ETH zürich

Navigating Autonomy

Unveiling Security Experts' Perspectives on Augmented Intelligence in Cybersecurity

Neele Roch
ETH Zurich

Hannah Sievers
ETH Zurich

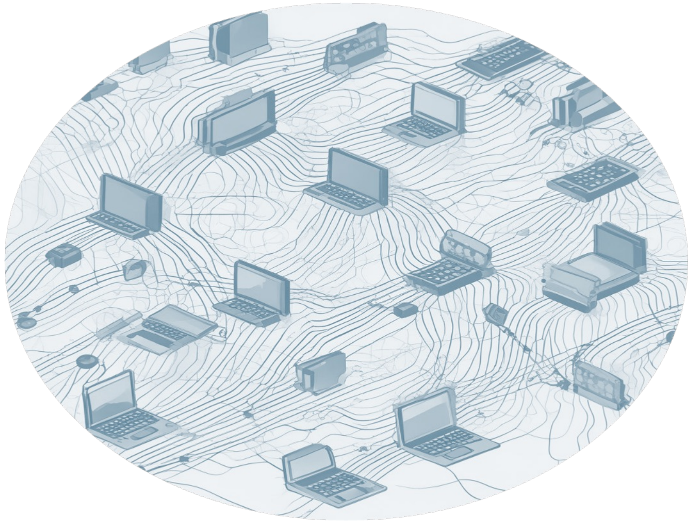
Lorin Schöni
ETH Zurich

Verena Zimmermann
ETH Zurich

August 11–13, 2024
Philadelphia, PA, USA

Motivation

Workforce gap



Data-driven environment

Complementary capabilities

Opportunities?

Research Aims + Objectives

What is the cybersecurity experts' perspective on collaborating with AI tools to complete their tasks?

→ Competencies of both actors

→ Task sharing mode (Autonomy level)

What are the cybersecurity experts' perceptions on

→ automation,

→ autonomy, and

→ trust

in expert-AI collaboration?

Method + Demographics

Expert Interviews with 27 Cybersecurity Experts

- **Recruitment:**
  Purposive and snowball sampling
- **Data generation + analysis:**
  Grounded Theory

Men	25
Women	2

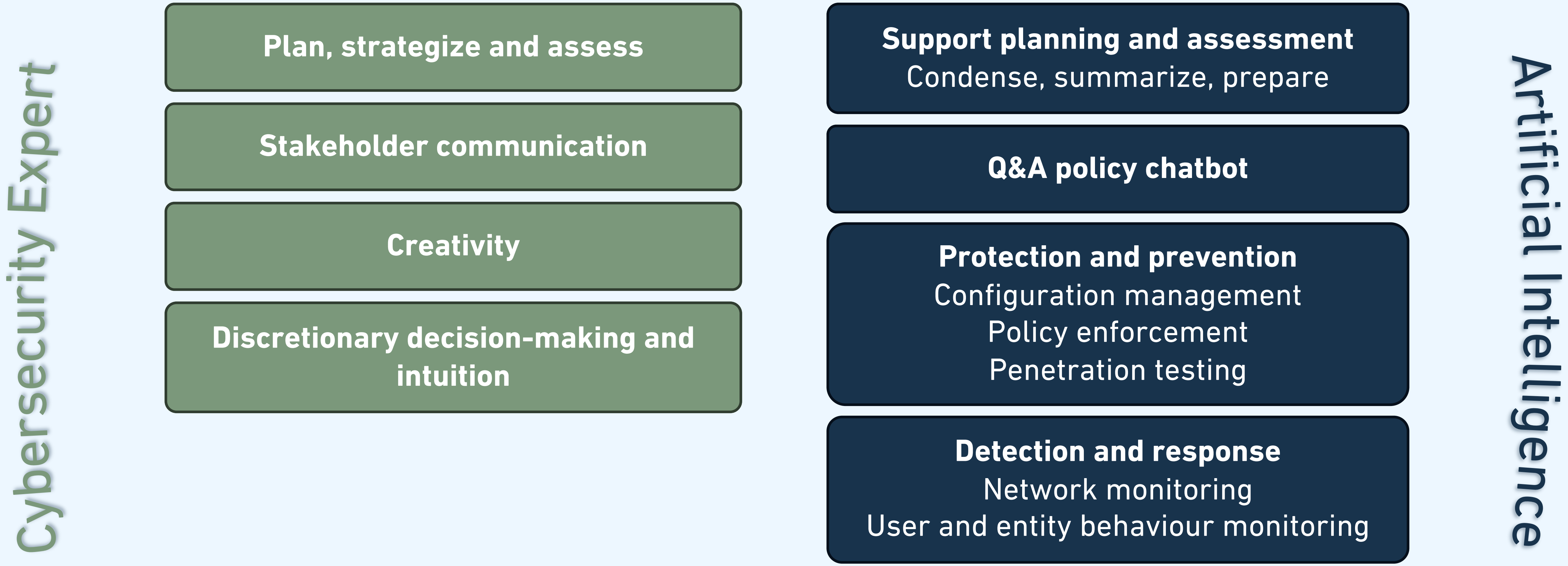
Chief Information Security Officer	16
Information Security Officer	2
Chief Security Officer	2
Head of Security	2
Other	5

