TEMET
end-to-end IT security

In our SOC we Trust

Swiss Cyber Storm 2019

Bruno Blumenthal

15.10.2019

About the speaker

Bruno Blumenthal

Dipl. Inf. FH Informatik
CISM, CISA, CISSP

Expert Security Consultant
In IT Security since 2004

Specialties
Information Security Management
Security Architecture and Strategy
Risk Management

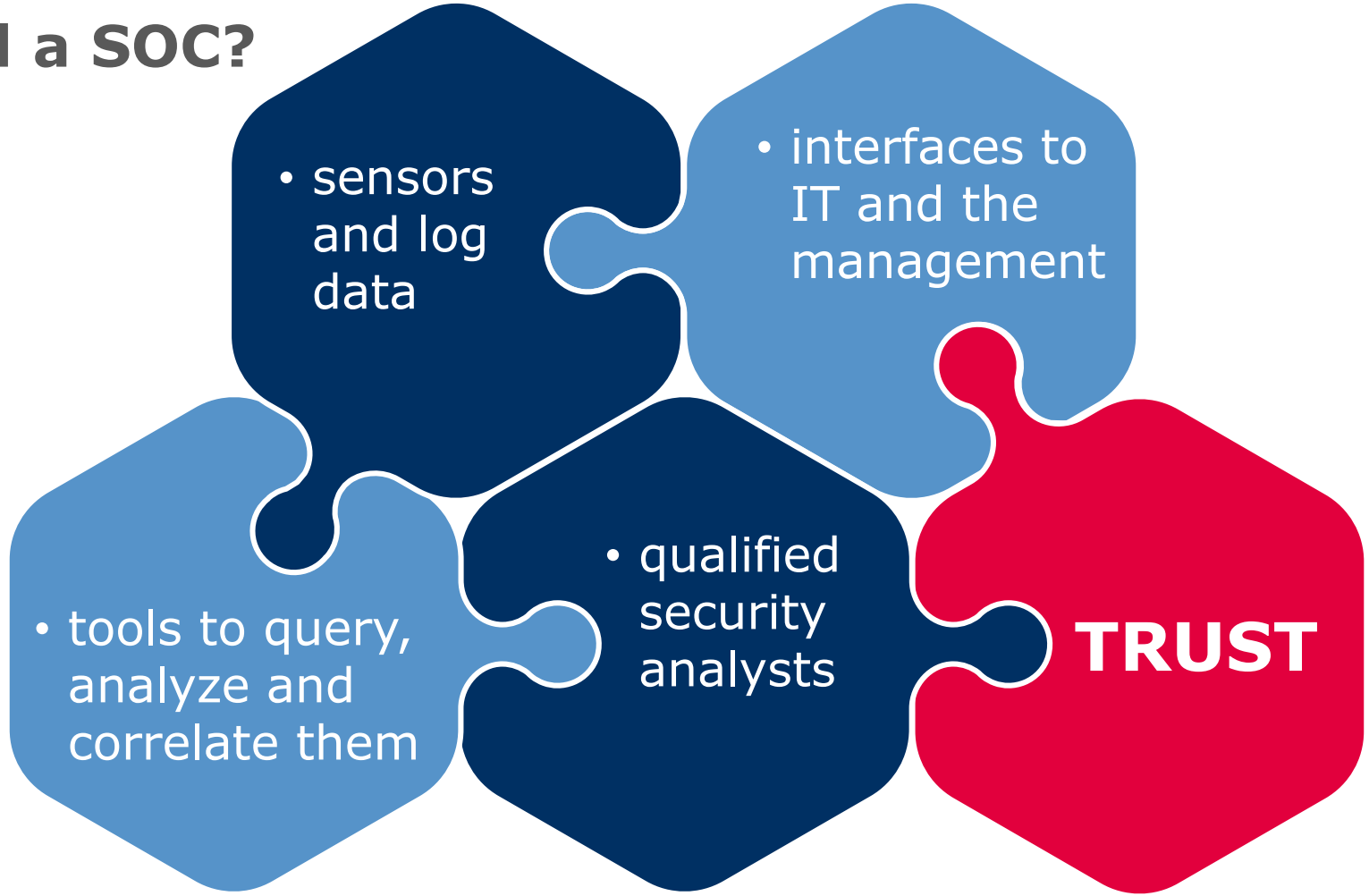
Contact
Mobile: +41 78 859 57 15
E-Mail: bruno.blumenthal@temet.ch

The missing piece

TEMET
end-to-end IT security

So, you want to build a SOC?

You'll need:



Trust in the SOC

TEMET
end-to-end IT security

You say of course, a SOC needs to be trusted by its peers!

