Blue Team Fundamentals

Roles and Tools in a Security Operations Center

Jenny Hofbauer
(jeh7703@thi.de)

Dr. Kevin Mayer
(kevin.mayer@carissma.eu)

SECURITY IN MOBILITY – THI

JENNY HOFBAUER

SOC Analyst

Vehicle SOC Researcher

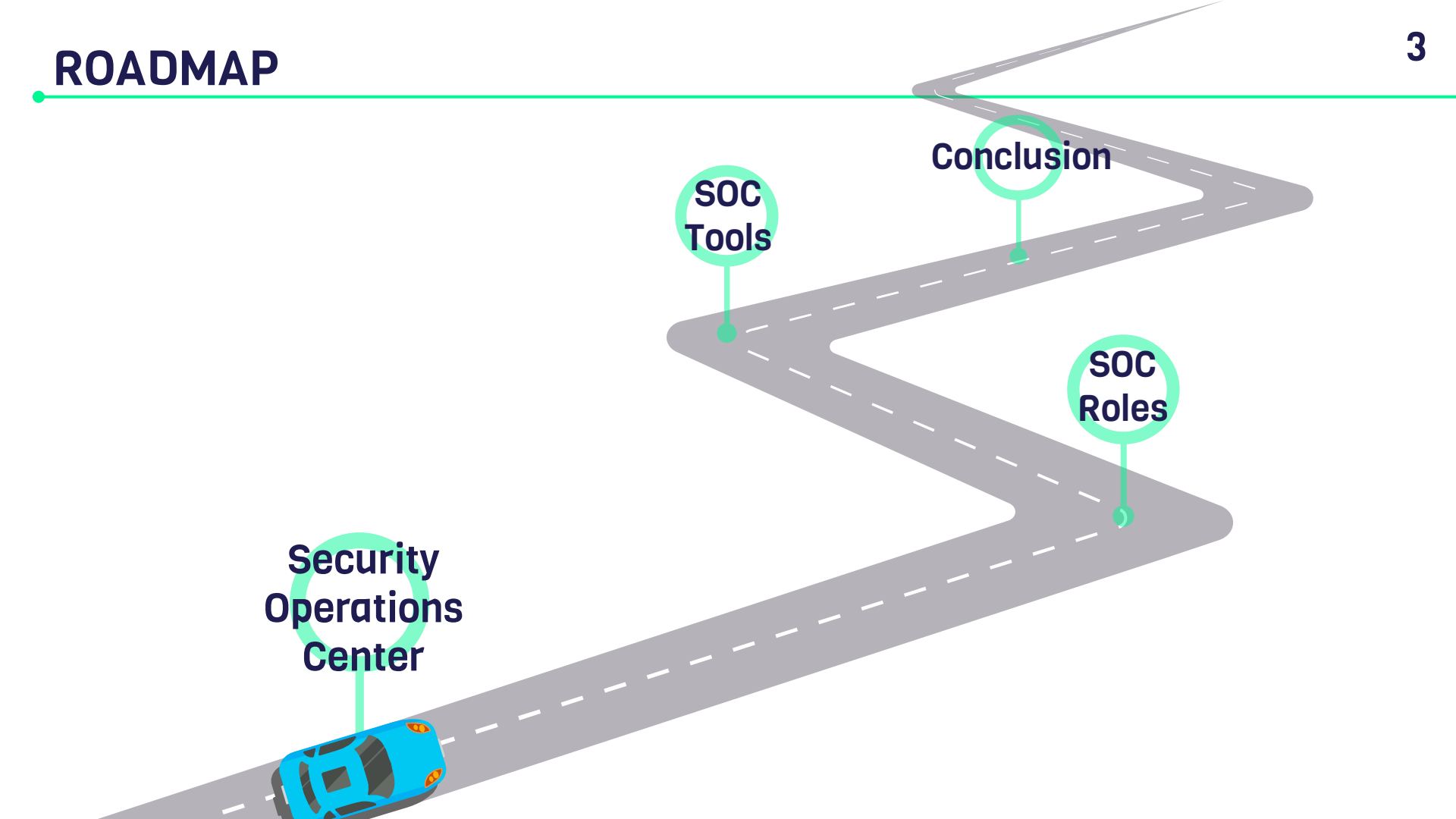
DR. KEVIN MAYER

Automotive Digital Forensics Researcher

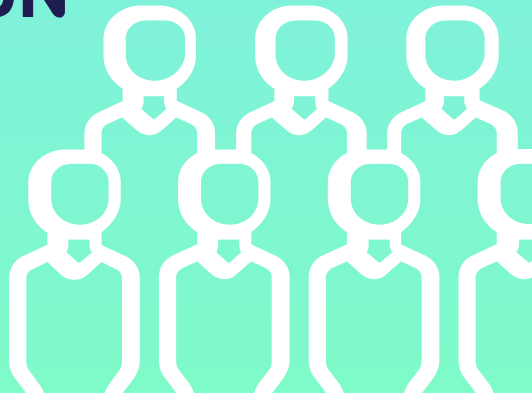
Developing tools for a cyber secure and trustworthy Cooperative Connected Automated Mobility

The SELFY project has received funding from the Horizon Europe programme under grant agreement No. 101069748. This work reflects only the author's view. Neither the European Commission nor the CINEA is responsible for any use that may be made of the information it contains.

