

Ten Strategies to implement a Security Operations Center for SMBs

Thomas Kastner, Security Consultant





Wir sind VACE

Digitalisierung mit der nötigen Compliance im Vordergrund.



40 Mitarbeiter/innen

VACE GROUP

ca. 1.100 MA

Human Resources, wann und wie Sie diese benötigen.



900 Mitarbeiter/innen - intern und extern

130 Mitarbeiter/innen



Ingenieurdienstleistungen auf höchstem Niveau. 10 Mitarbeiter/innen



Industrial education for underpriviliged people around the world.





Entwicklungsprozess



Gründung der VACE (Ursprung: voestalpine) mit zwischenzeitlicher Eingliederung in die MCE



2010

Dreißig Jahre nach ihrer Gründung ist die VACE erstmals völlig eigenständig



2014 VACE

VACE Systemtechnik mit der Abteilung Netzwerktechnik wird gegründet

03|17

Fertigstellung unseres DSGVO Umsetzungsmodells



01|17

Gründung der VACE Security als eigene Abteilung (anorganisch)



4 Mitarbeiter





06|2018

Verschmelzung von Vace Security und IT-Services zu **VACE Digital Solutions**



Value Added Consulting & Enginieering 1100 interne und externe Expertinnen und Experten





Die Entwicklung - Gruppe



Gründung der VACE (Ursprung: voestalpine) mit zwischenzeitlicher Eingliederung in die MCE



(L) 2010

Dreißig Jahre nach ihrer Gründung ist die VACE erstmals völlig eigenständig



2014

8 STandorte in AUT und GER mit HR & Engineering Dienstleistungen. Vace wird auch IT Dienstleister



01|17

Grundung der VACE Security als eigene Abteilung (anorganisch)



09|16

Gründung der VACE Education & Training als eigene Abteilung (anorganisch)









INTERNATISNAL



08|18

Neue Ausrichtung der Gruppe in 4 Bereiche ebnet den Weg für internationale Expansion und regionalen Stärkung der Marke



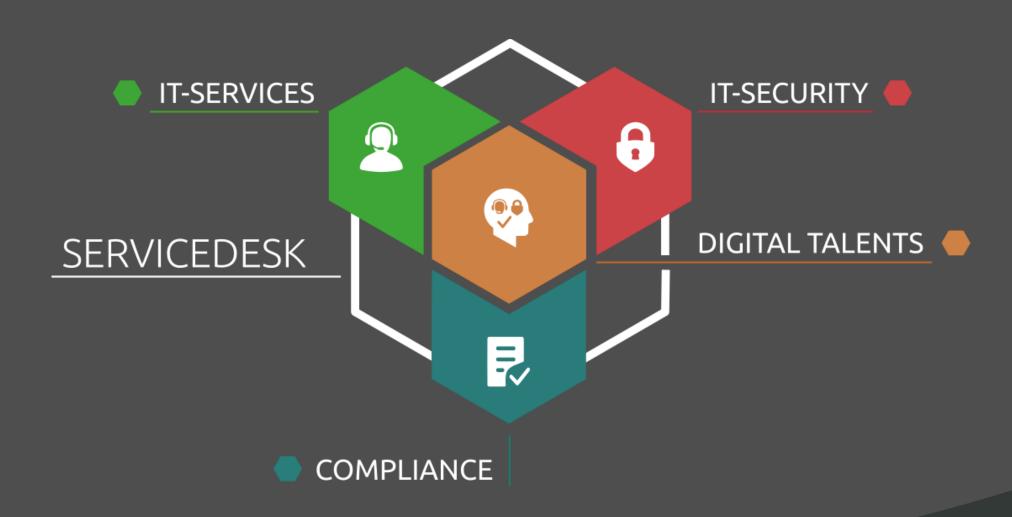
HEUTE

Value Added Consulting & Enginieering 1000 interne und externe Expertinnen und Experten





