



# Ten Strategies to implement a Security Operations Center for SMBs

Thomas Kastner, Security Consultant



Digitalisierung mit der nötigen Compliance  
im Vordergrund.

**DATEN**



40 Mitarbeiter/innen

Human Resources, wann und wie Sie diese  
benötigen.

**MENSCHEN**



900 Mitarbeiter/innen - intern und  
extern

130 Mitarbeiter/innen

**TECHNIK**



Ingenieurdienstleistungen auf höchstem  
Niveau.

10 Mitarbeiter/innen

**INTERNATIONAL**

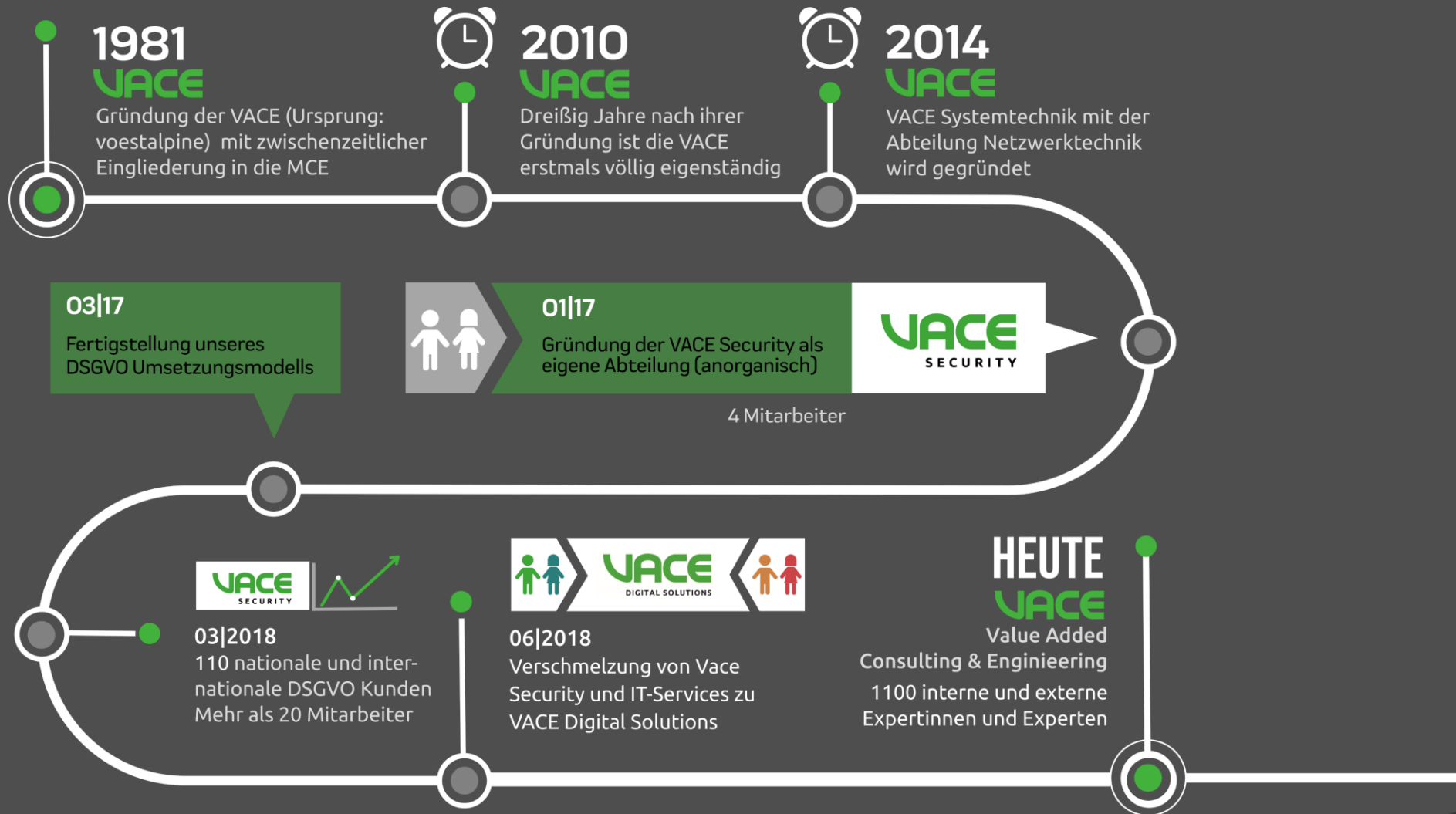
Industrial education for underprivileged  
people around the world.