- Trust is the basis information sharing
- CERT organizations are based on trust

FIRST Improving Security Together

TF-CSIRT Trusted Introducer

But what about the **trust** in the **SOC** by the **organization** it is **tasked** to **protect**?

Trust in the SOC

TEMET
end-to-end IT security

Let's talk about the **trust**
of the **organization** in its **SOC**

The management needs to trust too

TEMET
end-to-end IT security

Especially when the inevitable happens!

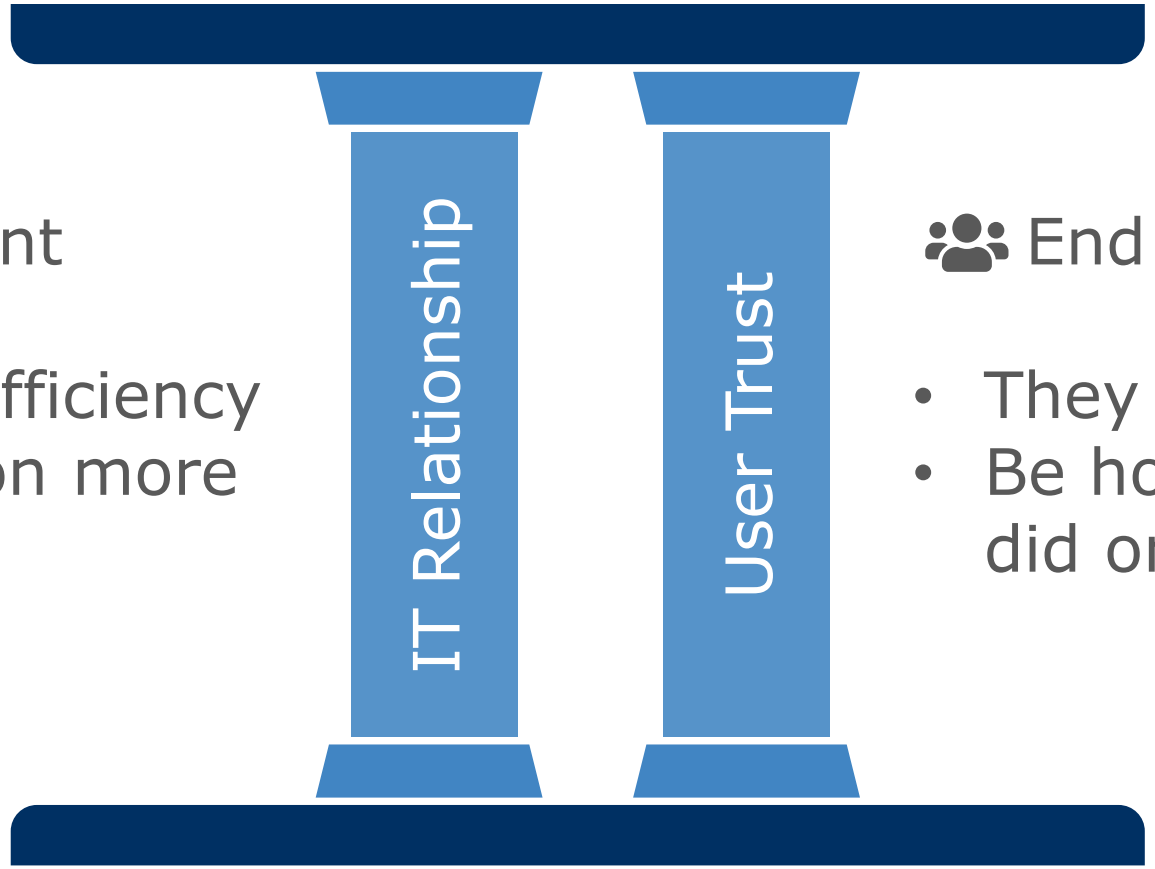
- Who they gonna call?
- You want tough decisions of them:
  - Shut down business applications
  - Cut network connectivity
  - Implement emergency changes or patches
  - Let the attackers keep going

It's the **management** that ultimately stays **accountable** and decides upon your **SOCs recommendations**

The everyday incident

TEMET
end-to-end IT security

Its not just the big shots that are important!