Portfolio - Digital Solutions





The Five Functions | NIST





SIRTCIRT SOC

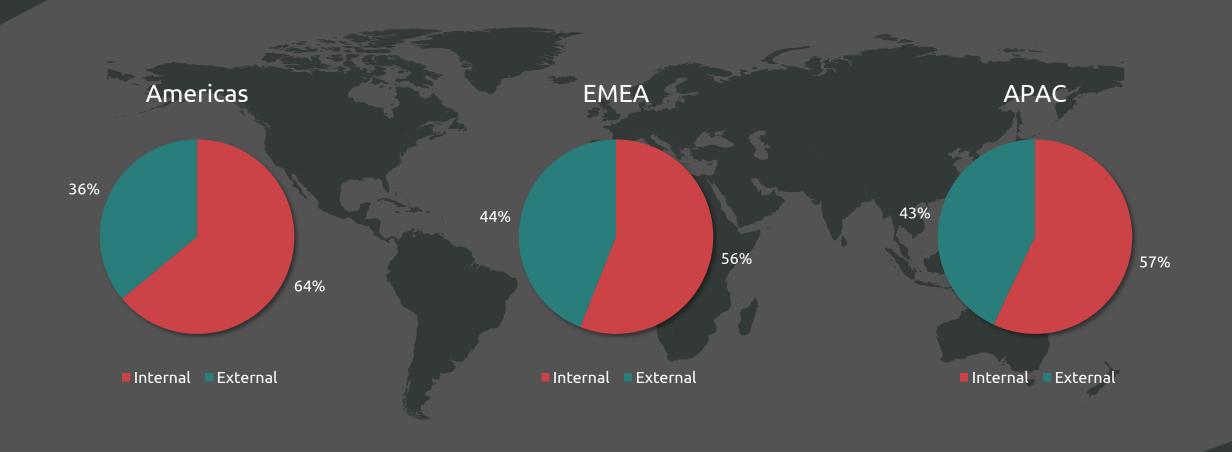


Median Dwell Time

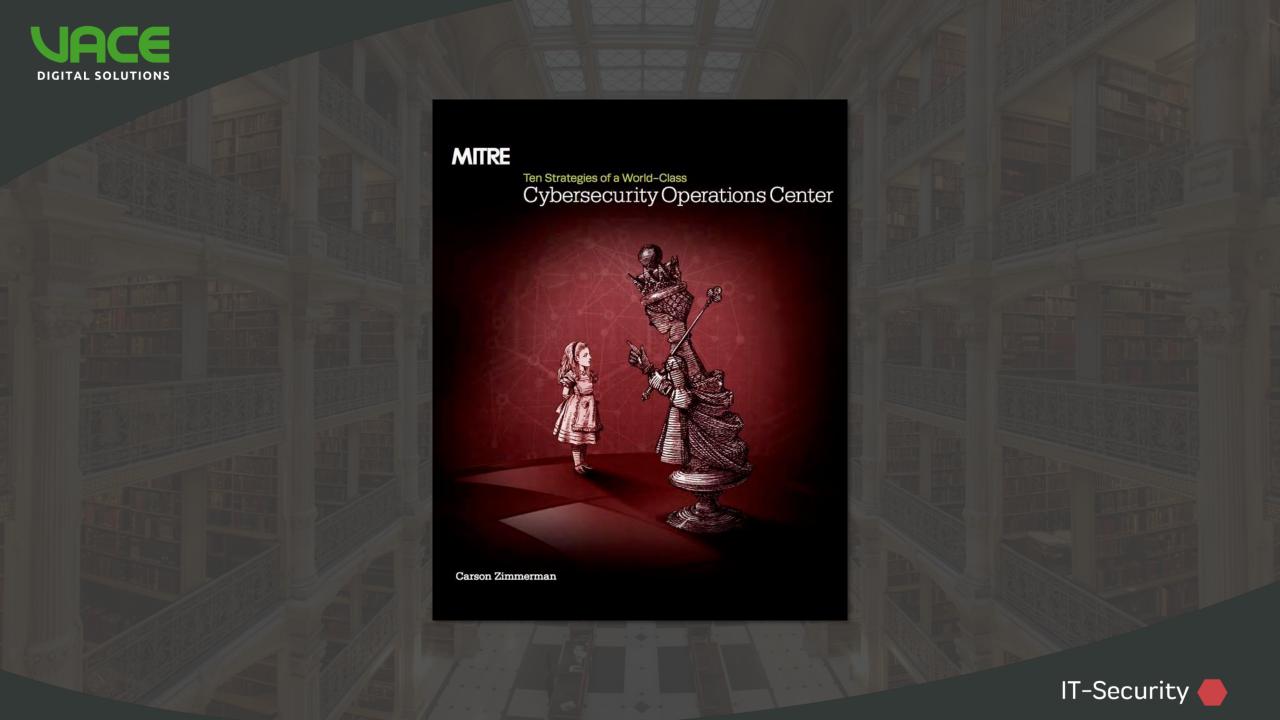




Notification Sources









SOC Enablers



Technology



Process

People





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

Ш

Insourcing

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





SOC

Budget

Authority



Do a Few Things Well



Incident Analysis and Response SOC Tool Life-Cycle Support

Real-Time Analysis Intel and Trending Scanning and Assessment

...