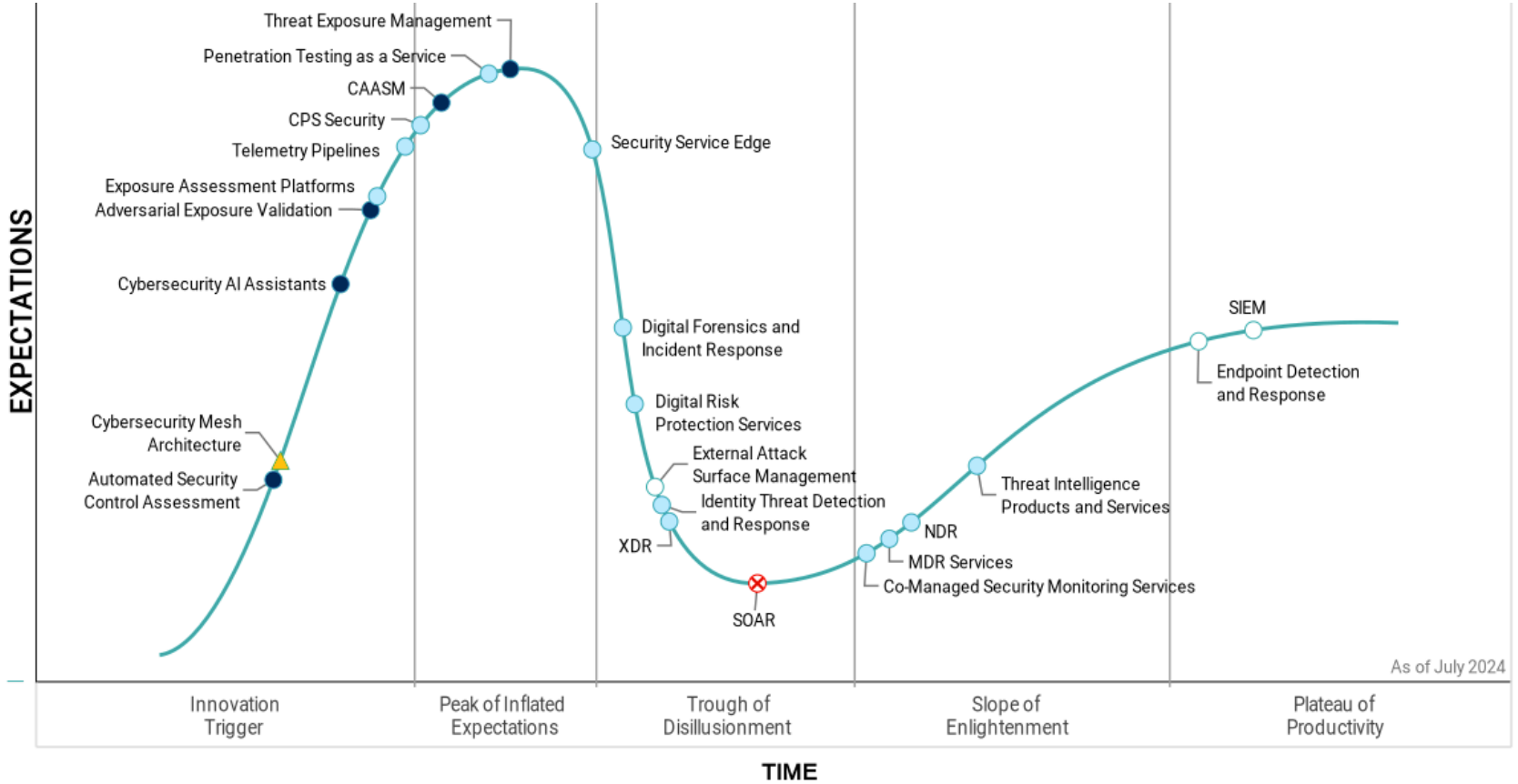
ROADMAP


Conclusion
SOC Tools
SOC Roles
Security Operations Center

“IT SECURITY SERVICES PROVIDER THAT PROTECTS AGAINST CYBERSECURITY THREATS AND INFORMATION LOSS.”