IT department

- Trust brings efficiency
- Less discussion more action

End Users

- They will report issues
- Be honest about what they did or didn’t do

Trust can’t be bought or ordered

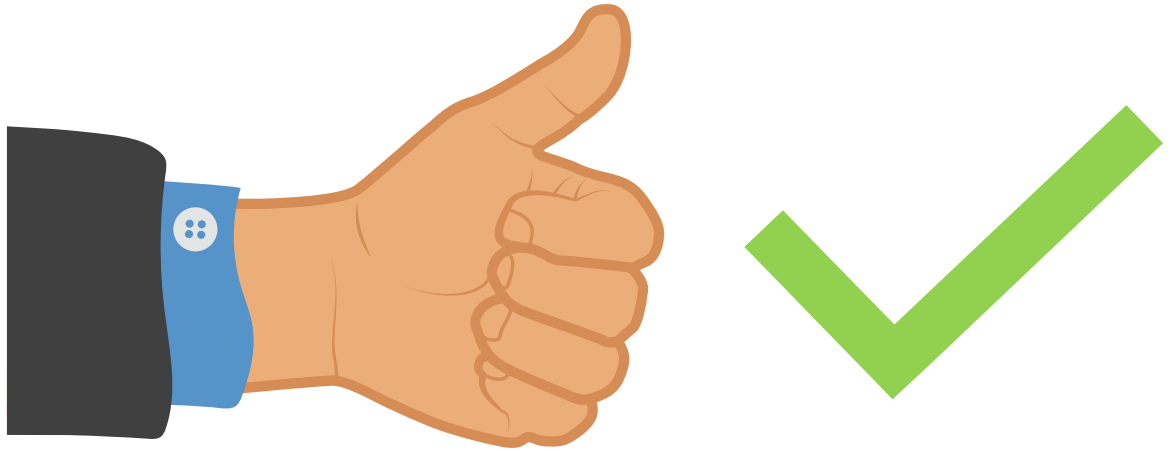
TEMET
end-to-end IT security

Become visible in a positive way!

Which isn’t easy if your task is to find thing that aren’t positive by definition!

You need to create:

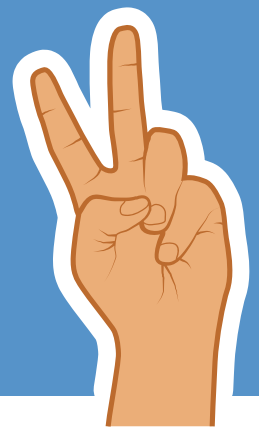
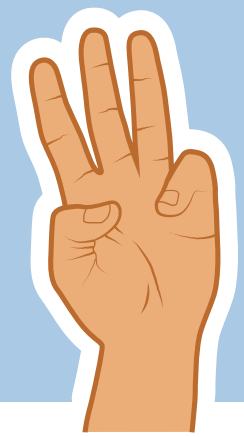
Positive Visibility



Positive visibility strategy

TEMET
end-to-end IT security

Three strategies to create positive visibility!

Be reactive and communicate	Trust-building as conscious activity	Use your capabilities to relieve the users
		

Be reactive

TEMET
end-to-end IT security

Give fast feedback with a positive attitude!

- React always on user input
- Be timely with your feedback

- Don’t shame and blame
- Thank them for helping

You want the **user** as **partner,**
not somebody who sees you as **enemy**

Actionable advice

TEMET
end-to-end IT security

What is their perspective?

- Who will be affected by countermeasures?
- Understand their view, their problems and challenges
- Be pragmatic and realistic
- Don’t tell them they should not do their job

They will **never trust** you if they think you **don’t understand** them

Do good and talk about it

TEMET
end-to-end IT security

Talk about incidents

Show how working together worked

Use all internal communication channels

It's about presenting yourself and your value added

Do good and talk about it

TEMET
end-to-end IT security

Marketing is not something inherently evil,
use it to get **positive visibility**

Report you improvements

TEMET
end-to-end IT security

Creating any value? Hopefully, yes!

- KPIs should measure improvement
- Avoid numbers you can't influence
- Look for numbers relating to you SOC capabilities
- You're implementing your Use-Cases for a reason
  → measure their positive effect

Trust-building as conscious activity

TEMET
end-to-end IT security

Plan with trust-building in mind

Select use-cases and capabilities based on

- Threat landscape, exposure
- and positive visibility

Include communication and marketing in your playbooks

- Prepared statements for users and other stakeholders
- Identify showcases as part of every lessons learned

