



# NAVIGATING SECURITY OPERATIONS IN THE CLOUD ERA

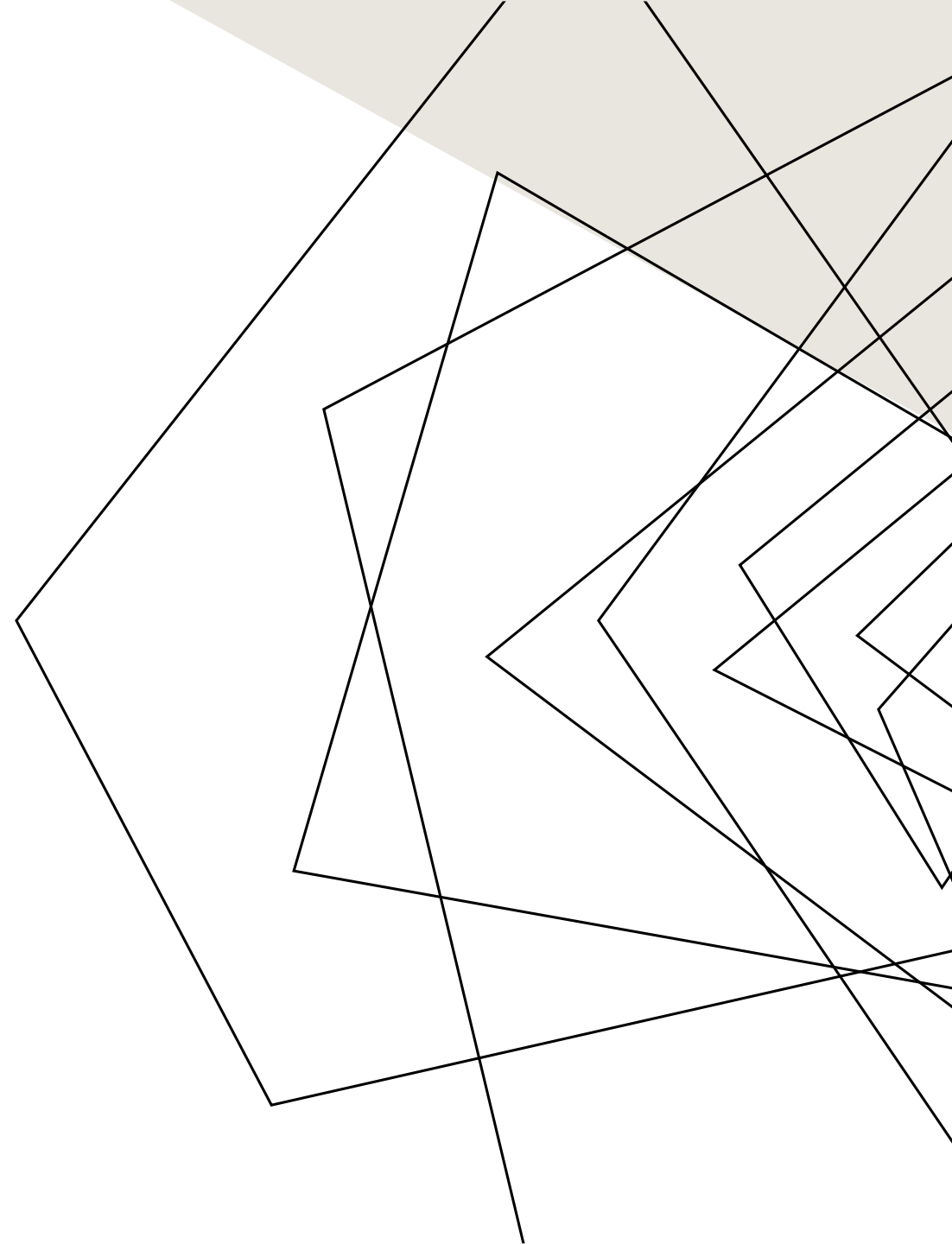
ESRA YILDIZ

# ABOUT ME

Esra Yildiz

Security Cloud Solution Architect at Microsoft

Interests: Cloud Security and SIEM, XDR, CSPM,  
now AI too





## WHAT WE WILL COVER TODAY?

How security operations is affected from cloud transformations?

