malean

malean.org

# Cyber Security Roundtable Liechtenstein

13. Juni 2024

Cyber Security in der Praxis:
Unterstützung bei der Wahl des richtigen Security Operations Centers (SOC) Partners

## Fabian Gentinetta

Gründer und Security Experte

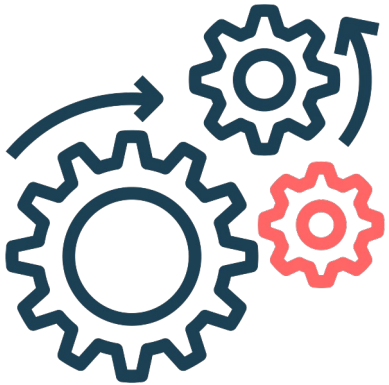
## Sandra Thurnheer

Gründerin und Geschäftsführerin
malean

# Kern-Technologien des modernen SOCs

## Hosts | **NDR + EDR**

Clients
Server
IOT
OT
On-premise
Cloud IaaS
Remote Users

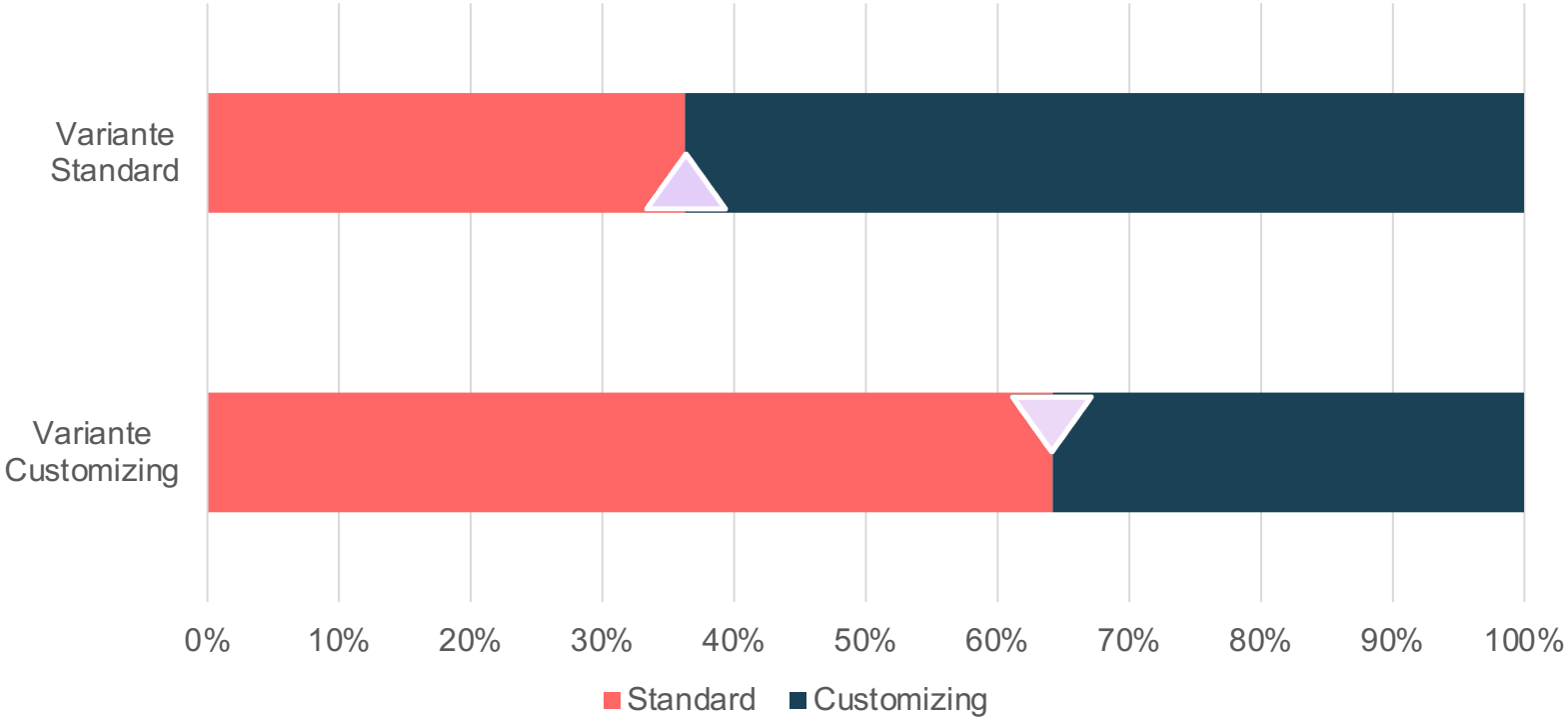


Alerts
Investigations
Workflow Automation
Search / Hunting (GenAI)
Incident Response
Forensic

## Identities | **I(T)DR**

Active Directory
Microsoft EntraID
Okta, Ping
Cloud Control Plane (PaaS)
M365
Salesforce
ServiceNow

# Gibt es DEN richtien SOC Partner?



# Merkmale eines effektiven SOCs

Ein effektives Security Operations Center (SOC) zeichnet sich durch mehrere wesentlichen Merkmale aus.

Klare Ziele und Strategie

Positive Unternehmenskultur

Moderne Technologie

ermöglichen Proaktive Bedrohungserkennung

Kontinuierliche Überwachung und Incident Response

# Prävention – nicht nur am Reisbrett

Regelmässige Tests und Bewertungen auch von Wiederherstellungsplänen

Resilienz und Wiederherstellungspläne

# Cultural impact on SOC

Die Kultur in einem SOC ist entscheidend für den Erfolg im Ernstfall aber auch im Alltag

- Fehlerkultur
- Kommunikationskultur
- Wissenstransfer
- Faktor Mensch

malean

# FRAGEN?

Vielen Dank!

www.malean.org