Trust-building as conscious activity

TEMET
end-to-end IT security

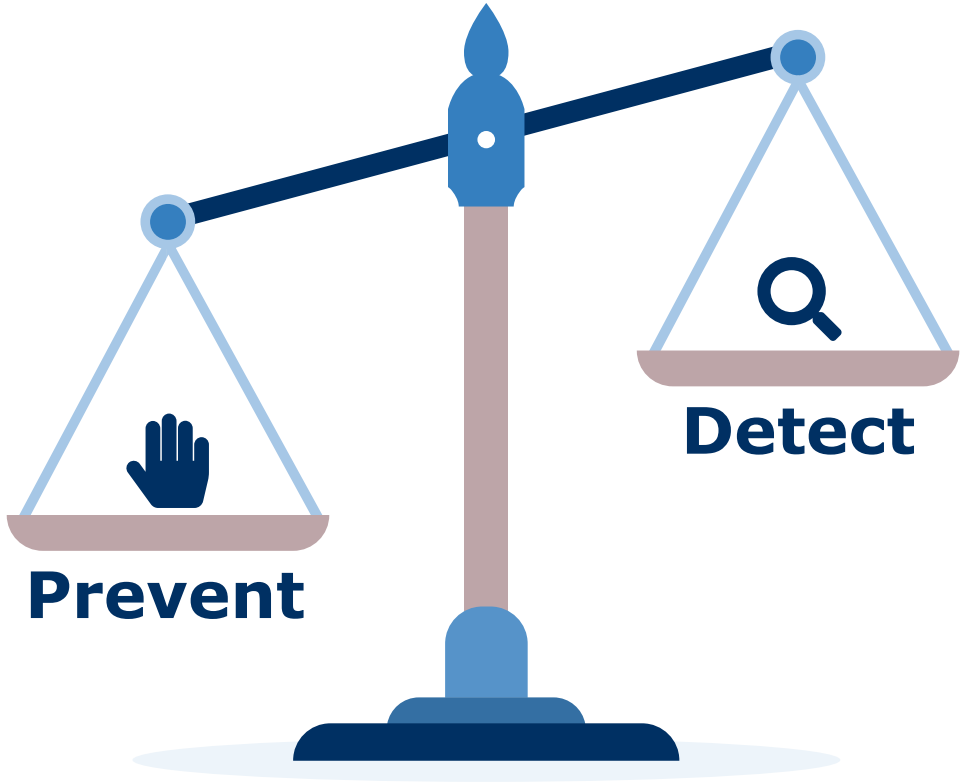
Set the **trust** of the organization as a **goal** for the **SOC** and **measure** your **progress**

Better detection capabilities

TEMET
end-to-end IT security

Use your power to relieve the users!

Preventive measures are perceived negative



Leverage your detective capabilities to reduced the users burden

Tip the scale to gain positive visibility

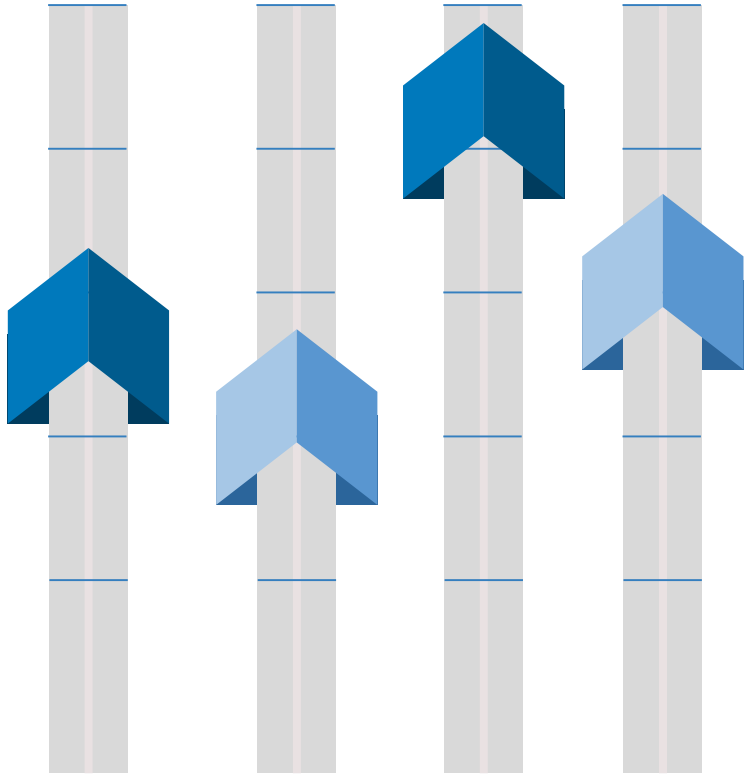
Focus on overall risk exposure

TEMET
end-to-end IT security

Shift the risk and improve you image!

Examples:

- Fewer access denied
  - Reduce access denied on legitimate requests
  - Compensate with better monitoring
- More time to patch
  - Leverage threat intel and monitoring
  - Give IT time to plan and test



Focus on overall risk exposure

TEMET
end-to-end IT security

Don’t **underestimate** the **risk** of
users circumventing obstructive measures

If the house is on fire

The management wants to know
who **to call**, who **to trust** for advice

If you have to **introduce yourself** first or they think
you're the guy **crying "wolf"** all the time

Without trust you won't be able to **fulfill** your **mission**
and protect the organization from further harm

Build your **SOC** to become a **trusted partner** for your organization

… to success

TEMET
end-to-end IT security

Thank you
for your attention

TEMET AG
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch