



Microsoft Security

USER GROUP

Who we are



Craig Forshaw
Azure Solutions Architect
@ Atea



Hafliði Fríðthjofsson
Senior Cloud Architect
@ Sopra Steria



Anders Kristiansen
Azure Security Lead
@ Devoteam M Cloud



Sanna Diana Tomren
Cloud Security Lead
@ Accenture



Microsoft Security USER GROUP

Connect & follow



github.com/msugn



<https://linkedin.com/company/msug>



<https://www.youtube.com/@MicrosoftSecurityUserGroup>



<https://twitter.com/MsSecUG>



<https://www.meetup.com/Microsoft-Security-User-Group/>

Call for speakers

<https://sessionize.com/microsoft-security-user-group-2024>

Why we do it



Have fun



Build network



Share knowledge



Learn from each other

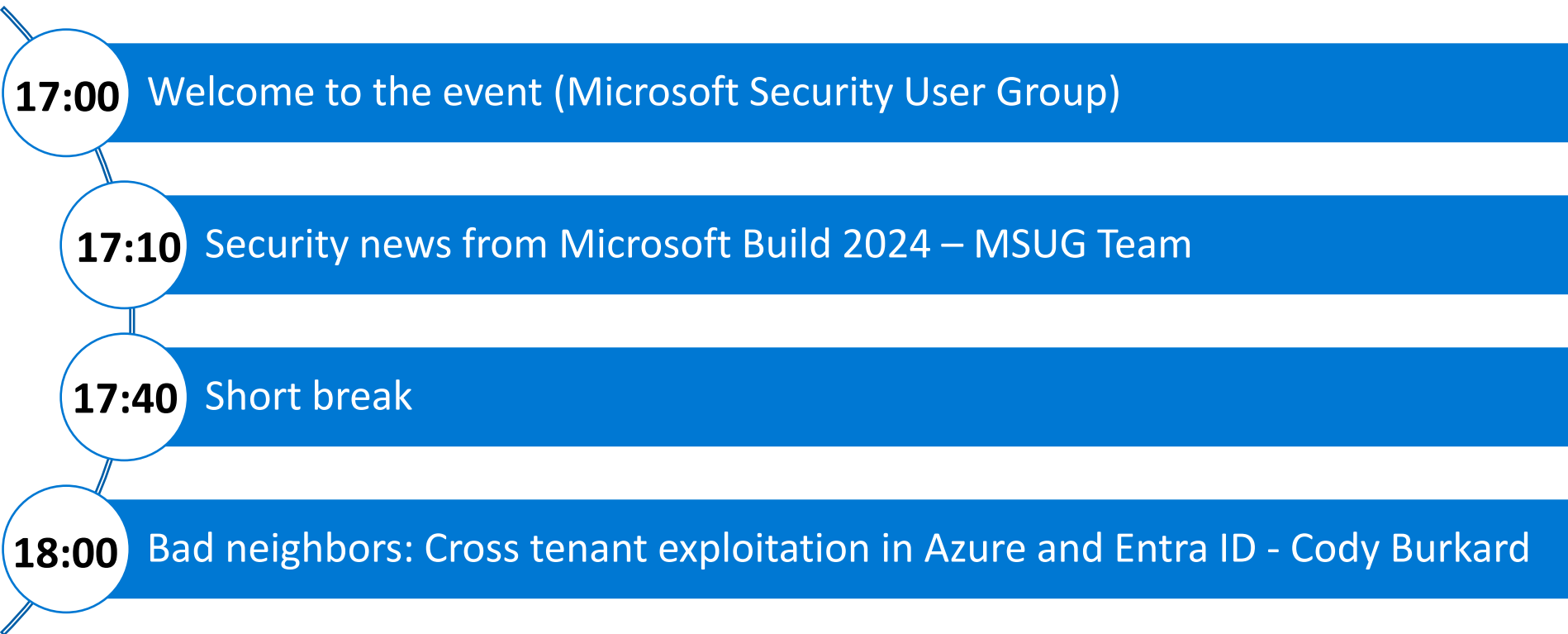


Giving power to the community



Develop technology for a secure and sustainable future

Event agenda



Thank you to
our sponsors
for this event



ATEA

Rebel

Sign up for our next event 24.06 11:00 CET

Virtual Lunch Meetup: Strengthening Cyber defence with AI and Microsoft Copilot

Speaker



Mark Jones

Mark Jones is Head of Cyber Security at Chorus, a UK-based MSSP delivering Microsoft MDR & MXDR services globally.