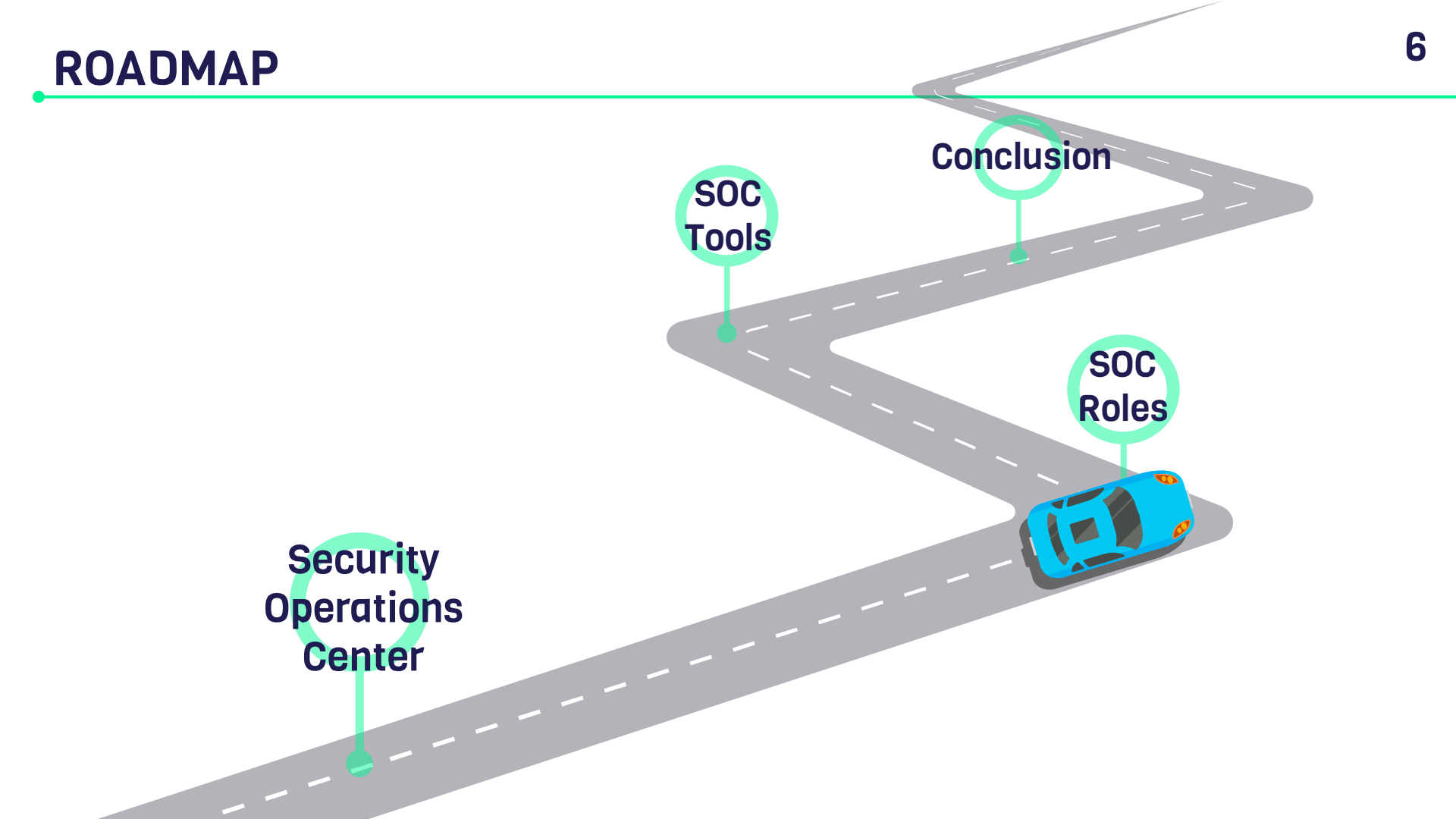


HYPE CYCLE SECURITY OPERATIONS 2024



https://netenrich.com/gartner-hype-cycle-for-security-operations-2024

ROADMAP


Conclusion
SOC Tools
SOC Roles
Security Operations Center

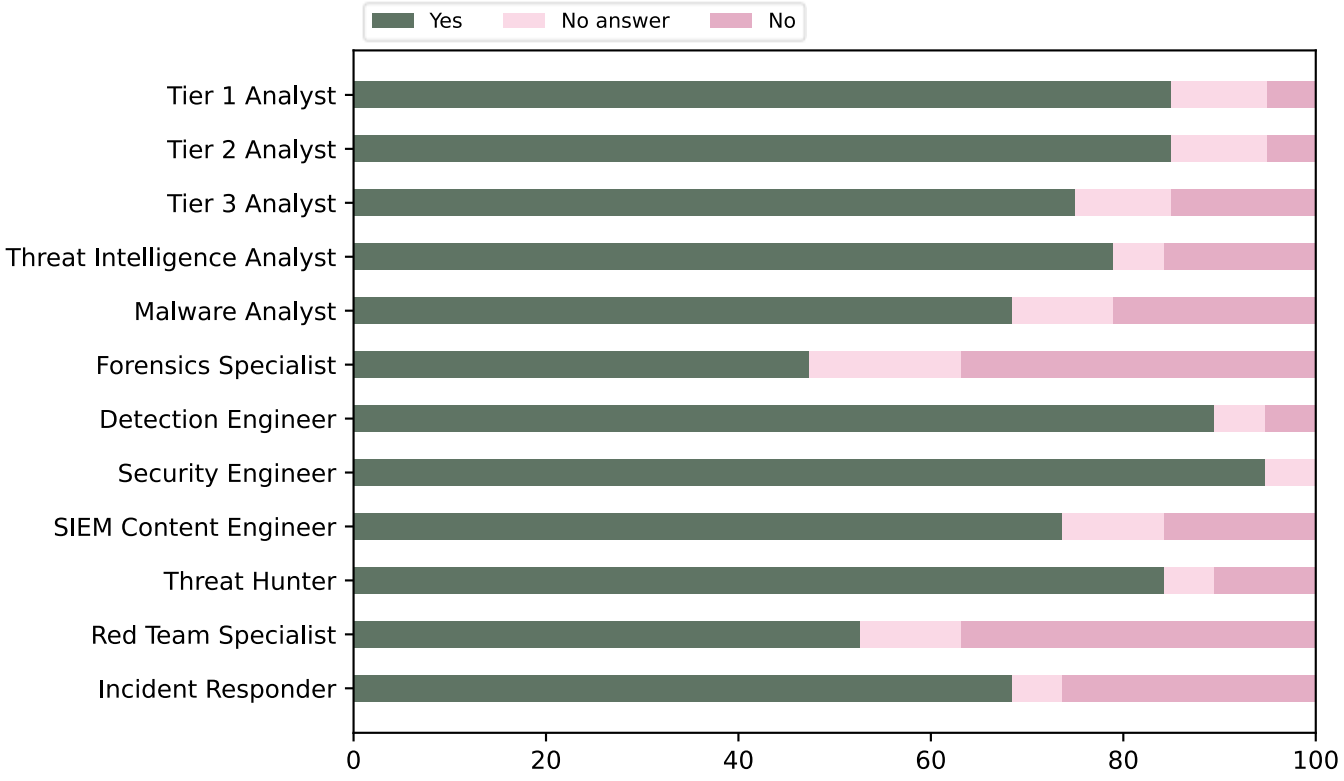
SOC ROLES

TECHNICAL SOC ROLES