**VACE**  
GROUP

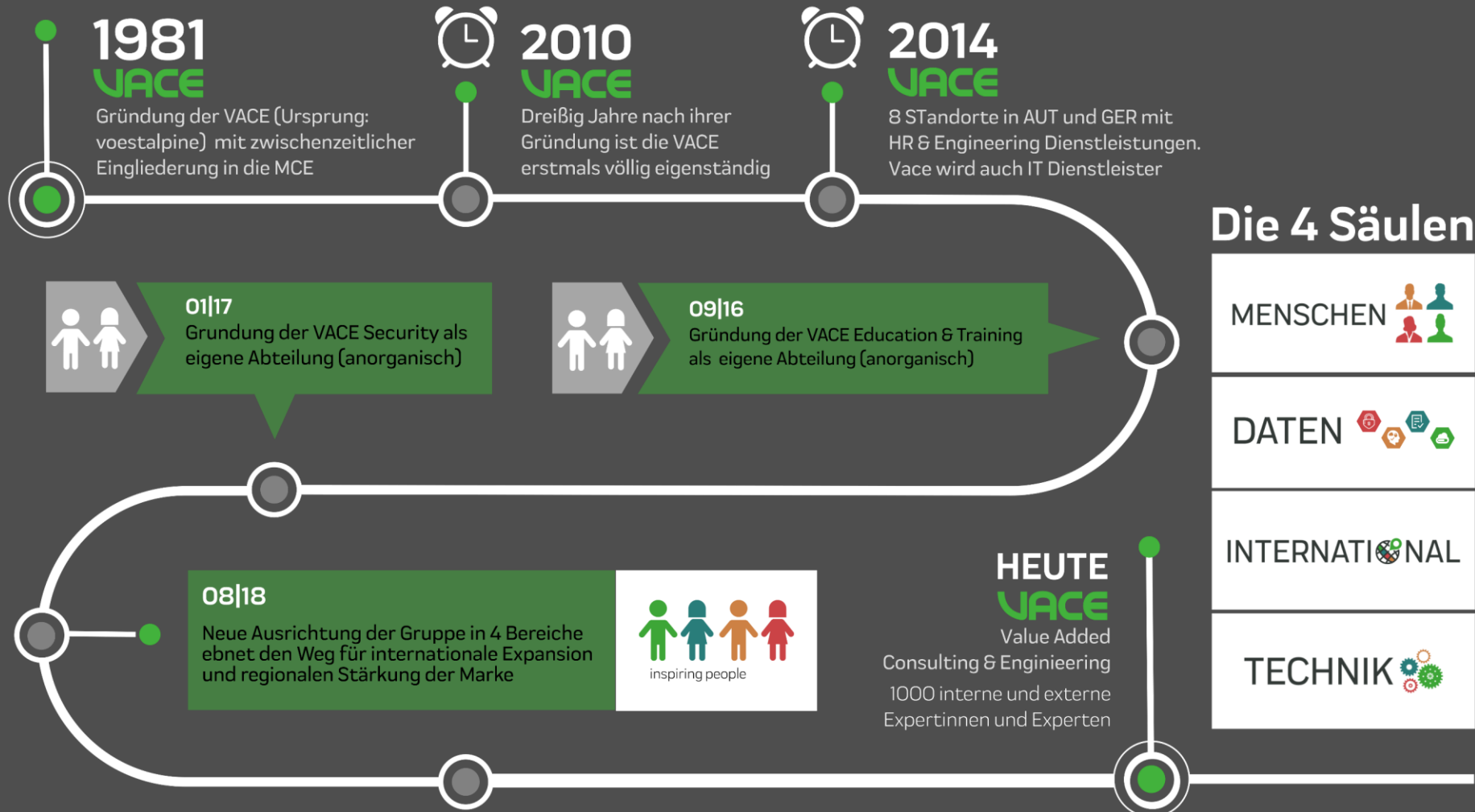
ca. 1.100 MA



# Entwicklungsprozess



# Die Entwicklung - Gruppe



# Portfolio - Digital Solutions

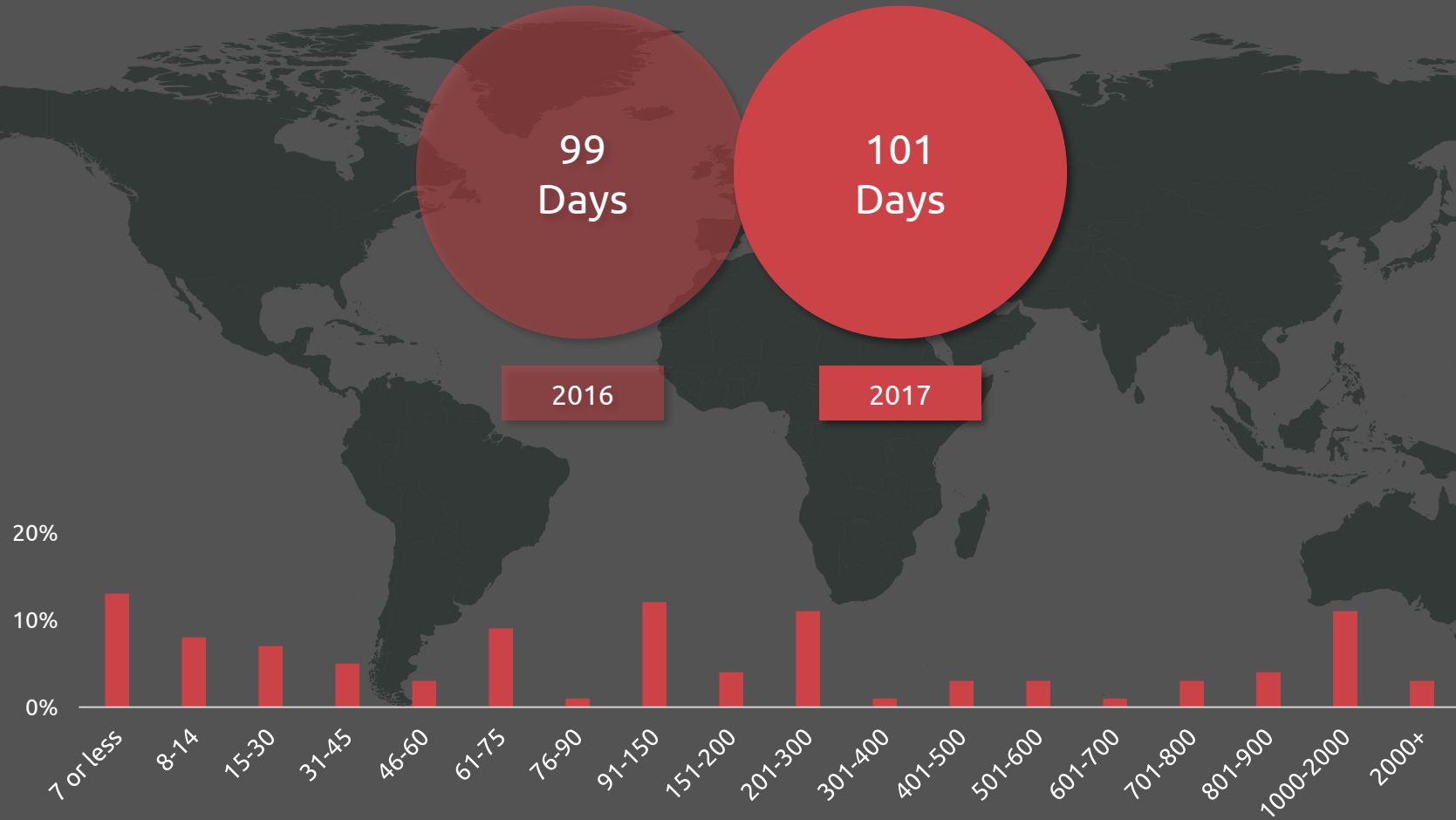


# The Five Functions | NIST



SAC CTAC IPC  
CSC CERT ISOC  
SNOC CCDC CIRC CSA  
CSOC CSIRC SDC  
SIOC CSIRT CIRT SOC  
CDOC CDC  
NSOC

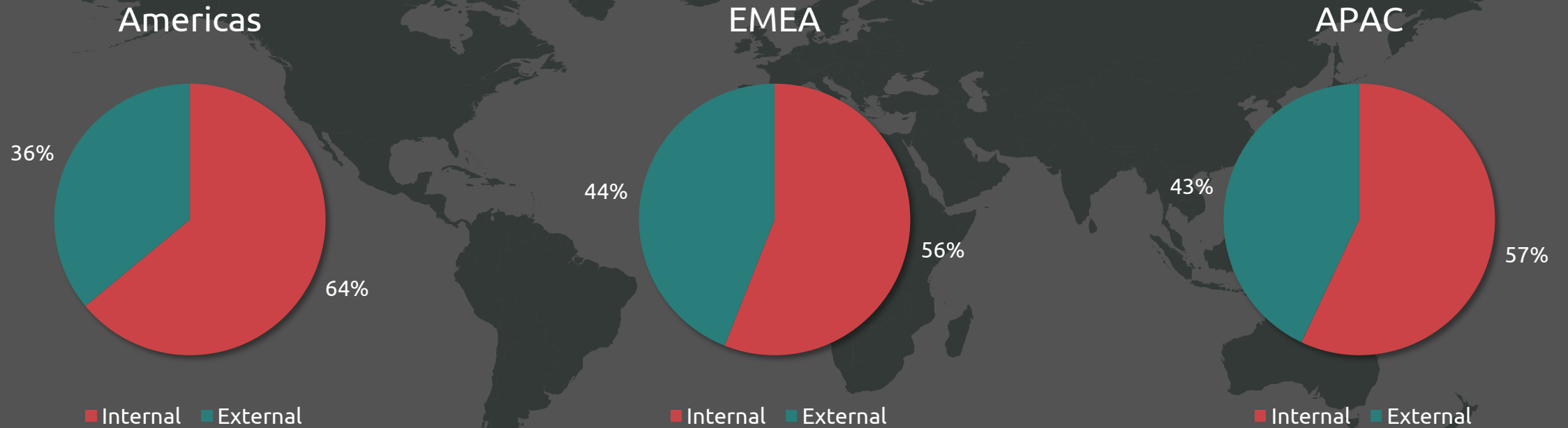
# Median Dwell Time



Source: M-Trends Report 2018



# Notification Sources



# How to implement a SOC in an SMB?

**MITRE**

Ten Strategies of a World-Class  
