Why SOCs Fail

Bradley Freeman

SENSE ON

ON A MISSION

v2

Who am I?

Director of Technology - SenseOn

Previously

- Threat Hunting - BT
- SOC Manager - EE
- Offshore security stuff - GE

CISSP, CISM, TOGAF, etc..

https://www.linkedin.com/in/b-freeman/

What you will learn

What you will learn

Understand common traps and reasons for SOC failure, based on my stories & experience.

Use this information to deliver more effective security operations.

What we will cover

- High level talk on SOC implementation.
- Getting the basics right, and common traps.
- How the SOC can reduce risk through the effective detection, response and management of security events

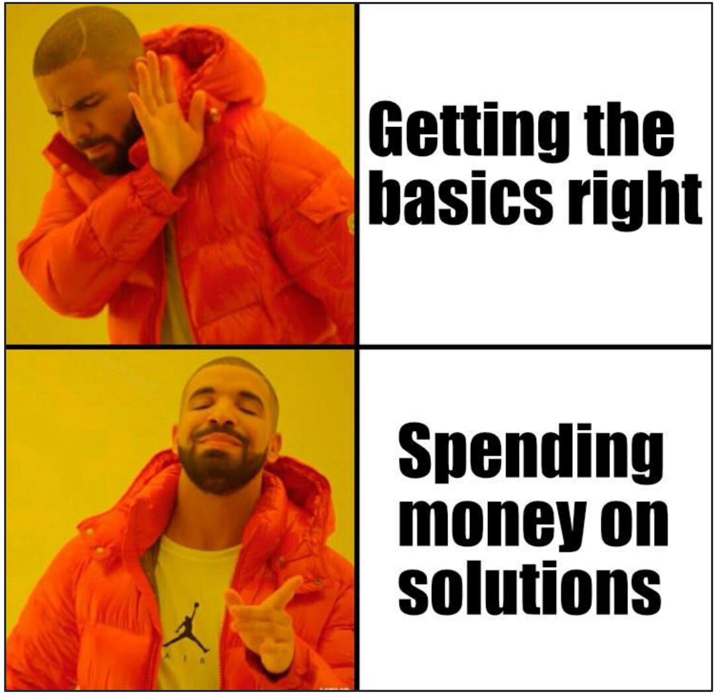
The basics, getting them right

Three fundamental components:

1. People
2. Process
3. Technology

Four basic levels:

1. Nothing
2. Good Hygiene
3. Standards Orientated
4. Best Practices



The catch 22 of security

Should:

Technology define processes or people?

People define technology or process?

Process define people or technology?

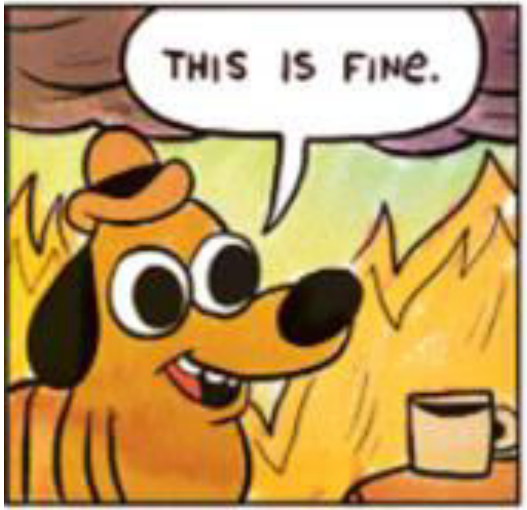
People

Skilled analysts

To retain good analysts you need to:

- Generate interesting investigations
- Enable technical curiosity (threat hunting)

Enabling curious analysts to reach their potential is fulfilling and promotes retention



How to upskill analysts?

Common trap

Fully outsourcing Security Operations as you don't have the skills.

Upskill your team

You don't need the best analysts.

Hire for coachability, intelligence and character.

Enable them to progress with the right tooling and training.

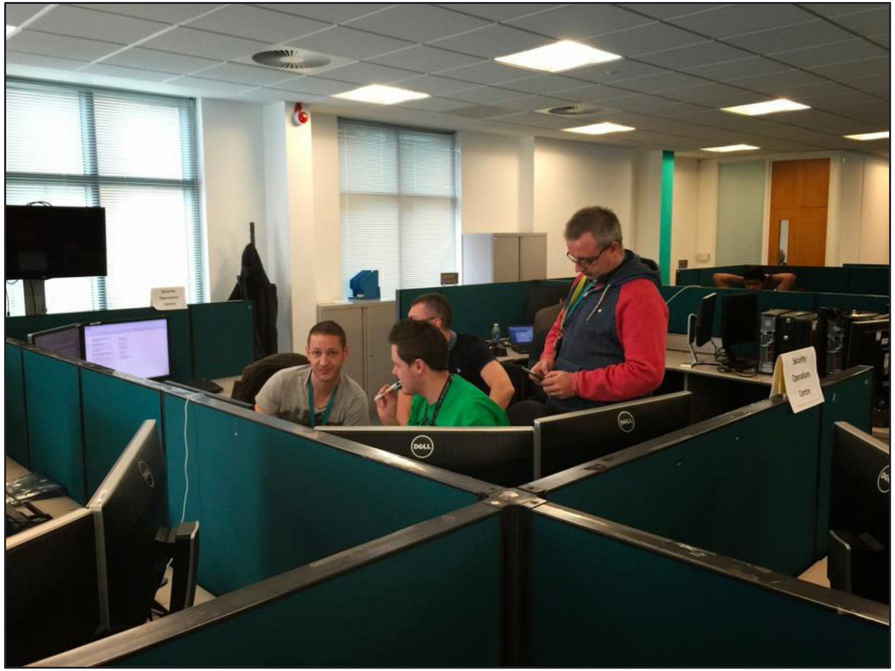
Make the SOC work

Make the SOC work

↓

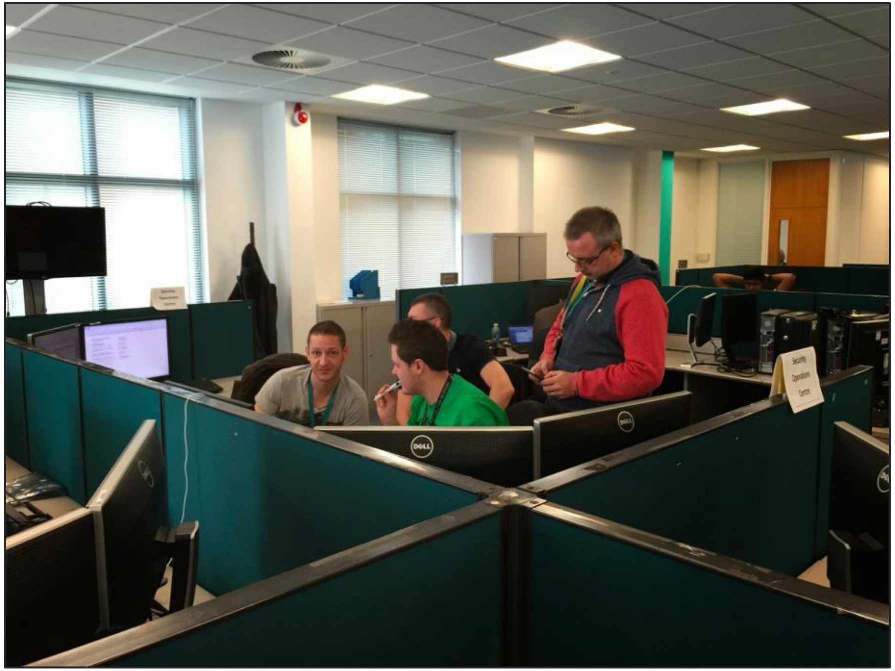
"Perception is reality"

An internal brand for your SOC

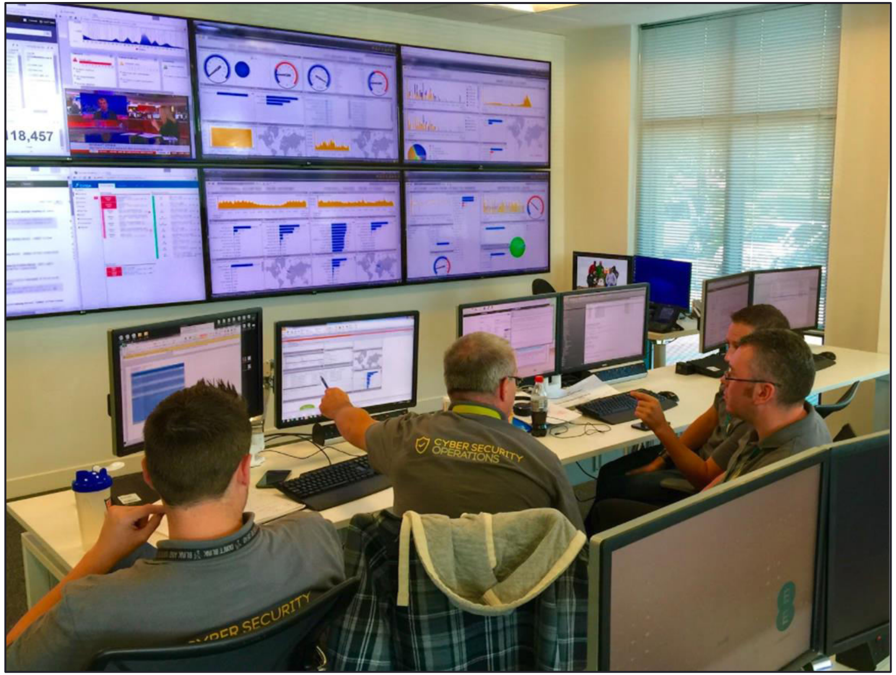


Before

An internal brand for your SOC



Before



After

Outward SOC engagement

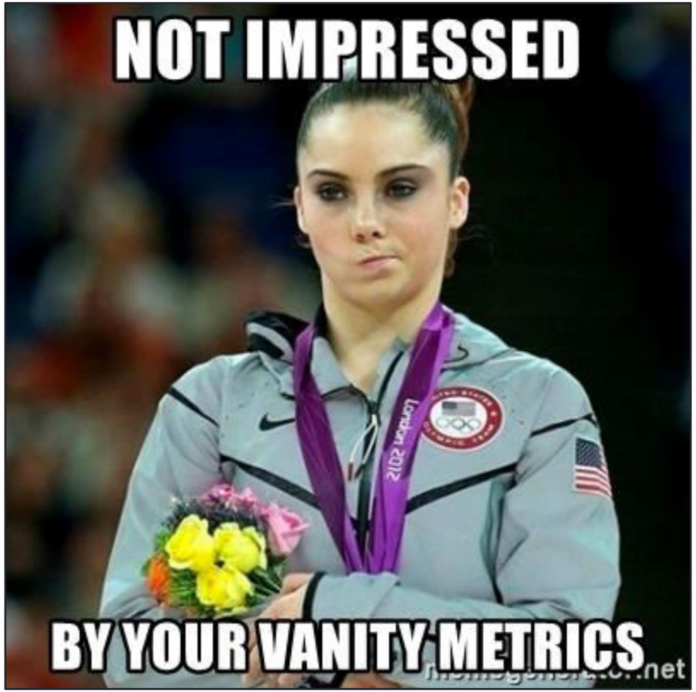
Internal and external team development.

Value engagement:

Show value to management

Show value to the wider business

Show value to the wider security team



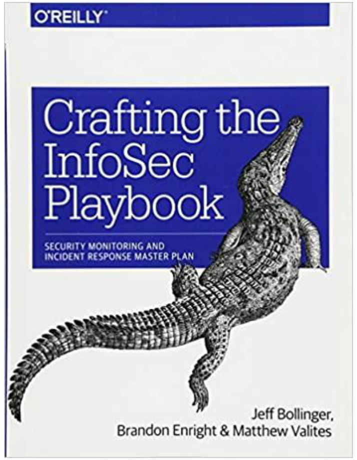
Process

Playbooks and use cases

Use Cases are essential to scale teams and processes effectively across skill levels.

However use case are often done wrong.

Iterative use case development will eventually overwhelm your level 1 analysts.


O'REILLY
Crafting the InfoSec Playbook
SECURITY MONITORING AND INCIDENT RESPONSE MASTER PLAN
Jeff Bollinger, Brandon Enright & Matthew Valites

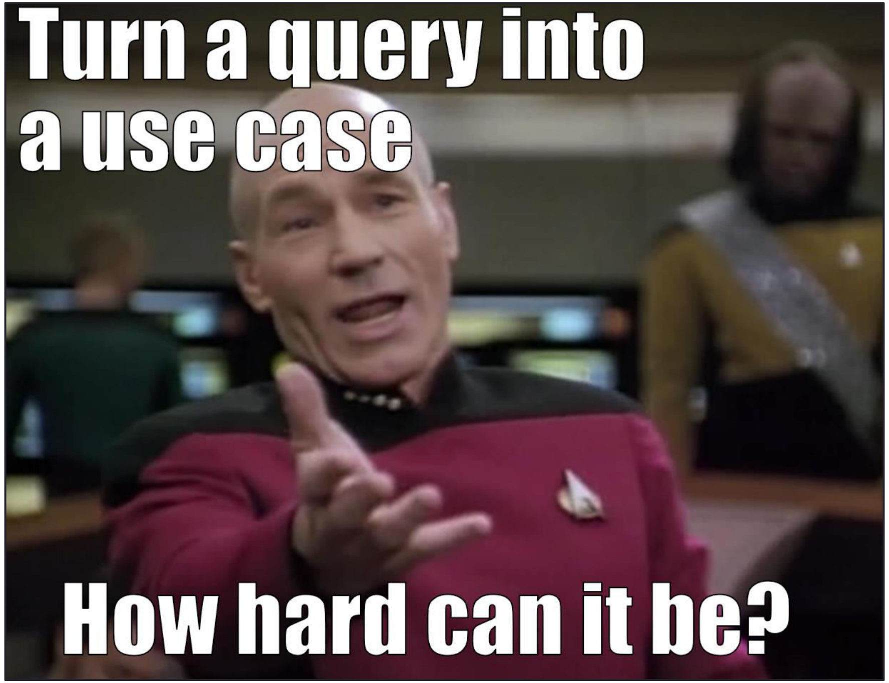
Good book on how to do it right

Detection processes done badly

Brute force attacks are simple right?

Don't drive technology decisions with process.

Process should support technology and people.



Technology

"Technology is not strategy"

Buying tools is complicated…

AV

Firewall

IDS

IPS

SIEM

DLP

EDR

NDR

UTM

WAF

Deception

UEBA

NG-?

Honeypot

EPP

VM

SOAR

XDR

CAS
B

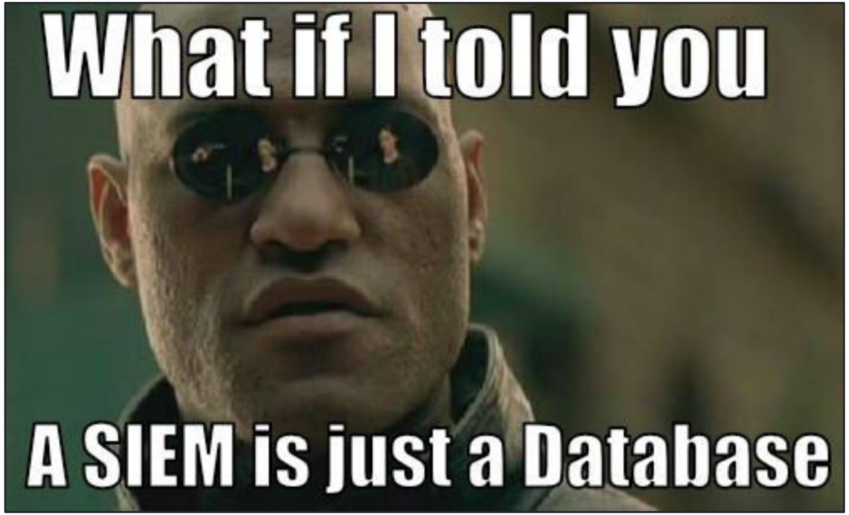
(C)TI

Bringing it together

There are lots of single point solutions.

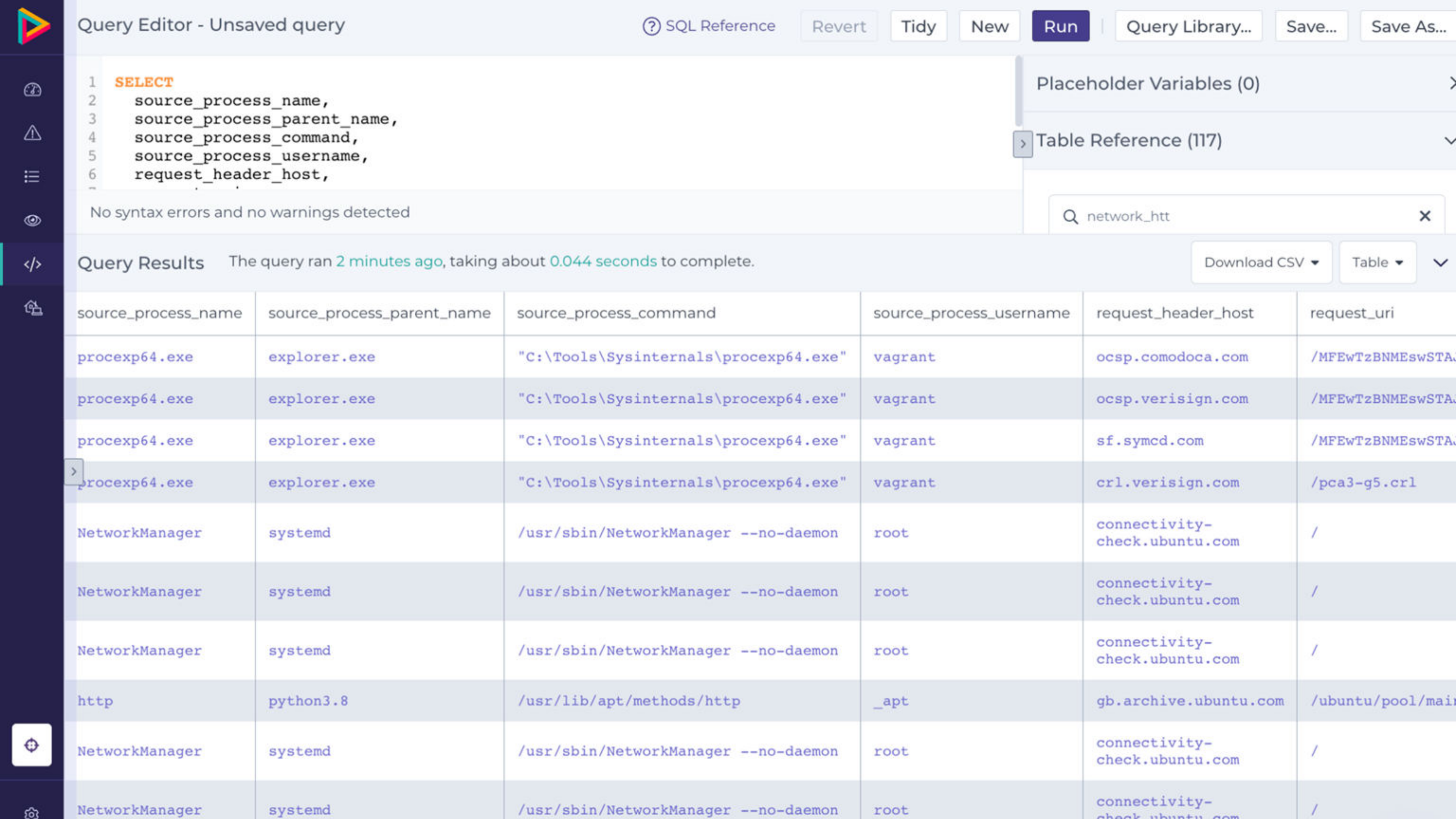
Enter the SIEM to bring it together.

Enter the SOAR to bring it together.



Case study:
Nation State Command & Control

Unified Telemetry



```
SELECT
  source_process_name,
  source_process_parent_name,
  source_process_command,
  source_process_username,
  request_header_host,
```

No syntax errors and no warnings detected

The query ran 2 minutes ago, taking about 0.044 seconds to complete.

source_process_name	source_process_parent_name	source_process_command	source_process_username	request_header_host	request_uri
procexp64.exe	explorer.exe	"C:\Tools\Sysinternals\procexp64.exe"	vagrant	ocsp.comodoca.com	/MFEwTzBNMEswSTA
procexp64.exe	explorer.exe	"C:\Tools\Sysinternals\procexp64.exe"	vagrant	ocsp.verisign.com	/MFEwTzBNMEswSTA
procexp64.exe	explorer.exe	"C:\Tools\Sysinternals\procexp64.exe"	vagrant	sf.symcd.com	/MFEwTzBNMEswSTA
procexp64.exe	explorer.exe	"C:\Tools\Sysinternals\procexp64.exe"	vagrant	crl.verisign.com	/pca3-g5.crl
NetworkManager	systemd	/usr/sbin/NetworkManager --no-daemon	root	connectivity-check.ubuntu.com	/
NetworkManager	systemd	/usr/sbin/NetworkManager --no-daemon	root	connectivity-check.ubuntu.com	/
NetworkManager	systemd	/usr/sbin/NetworkManager --no-daemon	root	connectivity-check.ubuntu.com	/
http	python3.8	/usr/lib/apt/methods/http	_apt	gb.archive.ubuntu.com	/ubuntu/pool/mai
NetworkManager	systemd	/usr/sbin/NetworkManager --no-daemon	root	connectivity-check.ubuntu.com	/
NetworkManager	systemd	/usr/sbin/NetworkManager --no-daemon	root	connectivity-check.ubuntu.com	/

Summary

Develop your people, enable their curiosity.

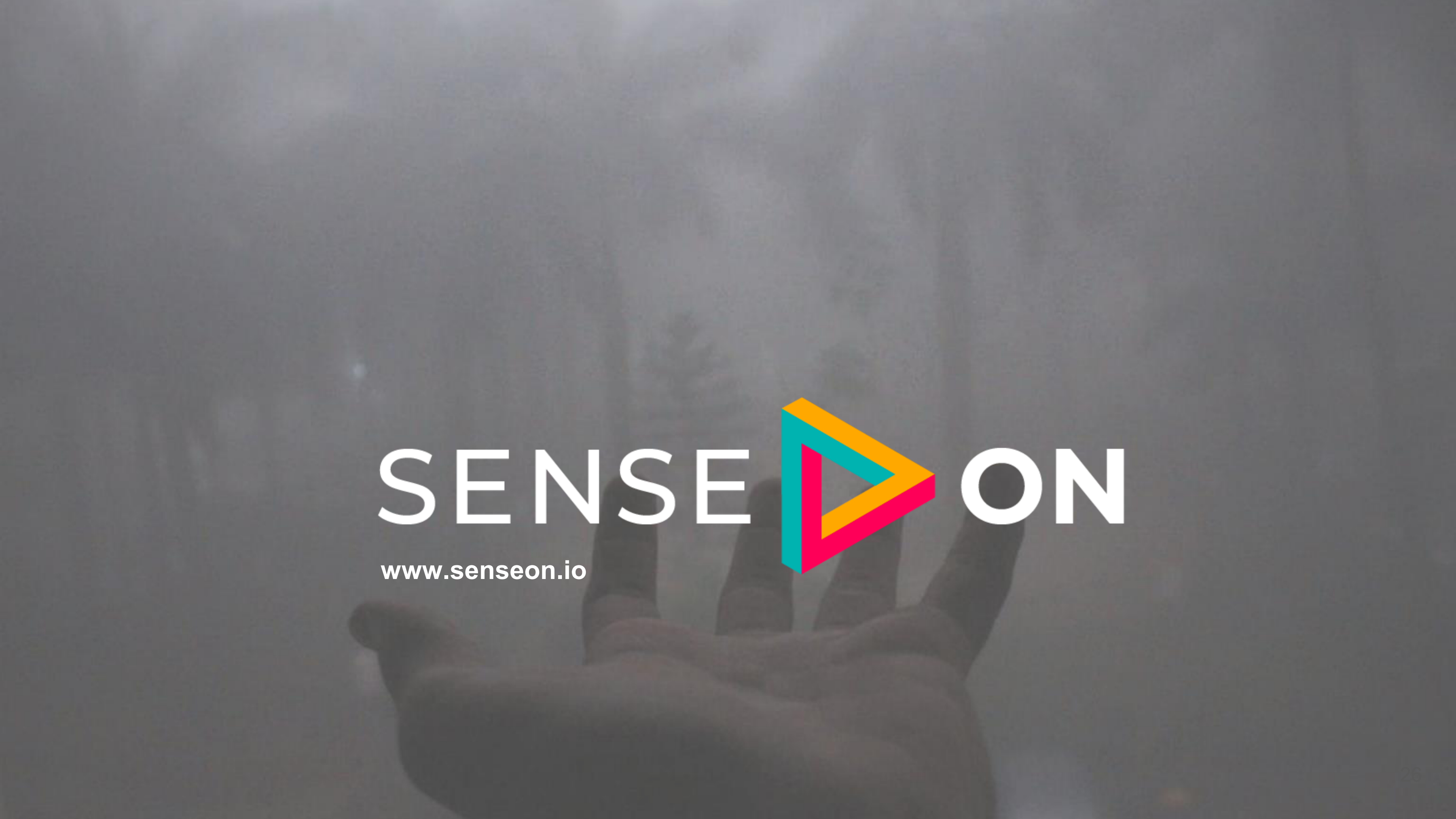
Show value to the business, much more than vanity metrics.

Use processes appropriately, don't be a burden to them.

Technology isn't a strategy, there is no silver bullet.

Make technology decisions that solve your problem, not fill a specific technology box.

YOUR MISSION IS OUR MISSION



SENSEON

www.senseon.io