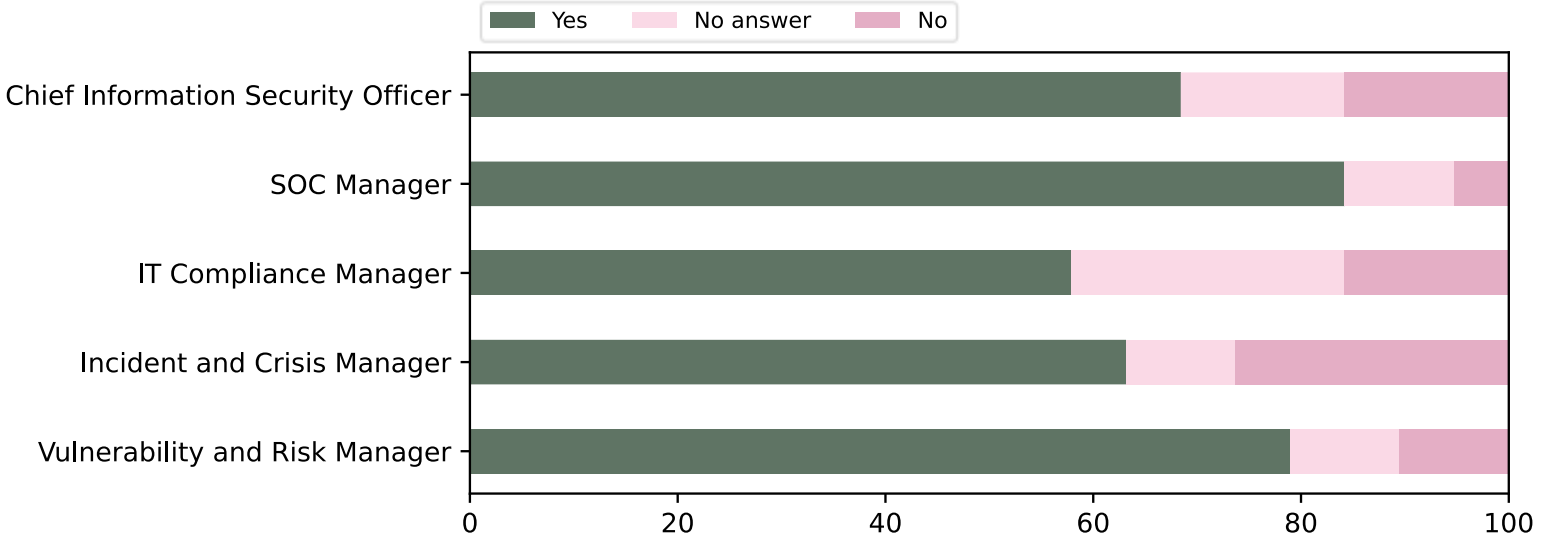
MANAGEMENT SOC ROLE

CONSULTING ROLES

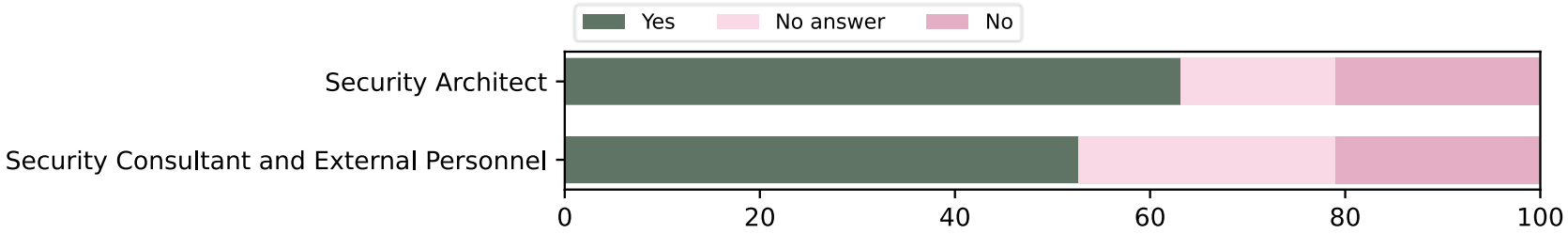
TECHNICAL SOC ROLES



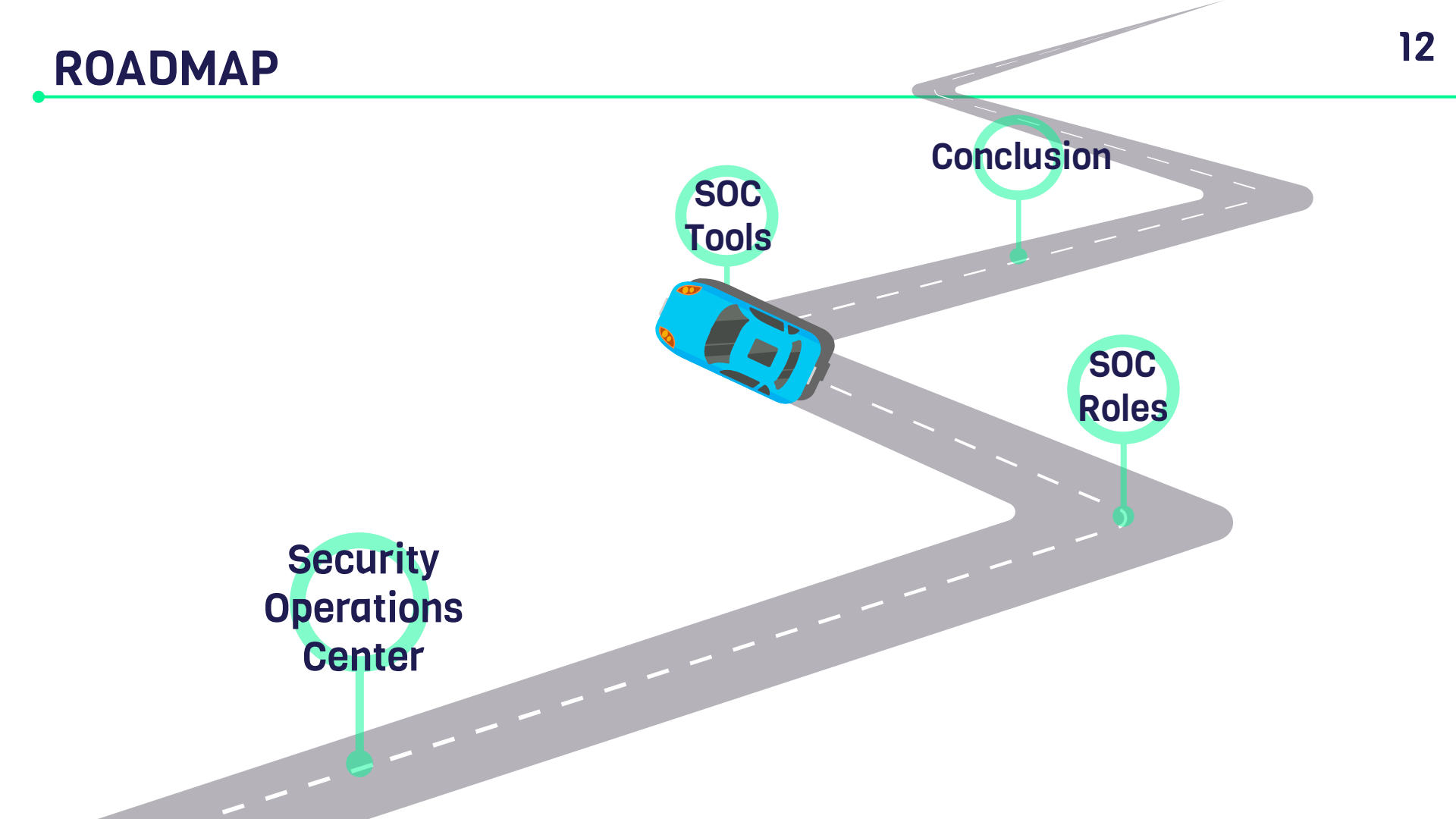
MANAGEMENT SOC ROLES



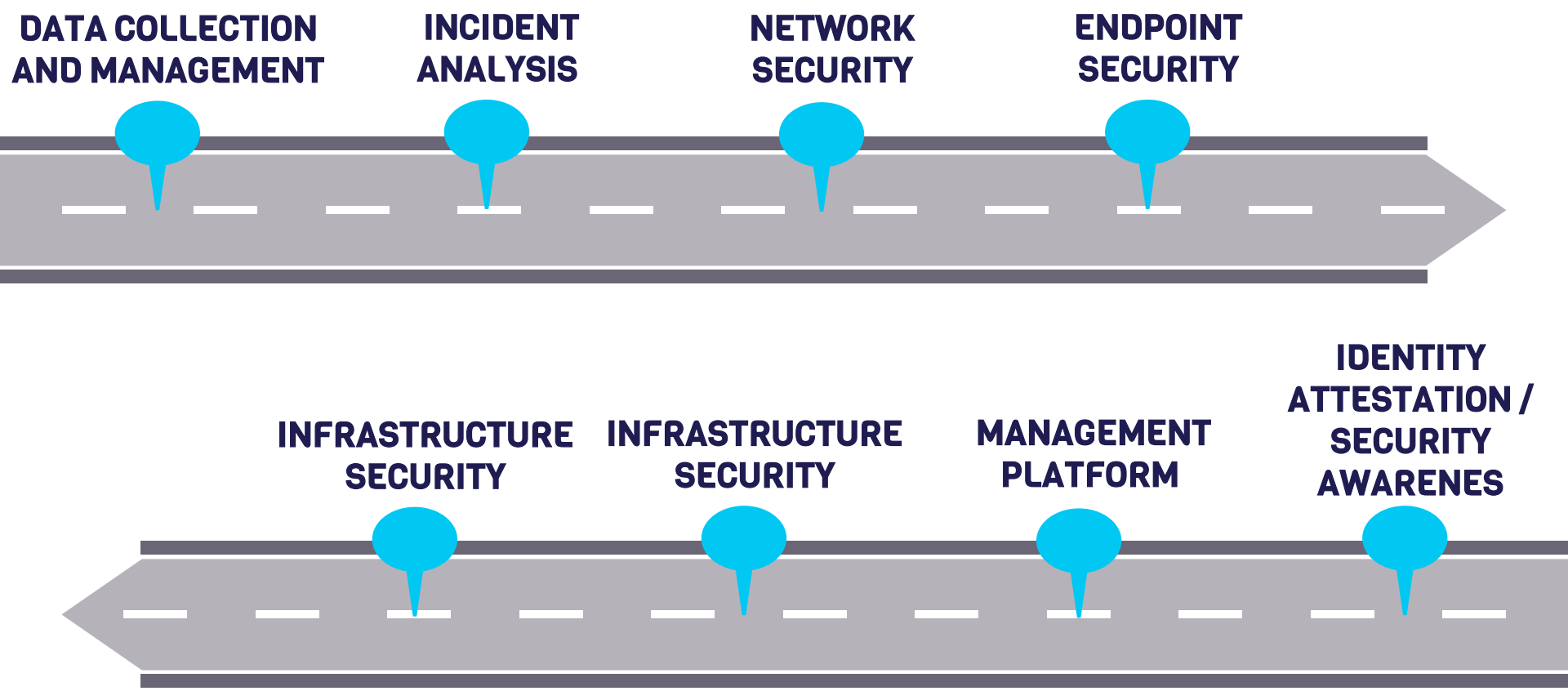
CONSULTING ROLES



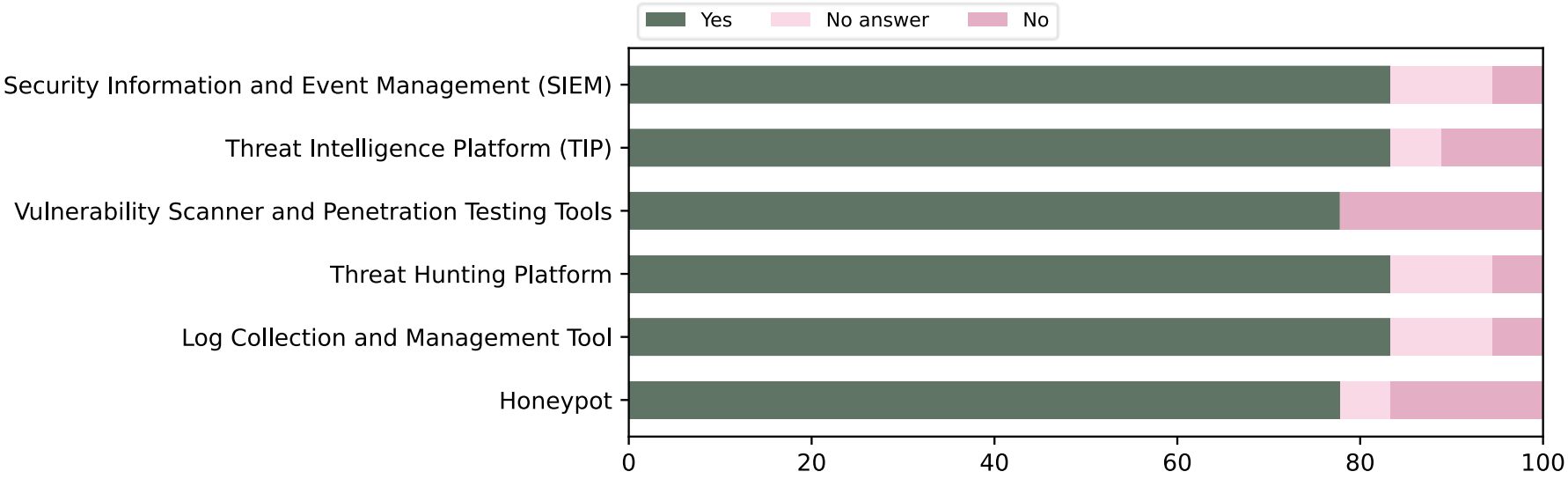
ROADMAP