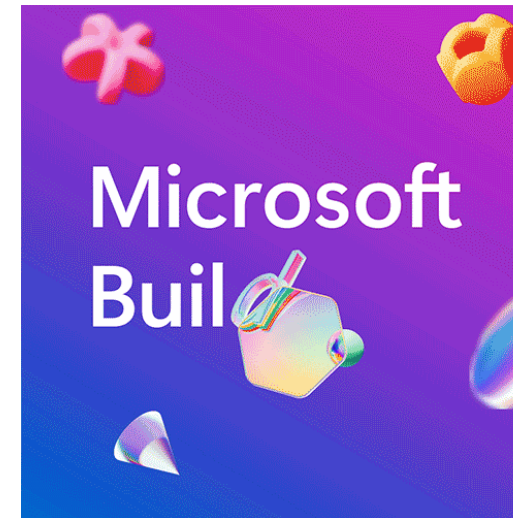


Microsoft Build



What is Microsoft Build?

- Annual flagship event for Software Engineers and Web Developers using Windows, Azure and other Microsoft technologies
- First held in 2011, and it serves as a successor for Microsoft's previous developer events;
 - The Professional Developers Conference (*an infrequent event which covered development of software for the Windows operating system*) &
 - MIX (*covered web development centering on Microsoft technology such as Silverlight and ASP.net*)
- Focus in 2024: Artificial intelligence and its integration across Microsoft's products and services
- **Microsoft Build 2024 Book of News**
 - The goal with the Book of News is to provide you with a roadmap to all the announcements we're making, with all the details you need
- **Microsoft Learn challenge**
 - Build Edition Registration | Microsoft Learn Challenge: Build Edition
 - May 21 - June 21, 2024



Our picks from Microsoft Build



Session Dive: Inside AI Security with Mark Russinovich – Craig





What's AKS Automatic & Azure Deployment stacks – Anders

Session Dive

Inside AI Security with Mark Russinovich

Tuesday, May 21 | 10:00 PM - 10:45 PM Central European Summer Time
Duration 45 minutes

 BRK227

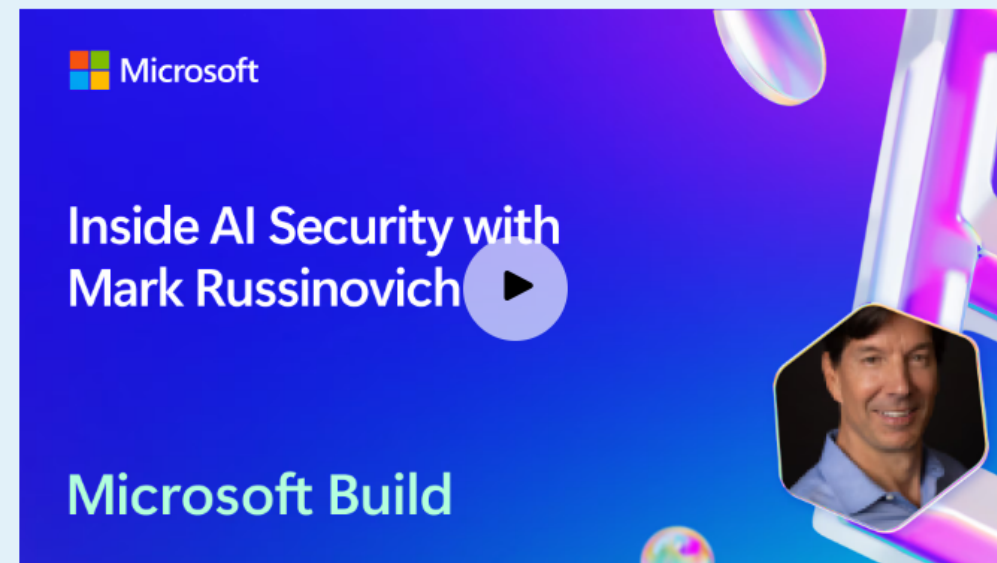
 Breakout

In Seattle + Online

Speaker:



[Mark Russinovich](#) | [Microsoft](#)



Join Mark Russinovich to explore the landscape of AI security, focusing on threat modeling, defense tactics, our red teaming approaches, and the path to confidential AI. You will learn about various kinds of attacks in AI systems and our defenses, such as backdoors, poison data, prompt injection attacks, and more.

