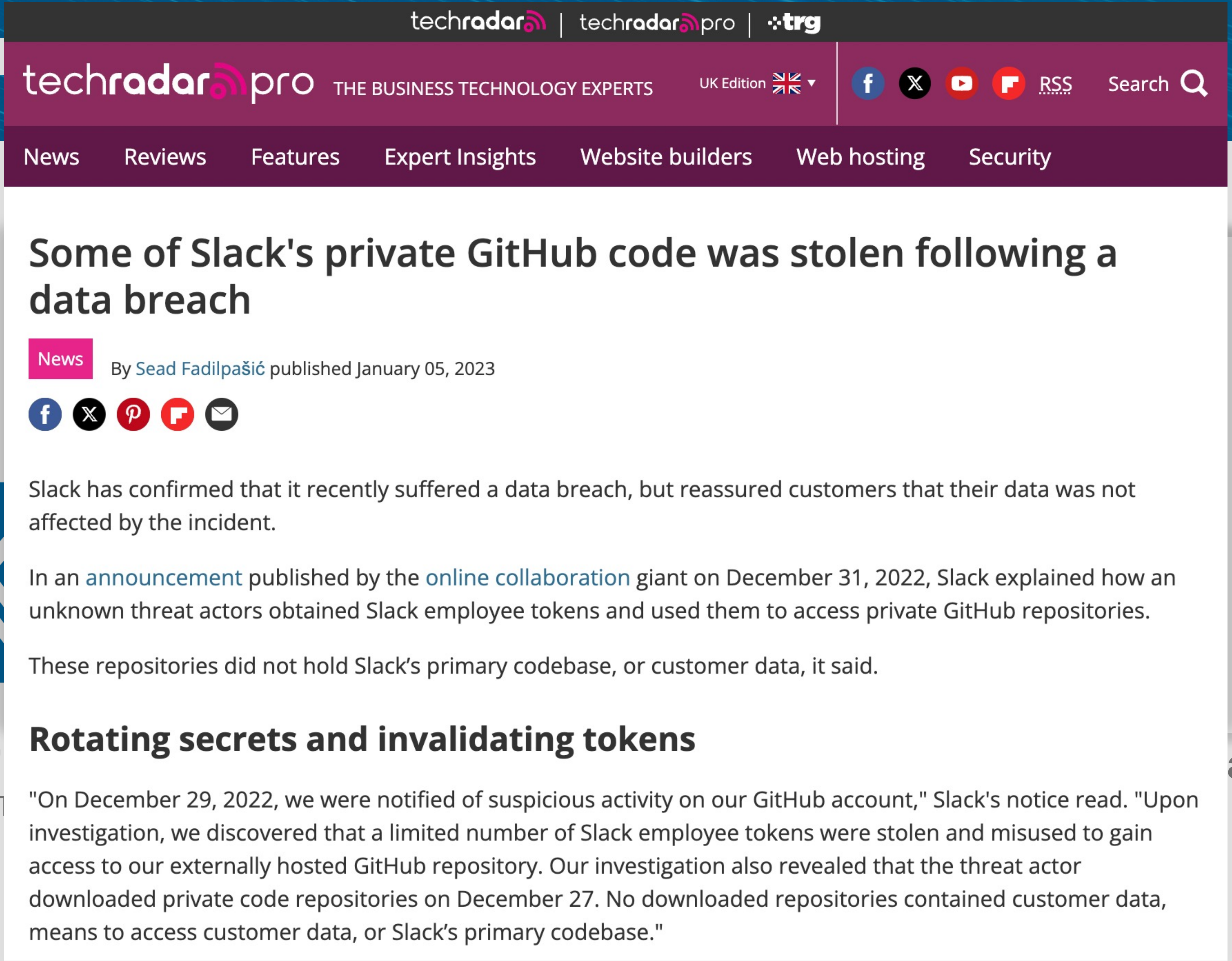
- The consequences of a successful insider threat could be a data breach, fraud, theft of trade secrets or intellectual property, or disruption of security measures.

Types of Insider Threat

Current employees	These could use privileged access to steal sensitive or valuable data for personal financial gain.
Former employees	Working as malicious insiders could intentionally retain access to an organisation's systems or pose a security threat by sabotaging.
Malicious actor (Cybercriminal)	Are external threat actors who gain the confidence of a current employee to get insider access to systems and data. Often, they're from an outside organisation hoping to steal trade secrets. Social engineering is a commonly used tactic to gain unauthorised access.
Unintentional insider	Caused by employees who inadvertently pose a significant risk because they don't comply with corporate security policies or use company systems or data in a negligent manner. While unintentional, negligent insiders can open the door to external threats, like phishing attacks, ransomware, malware or other cyber-attacks.