- Top 5 security risks in the cloud
- Challenges and opportunities
- Real world examples
- Q&A

# 1. ATTACK SURFACE X

## On-prem:

- Well-defined
- Limited by the organization's physical network
- Stable number of assets

## Cloud:

- Multiple cloud vendors
- External resources and apps such as SaaS
- Rise of AI

## Risk: Growing Attack Surface

- Assets are scattered all over the internet with many dependencies.
- Lack of standardization, losing control and visibility.

## 2. DIFFERENT TYPE OF WORKLOADS (UNFAMILIARITY)

### On-prem:

- Well-known
- Limited number of long-lived assets
- VMs, Networks, Databases, etc.

### Cloud:

- New workload types, new risks
- Cloud control plane, layers like identity, network
- Serverless functions, APIs
- Short lived assets

### Risk: Unfamiliarity

- “You can’t protect if you don’t know what you are protecting”
- Lack of context for the security teams

# 3. IDENTITY & ACCESS MANAGEMENT

## On-prem:

- Network perimeter
- Design, deploy, maintain

## Cloud:

- Identity perimeter, adoption of Zero Trust
- IAM complexity – within across CSPs
- Management of user and machine identities

## Risk: Easier to login than hack in

- If you have the keys to the kingdom, you can't just enter it but reconfigure it

## 4. MISCONFIGURATIONS

### On-prem:

- Not easily reachable
- Done by a central team

### Cloud:

- Examples: excessive permissions, leaving ports unrestricted, etc.
- Configuration drifts
- Drifting to Non-compliance

**Risk: By far cloud misconfigurations are the biggest threat in the cloud world.**

- Misconfigured assets can be an easy way for the attackers to gain access
- It can cause an organization to fall into a non-compliance causing legal/regulatory issues

## 5. SHARED RESPONSIBILITY

### On-prem:

- Well known boundaries
- Most work is done by the organization itself

### Cloud:

- Vague boundaries of control and responsibilities
- Lack of visibility
- Knowledge gaps

### **Risk: Moving workloads to cloud does not guarantee security per default**

- Lack of visibility and knowledge gap in terms of who is responsible for security – CSP vs Organizations





## WHAT WE WILL COVER TODAY?

How security operations is affected from cloud transformations?

- **Top 5 security risks in the cloud**
  - Attack Surface, Different Workloads, IAM, Misconfigurations, Shared Responsibility Model
- Challenges and opportunities
- Real world examples
- Q&A

# SPEED AND AUTOMATION + AI TOO

## Challenge:

- Things are scalable and fast
- Attack surface x -> Increasing number of alerts

## Opportunity:

- Automation, integration and machine learning
- Shift to a more unified/platform approach
- Support of AI

**Technology used by the modern SOCs needs to be more “smart” to support the operations**

# HARDENING AND PREVENTION FIRST

## Challenge:

- More reactive mindset
- Detection and Response > value

## Opportunity:

- Proactiveness
- Predict and prevent > value
- Influence the design decisions
- Understanding secure IAC

**The ability of SOC teams to influence the design decisions from the beginning will reduce the likeliness of an attack dramatically**

# VULNERABILITIES – WHAT TO FIX FIRST

## Challenge:

- Fluctuating number of assets
- Misconfigurations and security drifts
- What to fix first?

## Opportunity:

- Automated patching
- Configuration Management is a new “discipline”
- Ability to collect and correlate data
- Contextual posture management

**Vulnerability management is rising and changing – new roles and discipline**

**Using power of cloud for intelligent prioritization and remediation**

# PEOPLE

## Challenge:

- Close as many ticket as possible as soon as possible

## Opportunity:

- Proactiveness and breaking the silos
- Co-work cross-functional security teams
- Distributed workforces

**A chance to glue security to the foundation**

**Breaking the isolation results in faster feedback cycles that will enhance the quality of detections and responses.**

**It is getting more important to employ people who can creatively solve security problems, rather than buying the best-in-class security technology and relying on the technology (not the people).**



## WHAT WE WILL COVER TODAY?

How security operations is affected from cloud transformations?

- **Top 5 security risks in the cloud** – Attack Surface, Different Workloads, IAM, Misconfigurations, Shared Responsibility Model
- **Challenges and opportunities** – Automation and Speed, Hardening and Prevention, Changing Vulnerability Management, People
- Real world examples
- Q&A



# REAL WORLD EXAMPLES

1.) As the SecOps team member, what are the 3 challenges you are facing when moving to cloud?

