



# **SURVIVING IN THE CYBER-WILD: HOW TO GET THE MOST OUT OF YOUR SOC SERVICE**

---

Marios Theodoros Kampolis  
TMS Group

***"CYBERSECURITY IS A JOURNEY NOT  
AN ENDGOAL"***





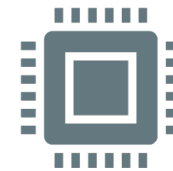
# ***SOC SERVICE***

- » The nerve center of an organization's cybersecurity posture
  - o Monitoring of the digital infrastructure and incident response process consolidation
- » Should not be considered as another outsourced service
  - o Joint effort of both MSSP and organization for an efficient service
- » SOC operations can set the basis of your cybersecurity strategy

# APPROACH



Ask the right question



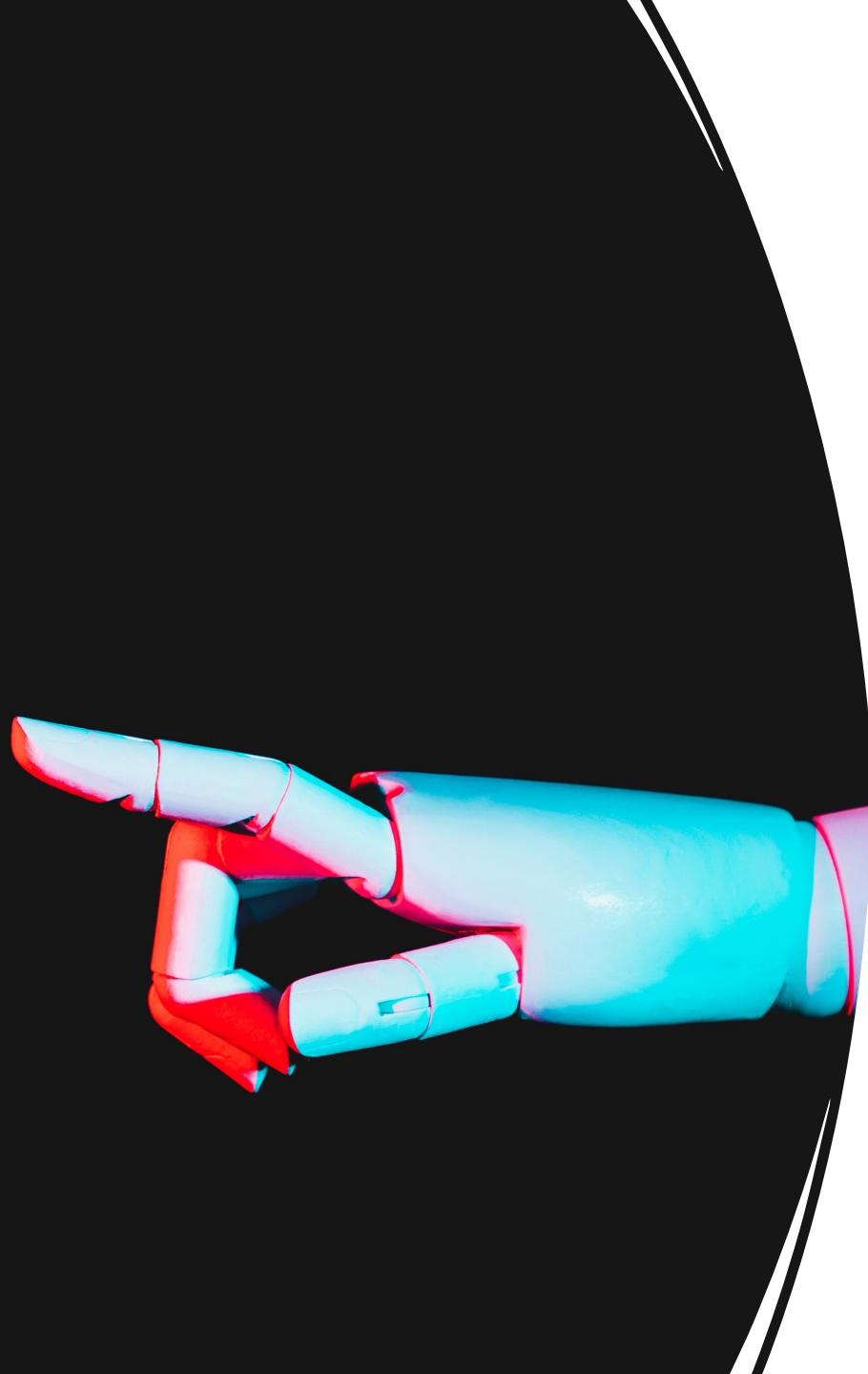
Modern cybersecurity operations  
require early detection  
mechanisms