Cybersecurity Operations Center



Carson Zimmerman



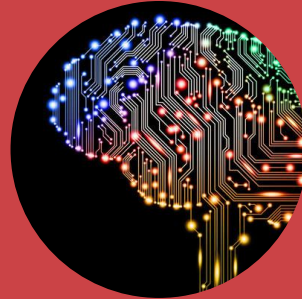
# Consolidate CND Under One Organization



Monitoring  
and Triage



Incident  
Analysis and  
Response



Threat  
Intelligence  
Collection



SOC System  
Administration



SOC Tool  
Engineering



# Achieve Balance Between Size and Agility



## **In-sourcing**

Perform all the activities within the SOC from within customer environment

## **Co-sourcing**

Outsource certain activities to a third party whilst retaining critical components within customer

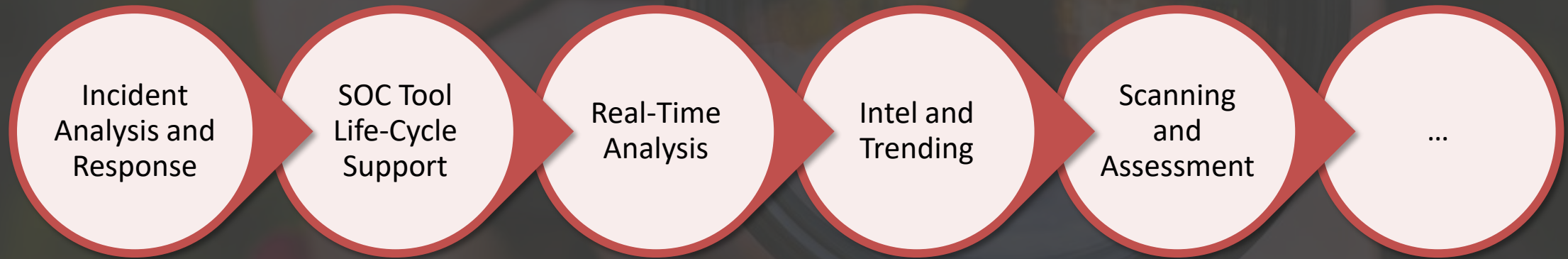
## **Outsourcing**

Engage a third party to perform SOC activities on behalf of customer

# Give the SOC the Authority to Do Its Job



# Do a Few Things Well




















# Favor Staff Quality over Quantity



With the right tools, one good analyst can do the job of 100 mediocre ones.

Analyst quality is vastly more important than analyst quantity.