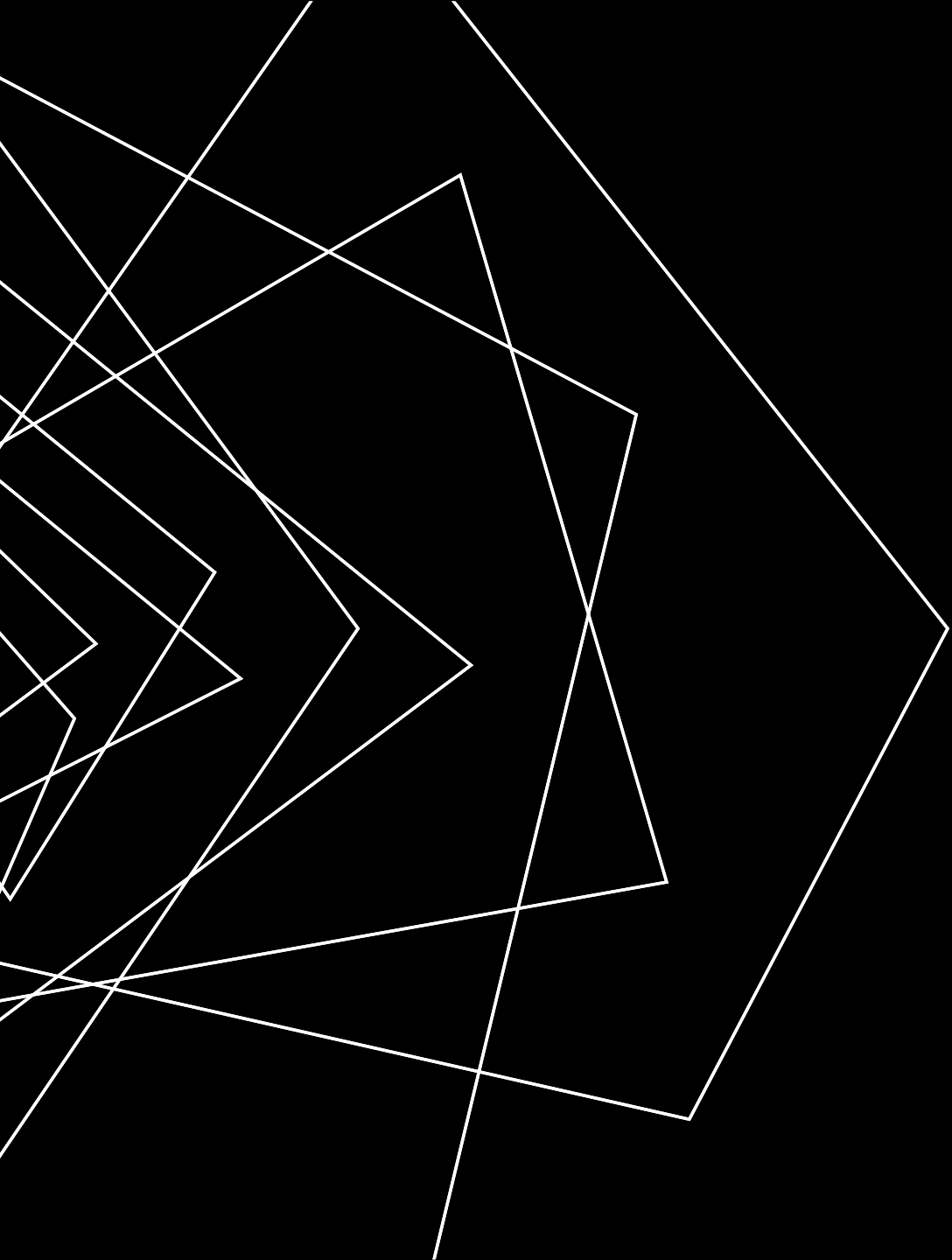
2.) How do you think the SecOps would look like in 5 years?



# THE FUTURE

- AI for Security and Security for AI
- Platformization & Information Sharing
- New acronyms like
  - CDR – Cloud Detection and Response
  - CIRA – Cloud Incident Response Automation





THANK YOU

QA