Personal Experience with AI	
M=5.50 (SD=1.10)	7-point Likert

Familiarity with AI	
M=5.54 (SD=0.65)	7-point Likert

Results

Perceived Capabilities and Task Sharing



Cybersecurity Expert

Plan, strategize and assess

Stakeholder communication

Creativity

Discretionary decision-making and intuition

Artificial Intelligence

Support planning and assessment
Condense, summarize, prepare

Q&A policy chatbot

Protection and prevention
Configuration management
Policy enforcement
Penetration testing

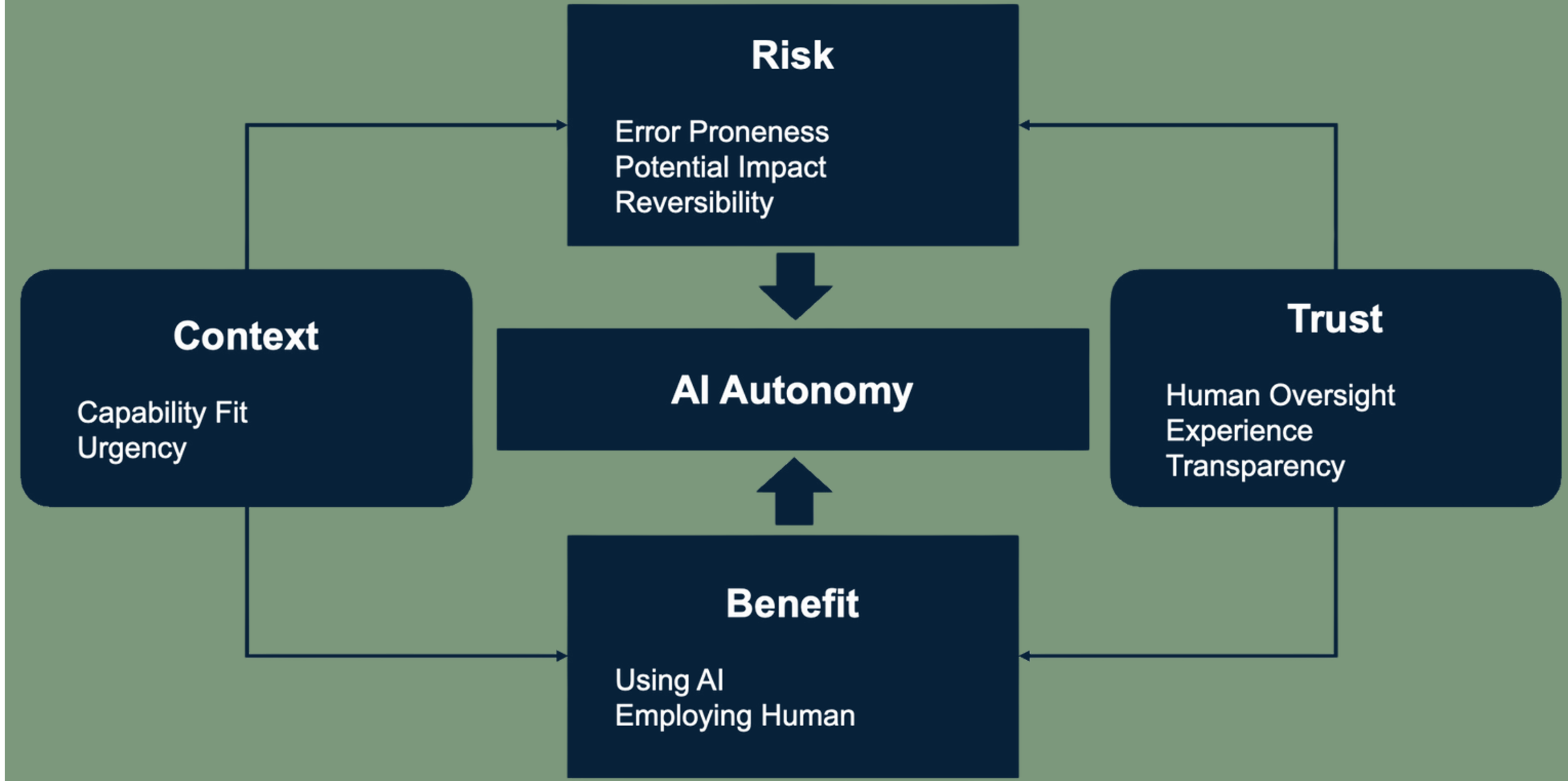
Detection and response
Network monitoring
User and entity behaviour monitoring