Favor Staff Quality over Quantity



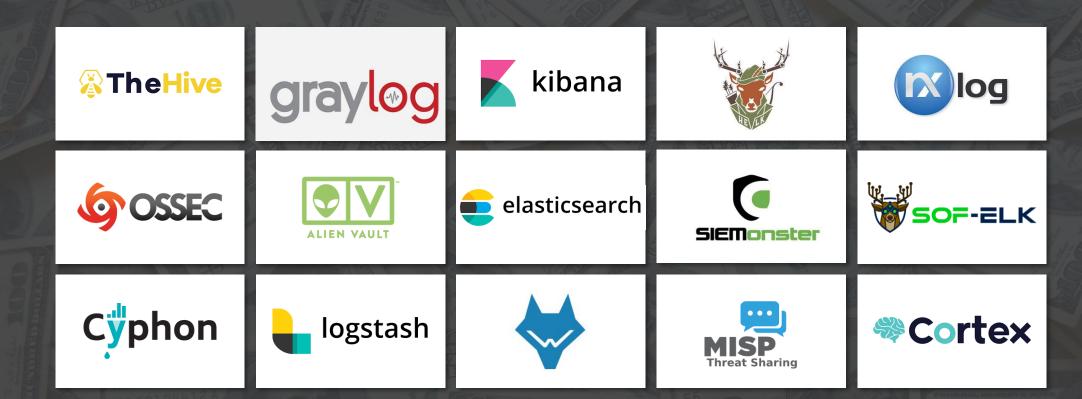
With the right tools, one good analyst can do the job of 100 mediocre ones.

Analyst quality is vastly more important than analyst quantity.



Maximize the Value of Technology Purchases

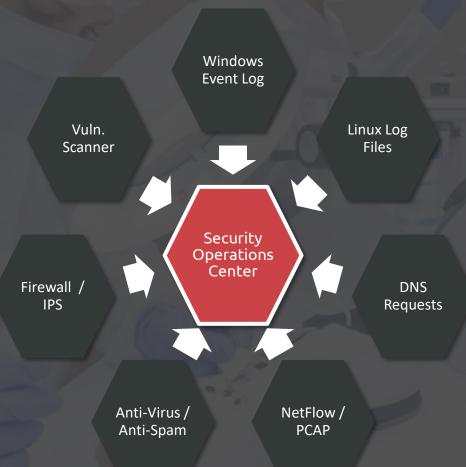






Exercise Discrimination in the Data you Gather

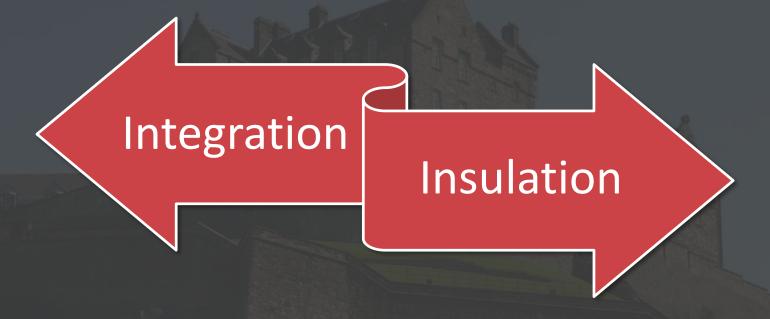






Protect the SOC Mission





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

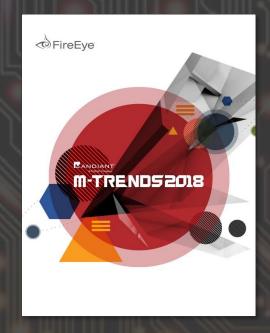


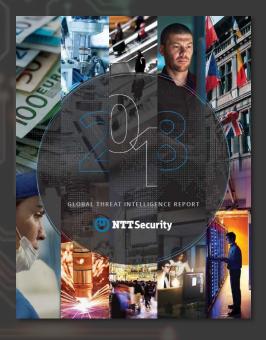
Consume Available Cyber Threat Intelligence



















Stop. Think. Respond ... Calmly







SOC Enablers



Technology



Process

People





www.vace.at

Thomas Kastner

SECURITY CONSULTANT

VACE Systemtechnik GmbH

Linzer Straße 16e

A-4221 Steyregg

t.kastner@vace.at

T +43 (0) 732 / 272277 62

M +43 (0) 664 / 88288774

F +43 (0) 732 / 272277 99



JUST DO IT.