Conclusion
SOC Tools
SOC Roles
Security Operations Center

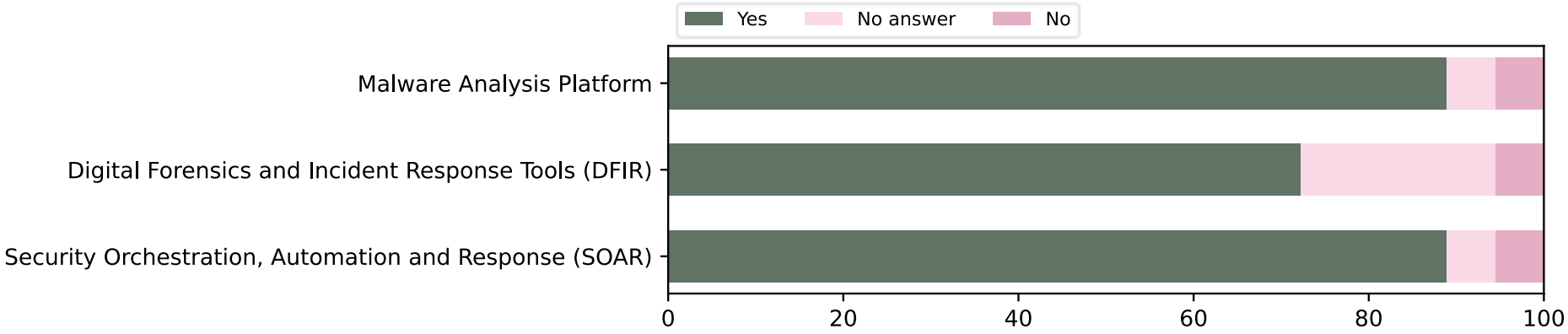
SOC ROLES


DATA COLLECTION AND MANAGEMENT
INCIDENT ANALYSIS
NETWORK SECURITY
ENDPOINT SECURITY
IDENTITY ATTESTATION / SECURITY AWARENES
MANAGEMENT PLATFORM
INFRASTRUCTURE SECURITY
INFRASTRUCTURE SECURITY

