RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART4-W08**

AI, ML and the Gig Economy — the Only Path Forward for the SOC

Gunter Ollmann

Chief Security Officer
Devo
@gollmann

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

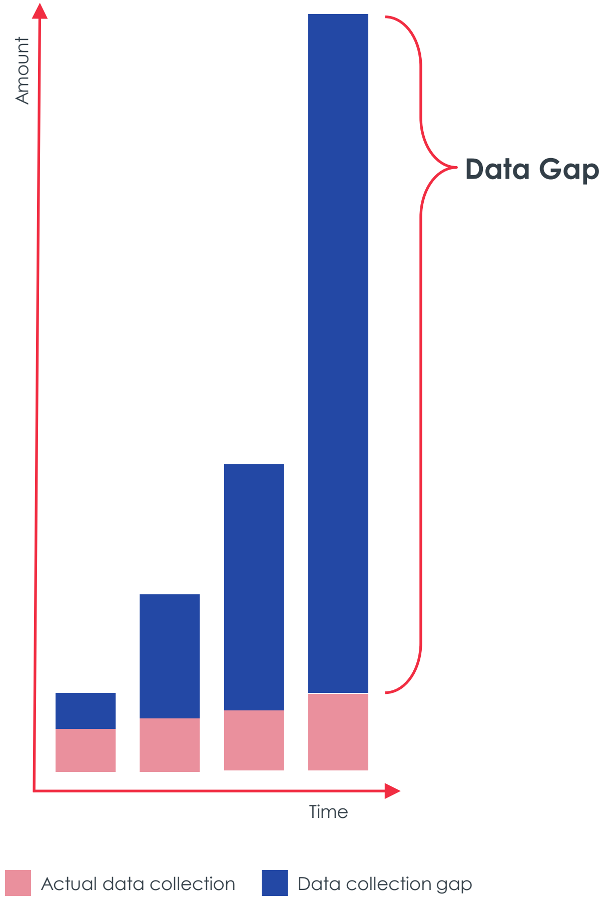
Agenda

- Up-level your team with AI and new work models
- Get real with security-focused AI
- Gig workers: how they fit into the security picture
- The successful path forward for the SOC

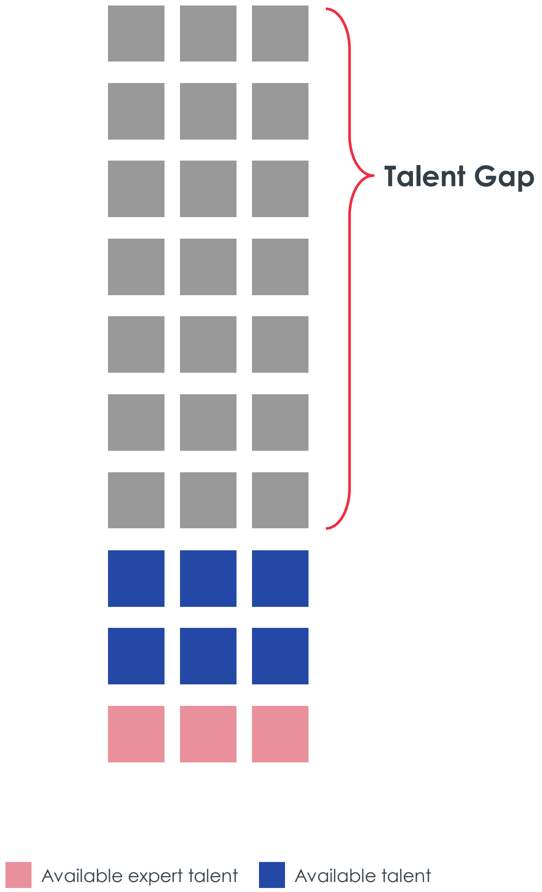
Assume breach, but can your team handle that?