Autonomy Levels

- Decision Support
- Human Approval
- Human Veto
- Automated with Information Provision
- Fully Automated

Autonomy Decision Framework

What are the cybersecurity experts' perceptions on
→ automation,
→ autonomy, and
→ trust
in expert-AI collaboration?



Risk

Error Proneness
Potential Impact
Reversibility

Context

Capability Fit
Urgency

AI Autonomy

Trust

Human Oversight
Experience
Transparency

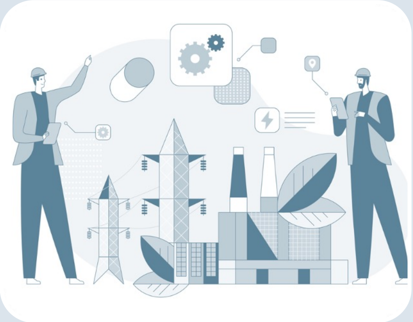
Benefit

Using AI
Employing Human

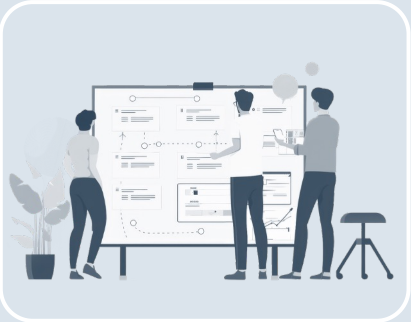
Discussion

Discussion

Building trust with the AI "employee"



"Never trust, and verify"



Importance of transparency for cybersecurity

ETH zürich

KEY TAKEAWAYS

- Cybersecurity professionals are open to deploying AI in certain areas of cybersecurity
- AI autonomy level decision framework for cybersecurity includes factors of risk, benefit, context and trust
- AI transparency is important in high-responsibilities and high-risk use cases for cybersecurity

Link to paper

Neele Roch

neele.roch@gess.ethz.ch

Security, Privacy and Society Group

spg.ethz.ch