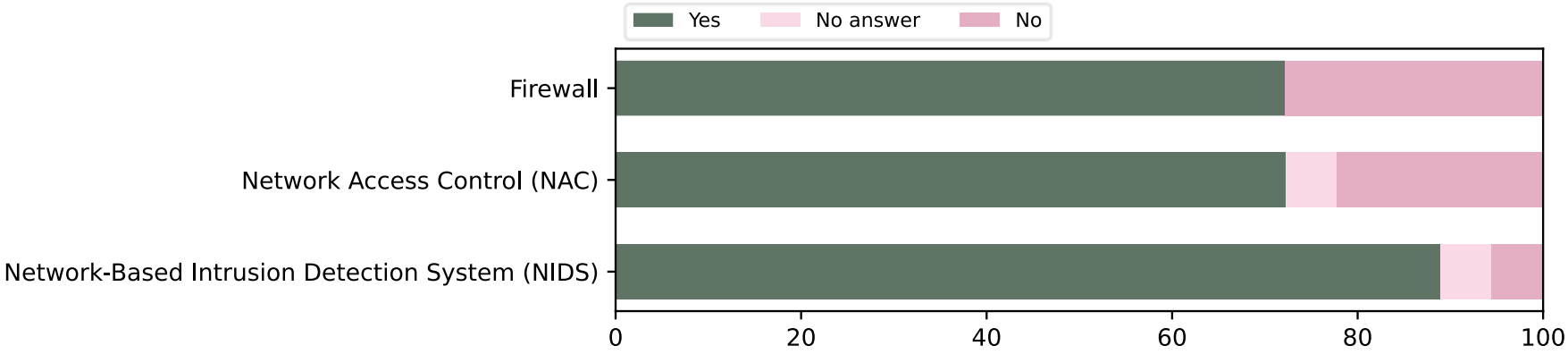
DATA COLLECTION AND MANAGEMENT



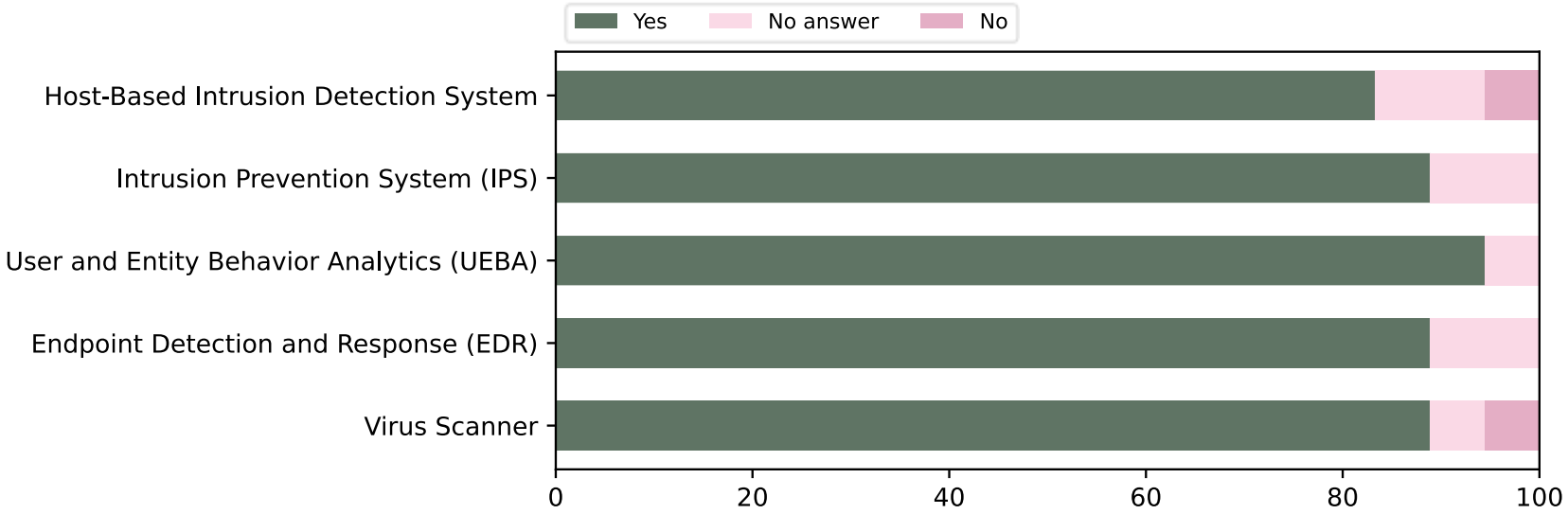
INCIDENT ANALYSIS



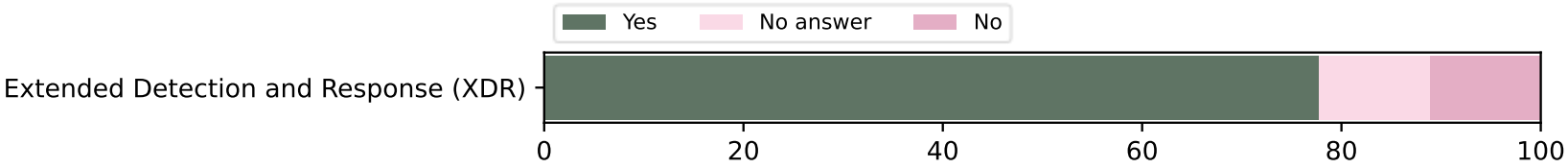
NETWORK SECURITY



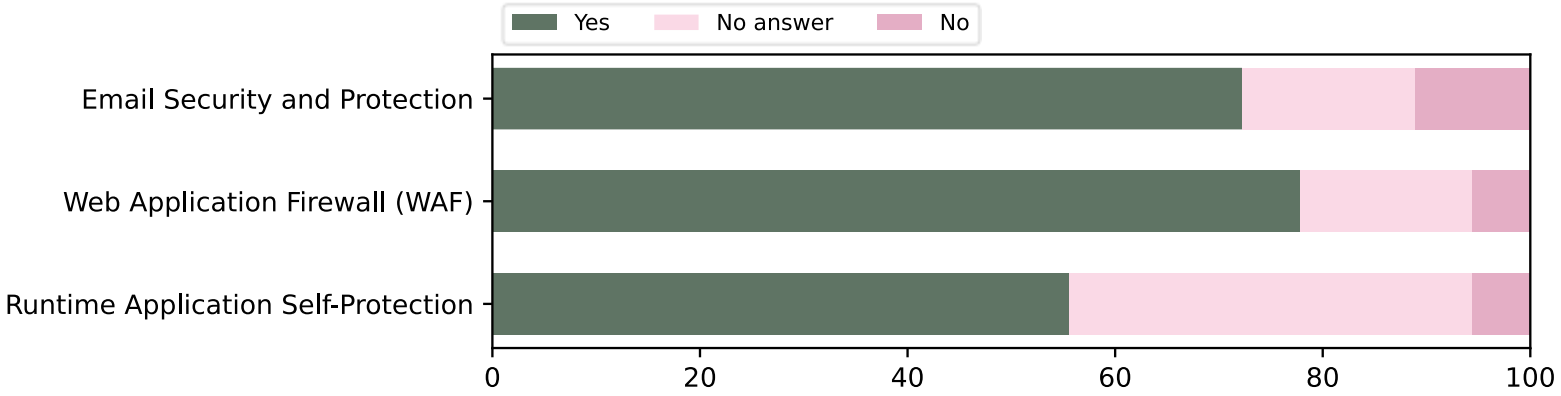
ENDPOINT SECURITY



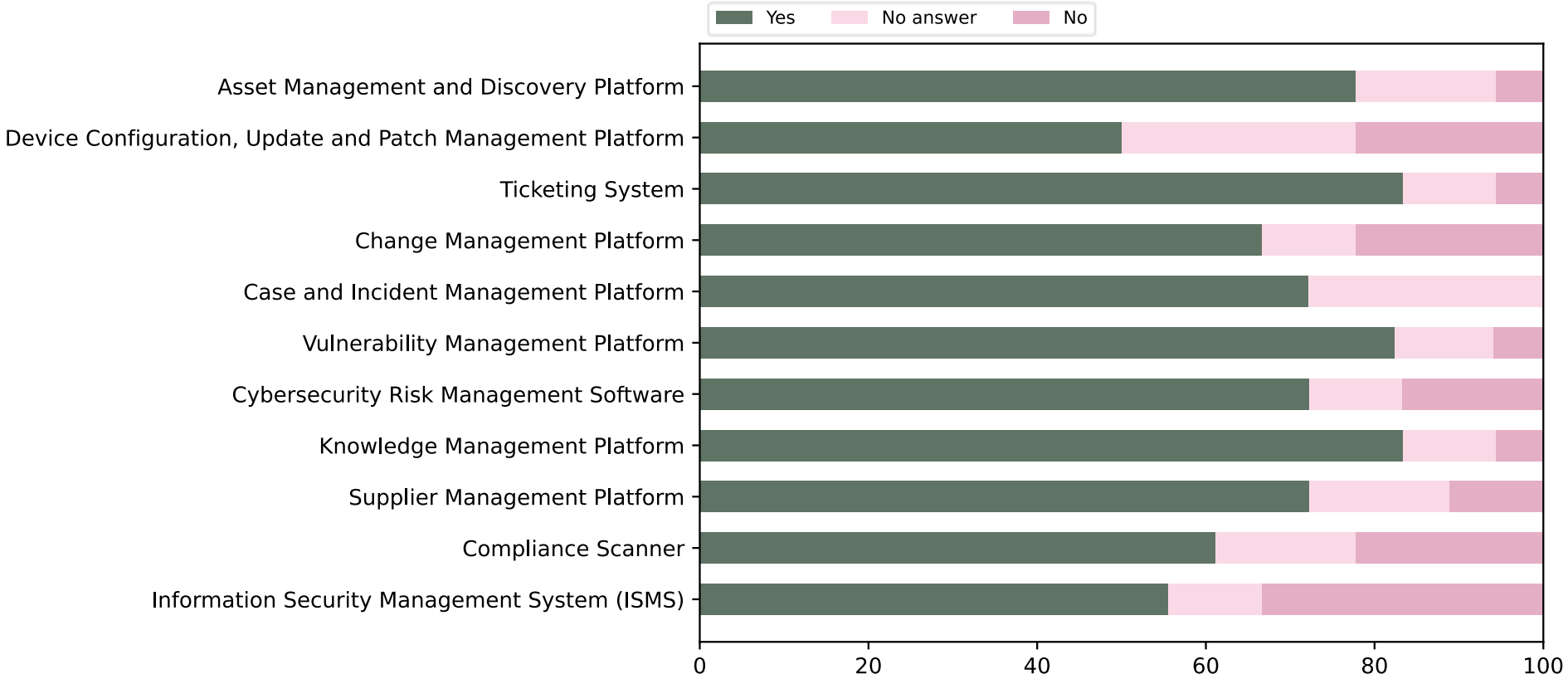
INFRASTRUCTURE SECURITY



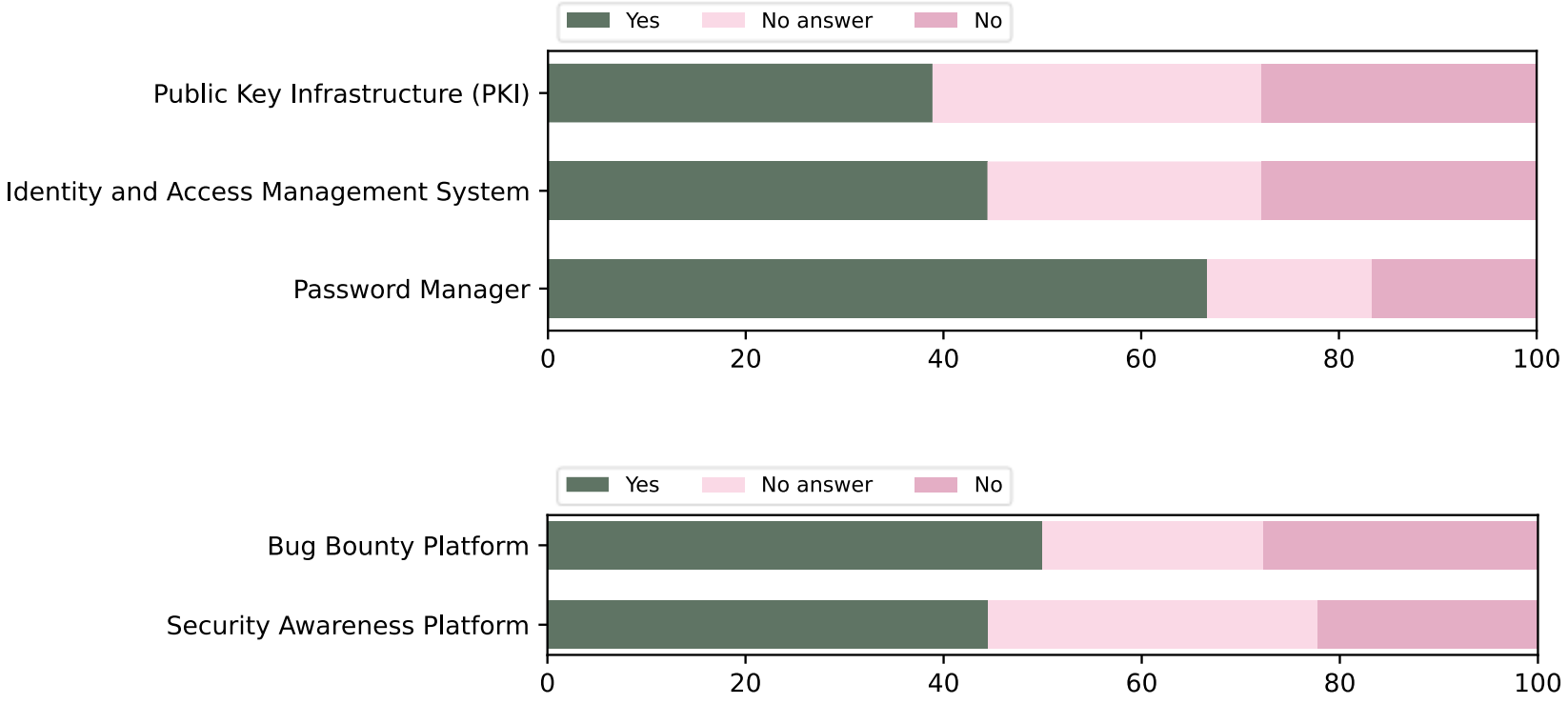
APPLICATION SECURITY



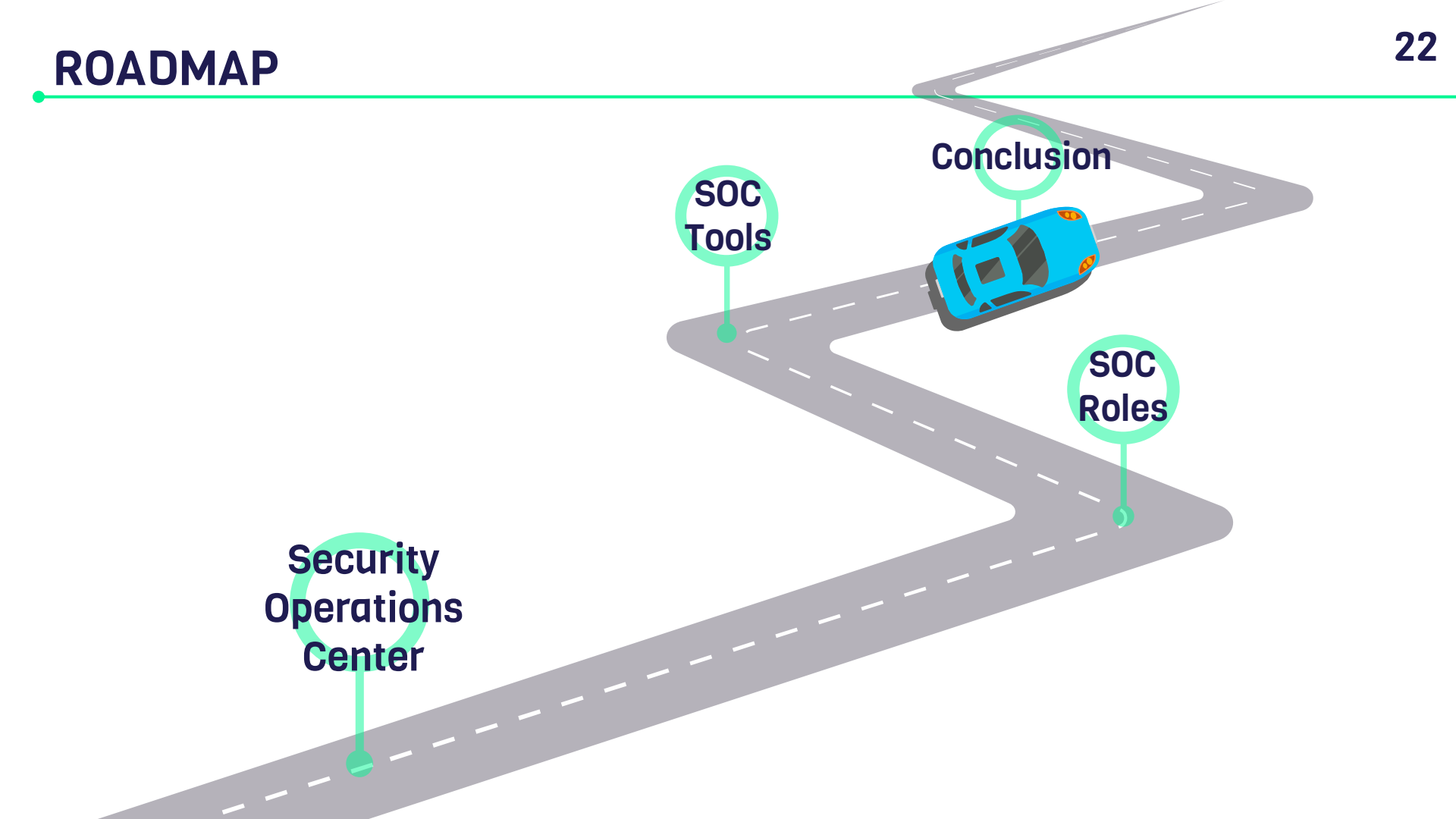
MANAGEMENT PLATFORM



IDENTITY ATTESTATION / SECURITY AWARENESS

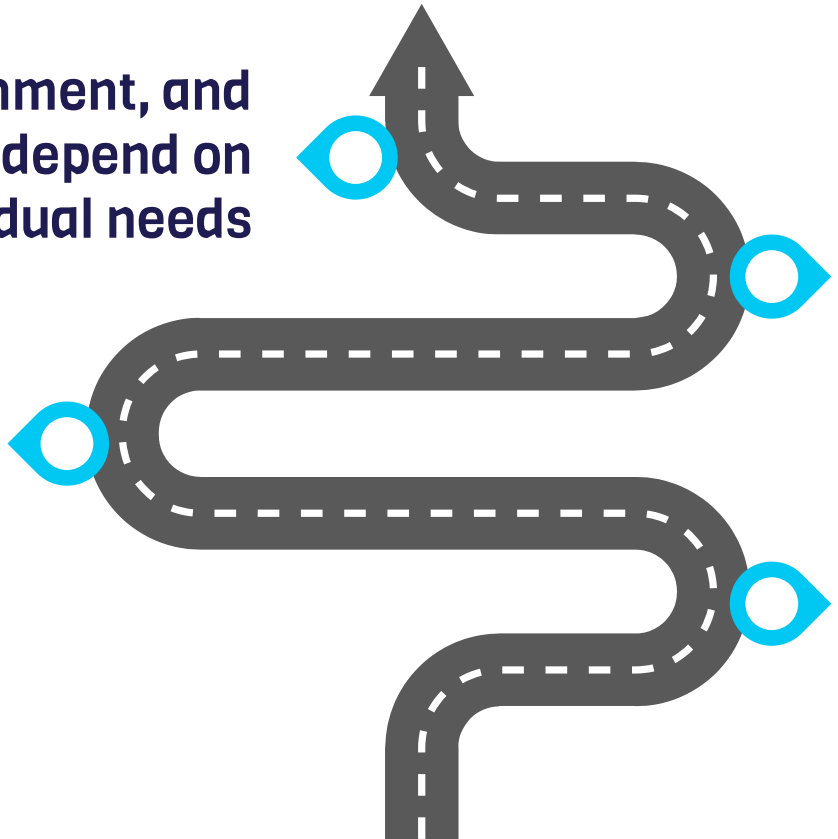


ROADMAP


Conclusion
SOC Tools
SOC Roles
Security Operations Center

CONCLUSION

Presence, assignment, and capabilities depend on individual needs



More specializations

Automation

Single-platform approach

CONTACT US!

jeh7703@thi.de

kevin.mayer@carissma.eu

https://www.thi.de/en/forschung/carissma/c-ecos-navi/security-in-mobility/