Generative AI threat map

MITRE ATLAS

OWASP Top 10 for LLM

MSRC AI Bug Bar

OWASP Top 10 for ML



AI usage security

User interaction with generative AI-based apps

Sensitive information disclosure

Shadow IT/harmful third-party LLM-based app or plugin

Jailbreak

Generative AI extended risks

AI insider risk, attack path, multimodal, overreliance



AI application security

Generative AI-based app lifecycle

Indirect Prompt Injection Attack

Data leak/exfiltration

Insecure plugin design



AI platform security

Foundation model and training data

Training data poisoning

Model theft

Inherent LLM risks

Imaginative but > Unreliable

Suggestible and > Literal-minded

Persuadable and > Exploitable

Knowledgeable yet > Impractical

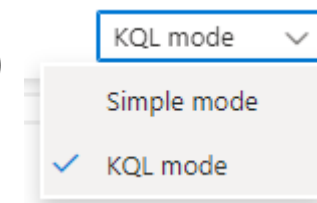
AKS Automatic

AKS Automatic ([learn](#))

- Comes with a bunch of predefined design decisions:
<https://landscape.cncf.io/>
- Improved security posture:
 - AKS RBAC enabled, SSH disabled.
 - Automatic updates
 - Node resource grp lockdown (no tampering, config, preview)
 - Keyvault provider is installed by default. (get secrets, certs into cluster)
 - Image cleaner (removes vulnerable images, open source eraser)
 - Workload identity enabled
 - Deployment safeguard (enforce best practice with az policy)
- Can be flipped to azure standard if you need full flexibility 😊

News in Observability:

- Public Preview: Kubernetes Metadata & Logs Filtering in Azure Monitor-Container Insights
- [Log analytics Simple Mode](#) ([Demo](#))



Azure Deployment stacks GA!



- Current challenges:
 - Lifecycle management / Cleanup
 - Lack of deny assignments (blueprint is not the solution, in deprecation)
- Collection of managed resources (all must be children of scoped resource)
- A stack will share a common lifecycle.
- Reuse existing templates using az stack command.
- Deny rules can exclude up to 5 principals, and 200 actions (tags, etc)
- 3 different actions

Action on unmanage *

- ☒ **Detach all**
detach all unmanaged resources, resource groups, and management groups from the Deployment Stack
- ☐ **Delete all**
delete all unmanaged resources, resource groups, and management groups from the Deployment Stack
- ☐ **Delete resources**
delete all unmanaged resources from the Deployment Stack and detach resource groups and management groups

Your feedback
is needed!
Menti code
3543 4019



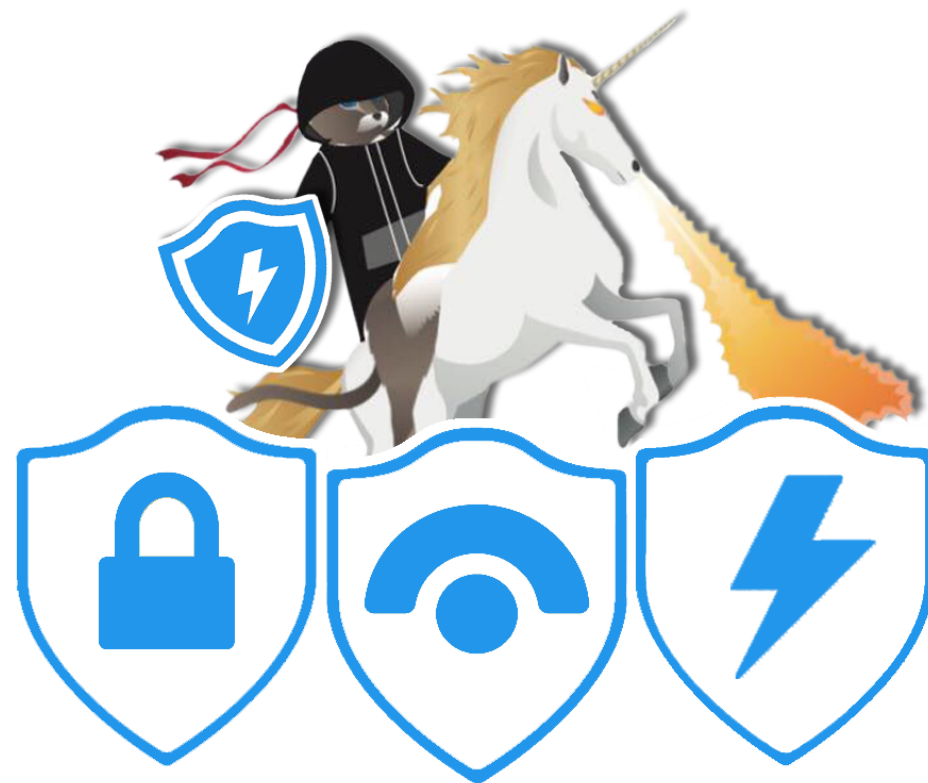


15 min break

Call for speakers

<https://sessionize.com/microsoft-security-user-group-2024>





Microsoft Security

USER GROUP