A new approach is needed to close critical security operations gaps

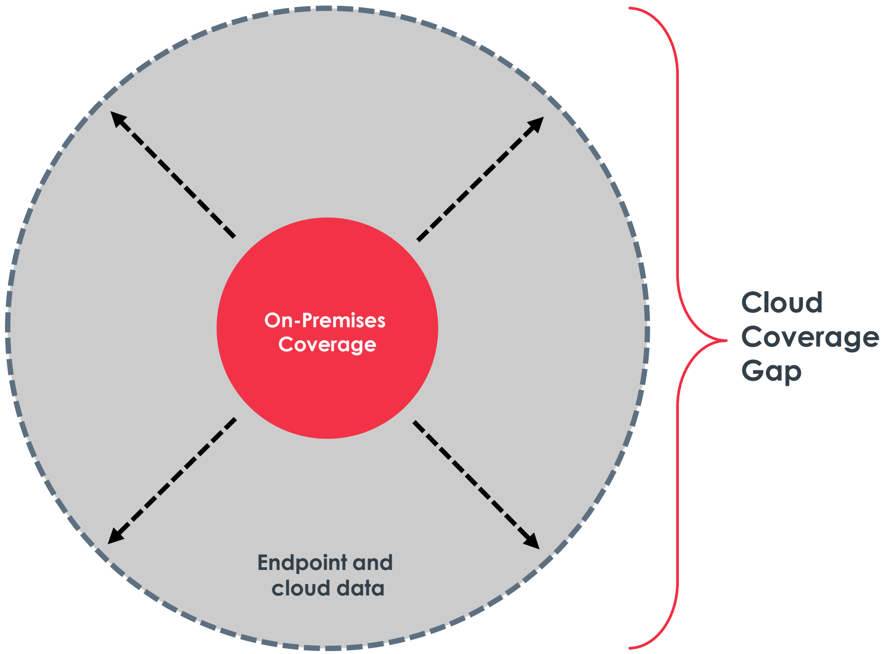
Data



Talent



Attack Surface



So, how can you up-level your team?

ML and Automation

Gig Economy

Getting real with security-focused AI

The current state of AI

- Pre-trained classifiers & NLP
- Cloud vendor unsupervised learning on data lakes