# Maximize the Value of Technology Purchases

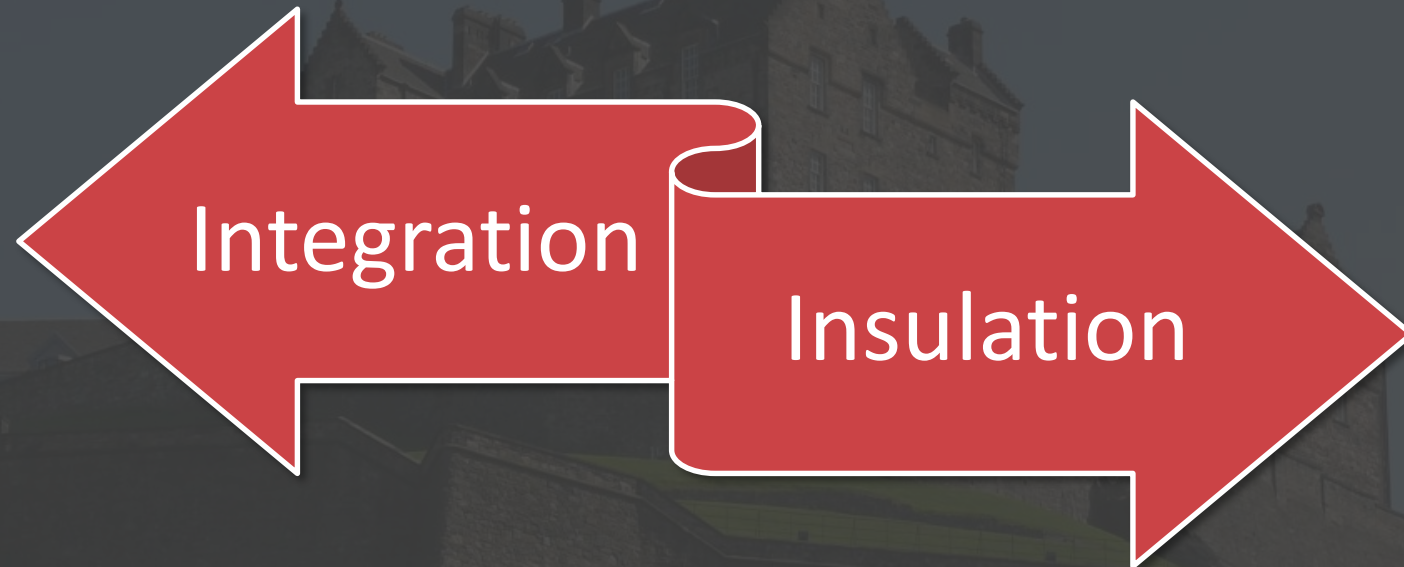
				
				
				

# Exercise Discrimination in the Data you Gather



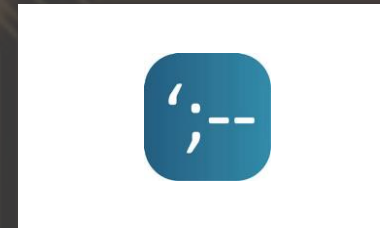
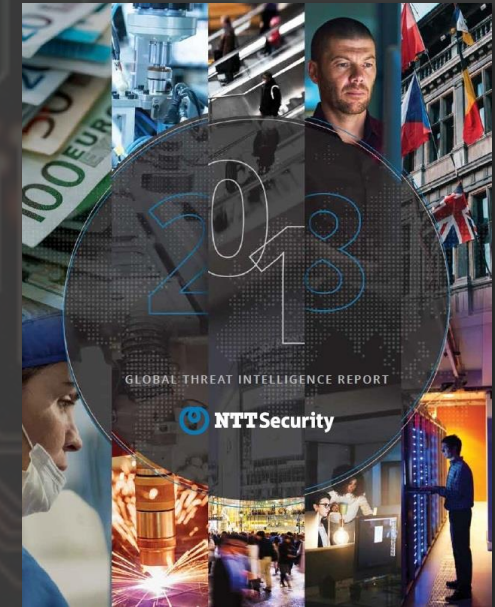
# Protect the SOC Mission

VIII



Never join SOC monitoring infrastructure, sensors, analysis workstations, or any other SOC equipment to the general constituency's Windows domain.

# Consume Available Cyber Threat Intelligence



# Stop. Think. Respond ... Calmly





[www.vace.at](http://www.vace.at)

Thomas Kastner  
SECURITY CONSULTANT

VACE Systemtechnik  
GmbH

Linzer Straße 16e  
A-4221 Steyregg

[t.kastner@vace.at](mailto:t.kastner@vace.at)

T +43 (0) 732 / 272277 62

M +43 (0) 664 / 88288774

F +43 (0) 732 / 272277 99



JUST DO IT.