Information Security Analyst in IT  
Security/ Cybersecurity team

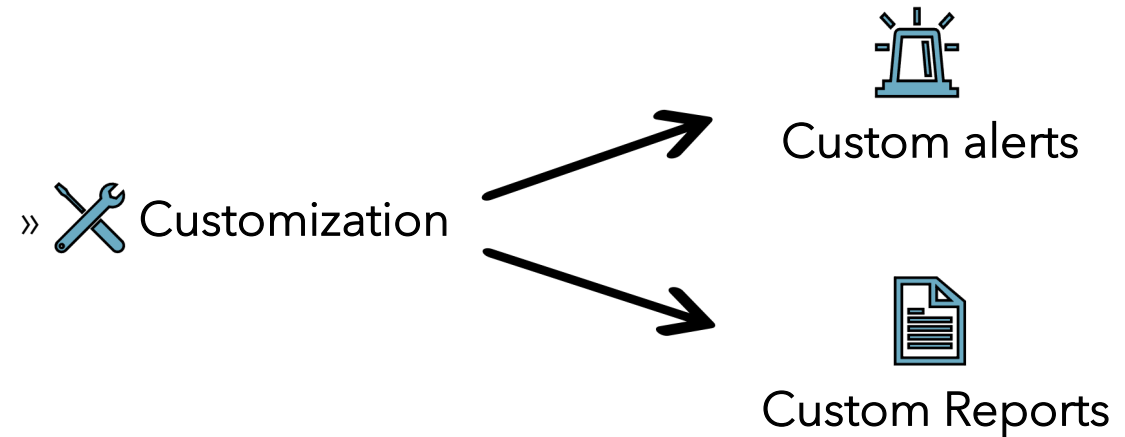


Essential pillar of cybersecurity is  
Communication



# ***SOC SERVICE ADMINISTRATION***

# ADMINISTRATION



## »SOC team profiles your daily incidents/cases

- Engage in this process: Define how specific incidents/cases should be reported/handled

## »Decisions on cybersecurity solutions based on the integration with your SIEM tool

- Default alerts
- Time saving for the configuration as logsources



# ***SOC SERVICE EVALUATION***

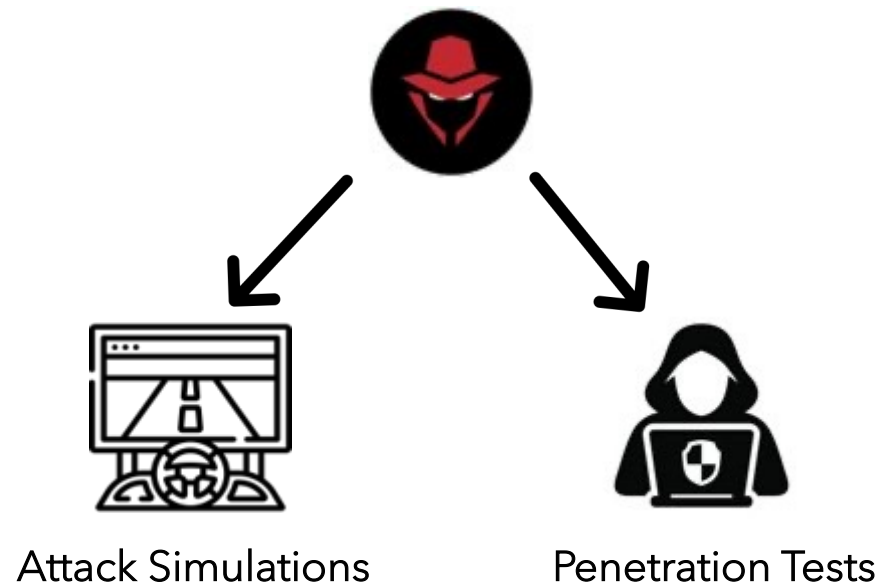
## ***INCIDENT HANDLING LIFECYCLE***





# EVALUATION

## Red Team Operations



*You don't have to wait for an actual attack*

# ***WHAT ABOUT THE VESSELS?***





## **VESSELS**


- » Impact of the upcoming digital transformation and connectivity enhancements
  - More immediate services and support
  - Vessels will become attractive targets
- » Vessels should be considered as remote sites
- » Cybersecurity solutions dedicated for vessels
- » Prior experience with the SOC service in the corporate offices
  - Smoother service integration in the vessels
- » Biggest challenge ahead: The OT realm



# ***AFTERWORD***

# Takeaways

- » **Core elements for efficient SOC service**
  - Communication
  - Planning
- » **Attack surface**
  - Servers facing the internet
  - Clients/Workstations
  - Inside threat
  - Through a Third Party Partner
- » **SOC service is one of the most dynamic services**
  - Different needs
  - Highly dependent on ever-changing trends



**Thank you for your attention**