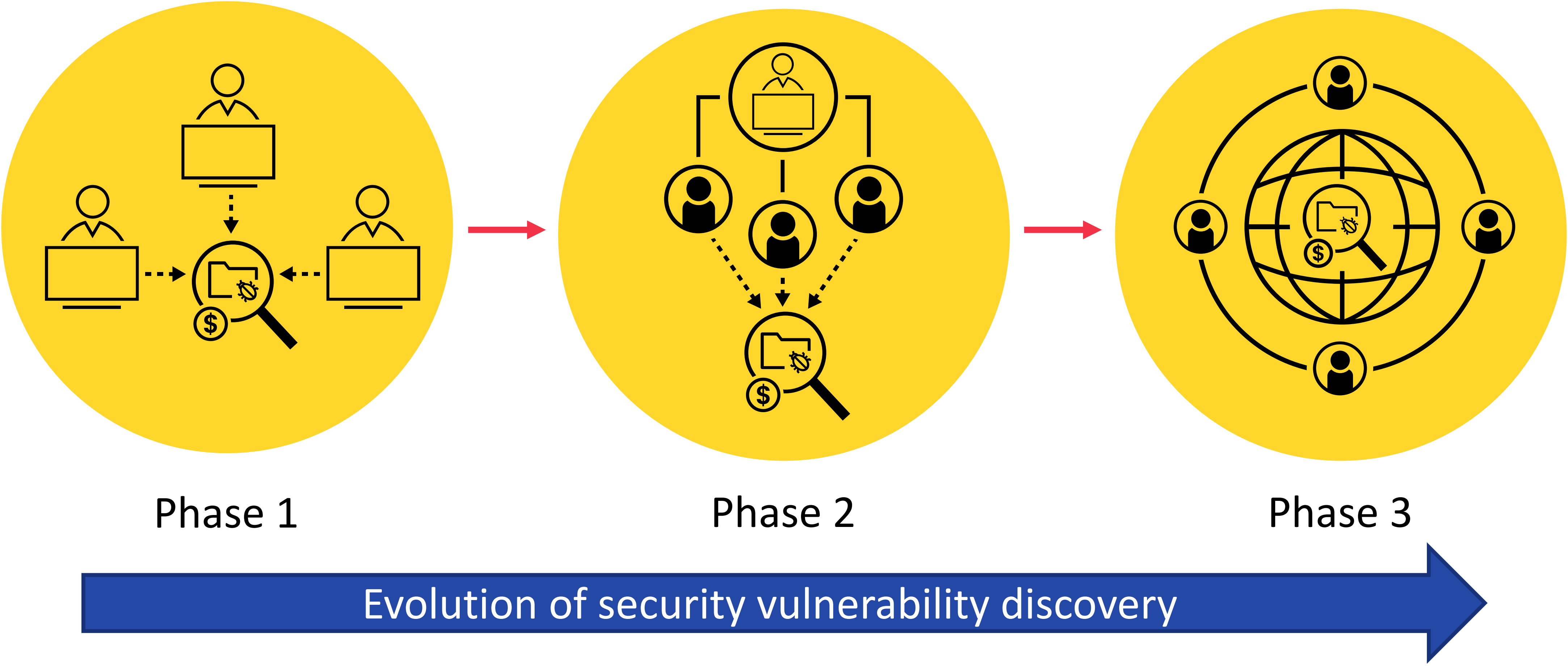
What's coming next

- Augmented intelligence
- Explainable AI
- Adversarial AI
- AI-as-code

What this means for you

- More advanced AI in-hand
- In-house AI adoption
- Community-sourced models

Gig workers: how they fit into the security picture



The building blocks for tomorrow’s SOC

Machine Learning

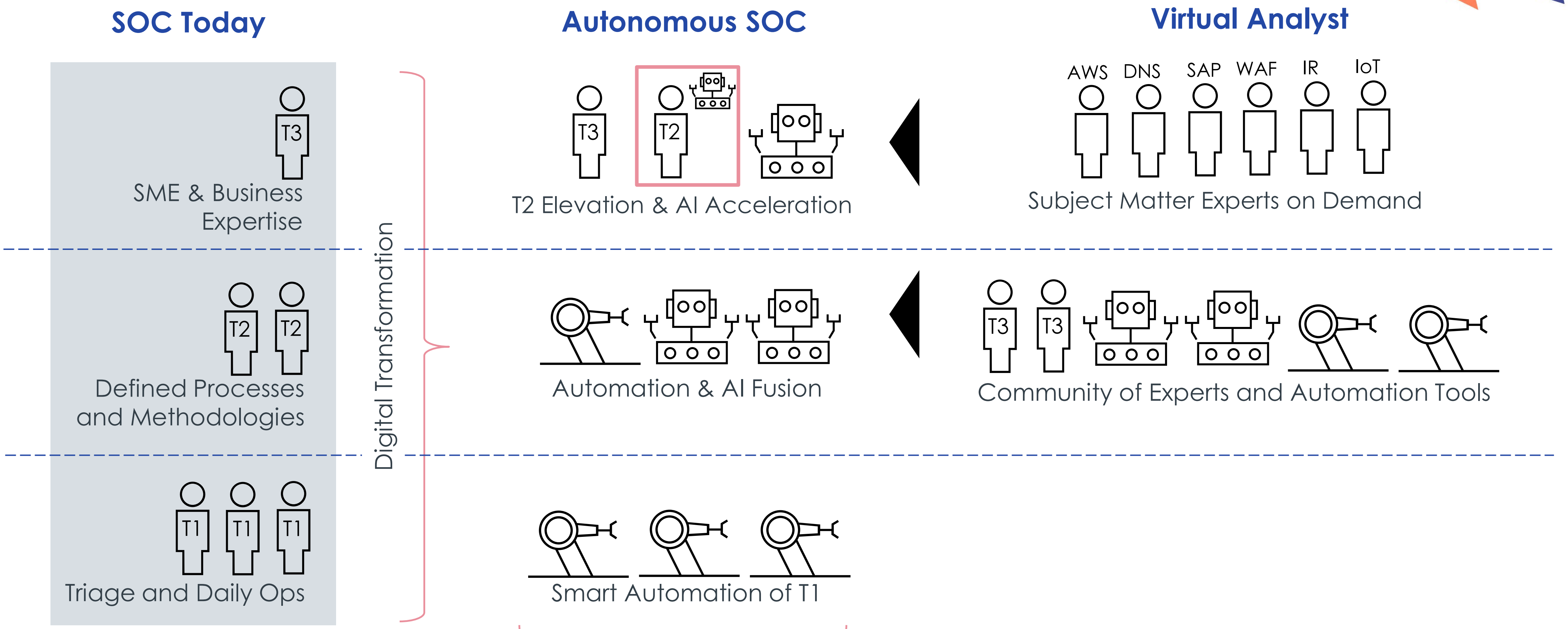
Artificial Intelligence

Data Science

Security Community

Global Security Analysts

Building the autonomous SOC



SOC Today

Autonomous SOC

Virtual Analyst

SME & Business Expertise

T2 Elevation & AI Acceleration

Subject Matter Experts on Demand

Defined Processes and Methodologies

Automation & AI Fusion

Community of Experts and Automation Tools

Triage and Daily Ops

Smart Automation of T1

Collective Defense

Observe, learn, hunt and respond across **all customers all the time**

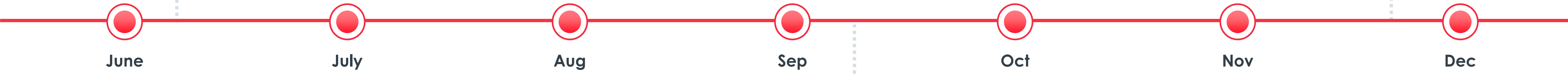
Apply what you've learned today

Next week

- Use the SOC metrics you already track to ID the top 3 most frequent threat types that require the most manual investigation & response

This year

- Evaluate technologies that provide the AI and automation that do this for you automatically



June July Aug Sep Oct Nov Dec

In the next few months

- Automate away those three, and tackle the next chunk

Key takeaways

Embrace AI

- Opportunity to guide SOC analysts and preemptively enrich a threat investigation, speeding response

Adopt an incident-first mindset

- Don’t just filter, correlate, and aggregate alerts; contextualize both events and alerts as an incident

Use the community

- Leverage the global pool of expert talent and embrace future “phone-a-friend” and on-demand expertise models

Get in touch with us!

- Visit us at booth 3241 in the South Hall
- Follow and engage with us on
  - Twitter – @devo_inc
  - LinkedIn – Devo
- Email us at rsa2022@devo.com