Real wo

brigantia



techradar | techradar pro | trg

techradar pro THE BUSINESS TECHNOLOGY EXPERTS UK Edition RSS Search

News Reviews Features Expert Insights Website builders Web hosting Security

Some of Slack's private GitHub code was stolen following a data breach

News By Sead Fadilpašić published January 05, 2023

Slack has confirmed that it recently suffered a data breach, but reassured customers that their data was not affected by the incident.

In an announcement published by the online collaboration giant on December 31, 2022, Slack explained how an unknown threat actors obtained Slack employee tokens and used them to access private GitHub repositories.

These repositories did not hold Slack’s primary codebase, or customer data, it said.

Rotating secrets and invalidating tokens

"On December 29, 2022, we were notified of suspicious activity on our GitHub account," Slack's notice read. "Upon investigation, we discovered that a limited number of Slack employee tokens were stolen and misused to gain access to our externally hosted GitHub repository. Our investigation also revealed that the threat actor downloaded private code repositories on December 27. No downloaded repositories contained customer data, means to access customer data, or Slack’s primary codebase."

‘X’

Formerly T

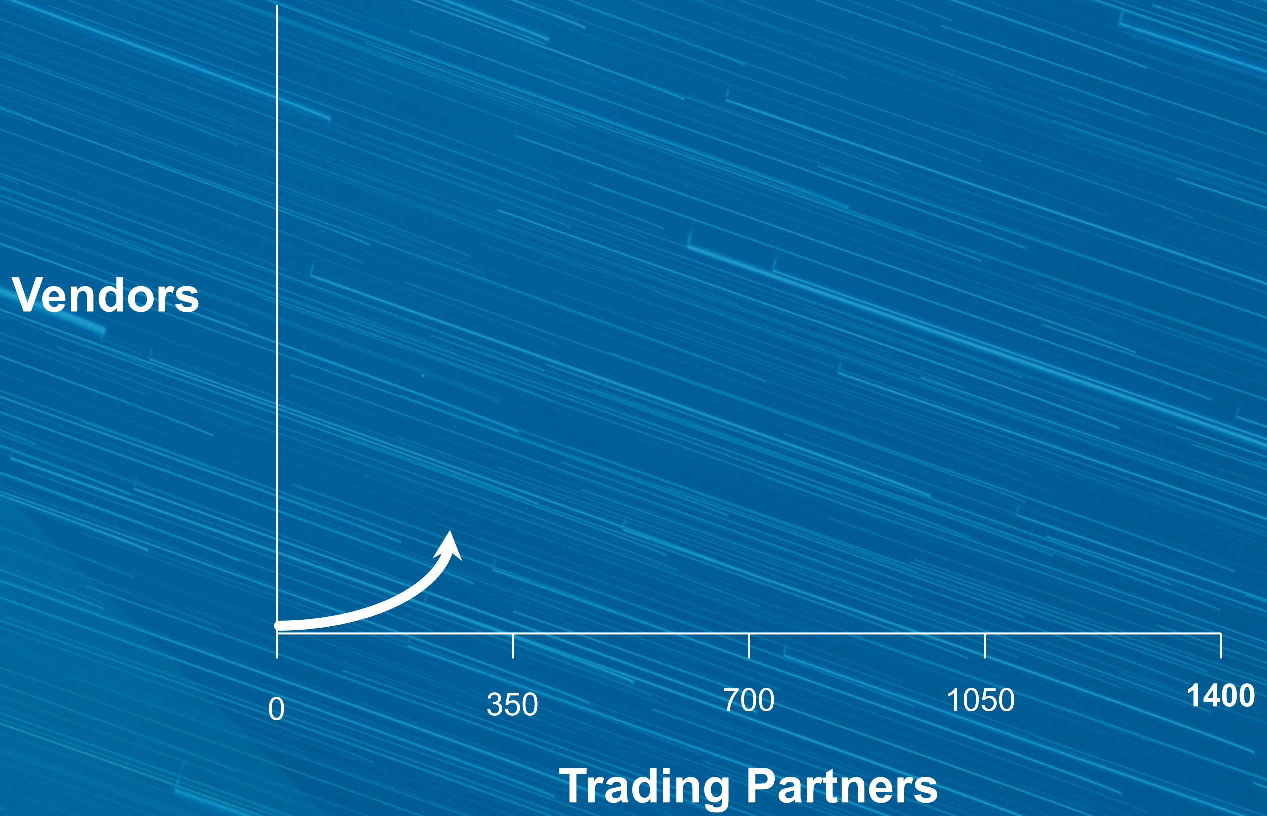
ack

Why do I need to protect my customers?

- Data Breach
- Fraud and Sabotage
- Compliance Violations
- Unauthorised Access
- Phishing and Social Engineering
- Employee Negligence

Opportunity for channel

- The channel is underprepared!! Opportunity for revenue



brigantia

Thank you