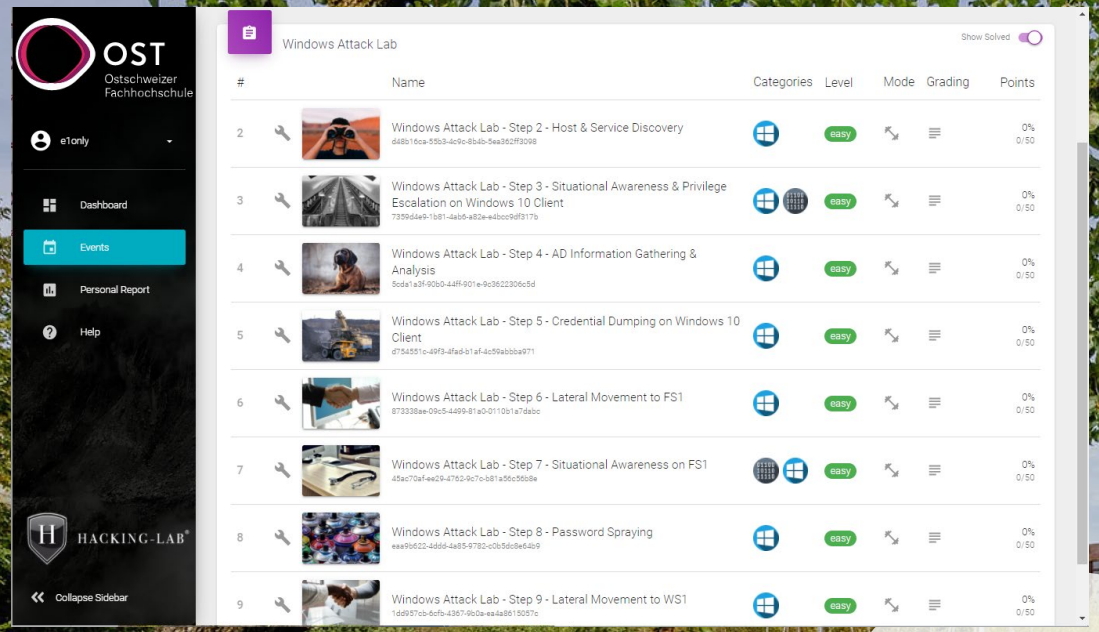


OST
Ostschweizer
Fachhochschule

SIEM, SOAR, EDR, CIRT, YARA

Cyber Defense – Ivan Bütler

Ivan Bütler

6. Oktober 2024

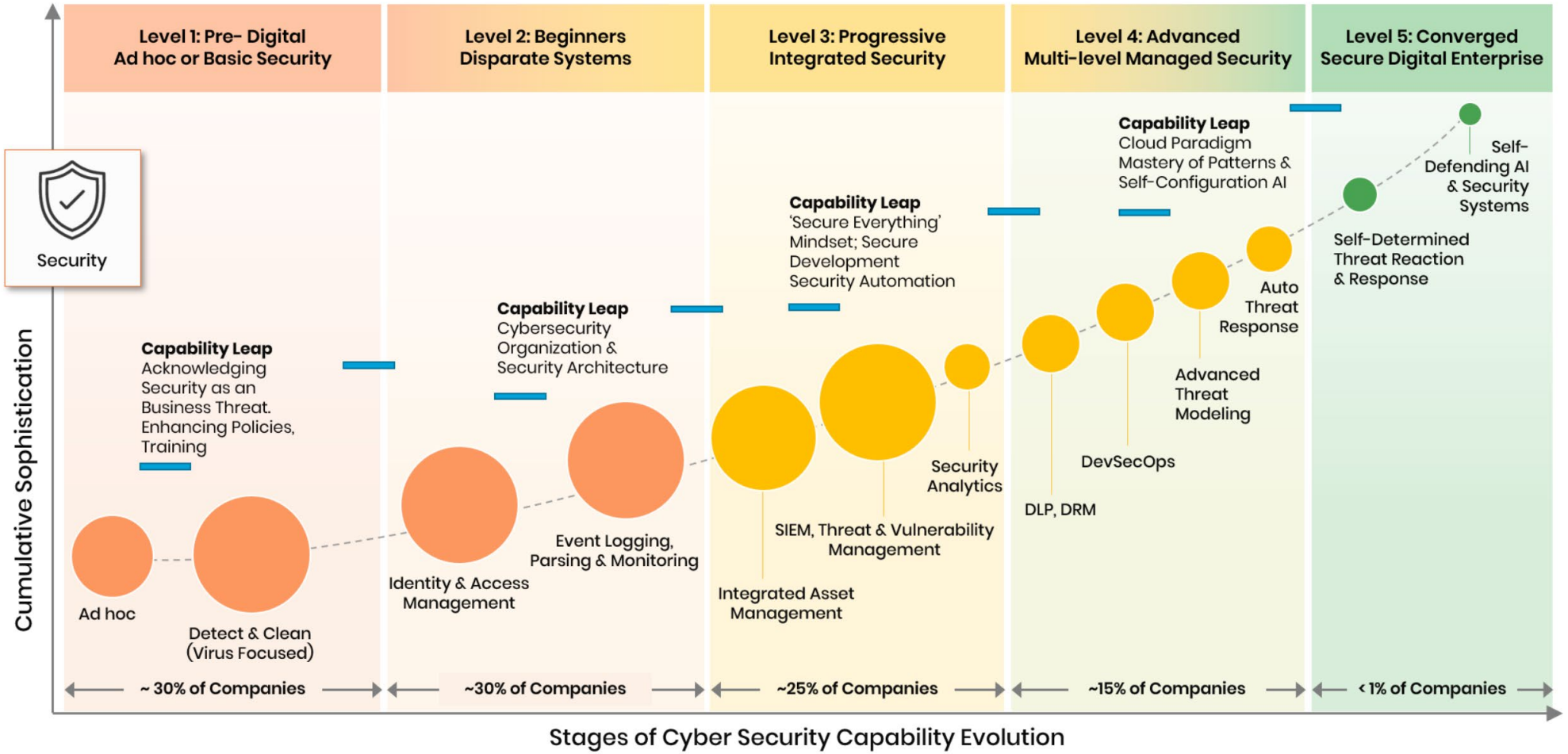
OST Cyber Defense

Agenda

- Digital Enterprise Security Level
- SIEM
- SOAR
- DER
- Velociraptor
- YARA
- CSIRT / CIRT

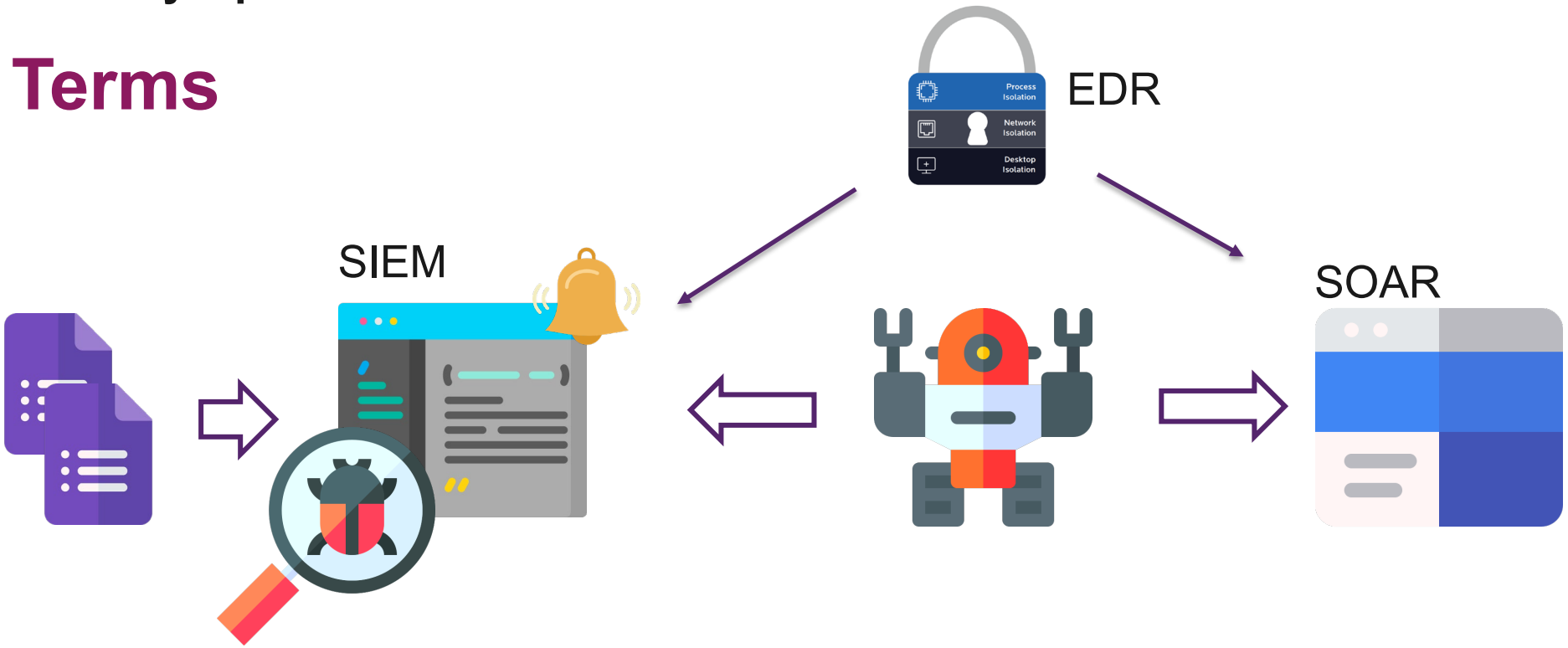
Evolution

Digital Enterprise Evolution Model™ - Cybersecurity Capability



Quelle: https://www.trianz.com/cybersecurity

Terms



SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response Solutions
EDR	Endpoint Protection and Response

SIEM

Security Information and Event Management solutions are responsible for collecting log and event data from various sources such as network, servers and applications and aggregating, identifying, categorizing and analyzing it in real time.

With a SIEM solution, security problems should be detected automatically as well as the ability to send an alert

- Enables pattern search in log data for indicators of a cyberattack (IOC)
- Enables correlation of event information and identifies abnormal activity
- Alerts according to defined alert rules

Explanation of terms

SIEM

For the seventh consecutive year, Splunk has been ranked by Gartner as a leader in the 2021 Magic Quadrant for Security Information and Event Management (SIEM).

splunk>

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (February 2020)

SOAR

SOAR also collects data from various sources similar to a SIEM, but SOAR supports the incident responder in managing the crisis. SOAR enables **automated** intervention when a security incident occurs. A SOAR system also supports the incident responder in rolling out security countermeasures (Active Directory).

- Alert Investigation
- Orchestration
- Automation workflow

Begriffe

EDR

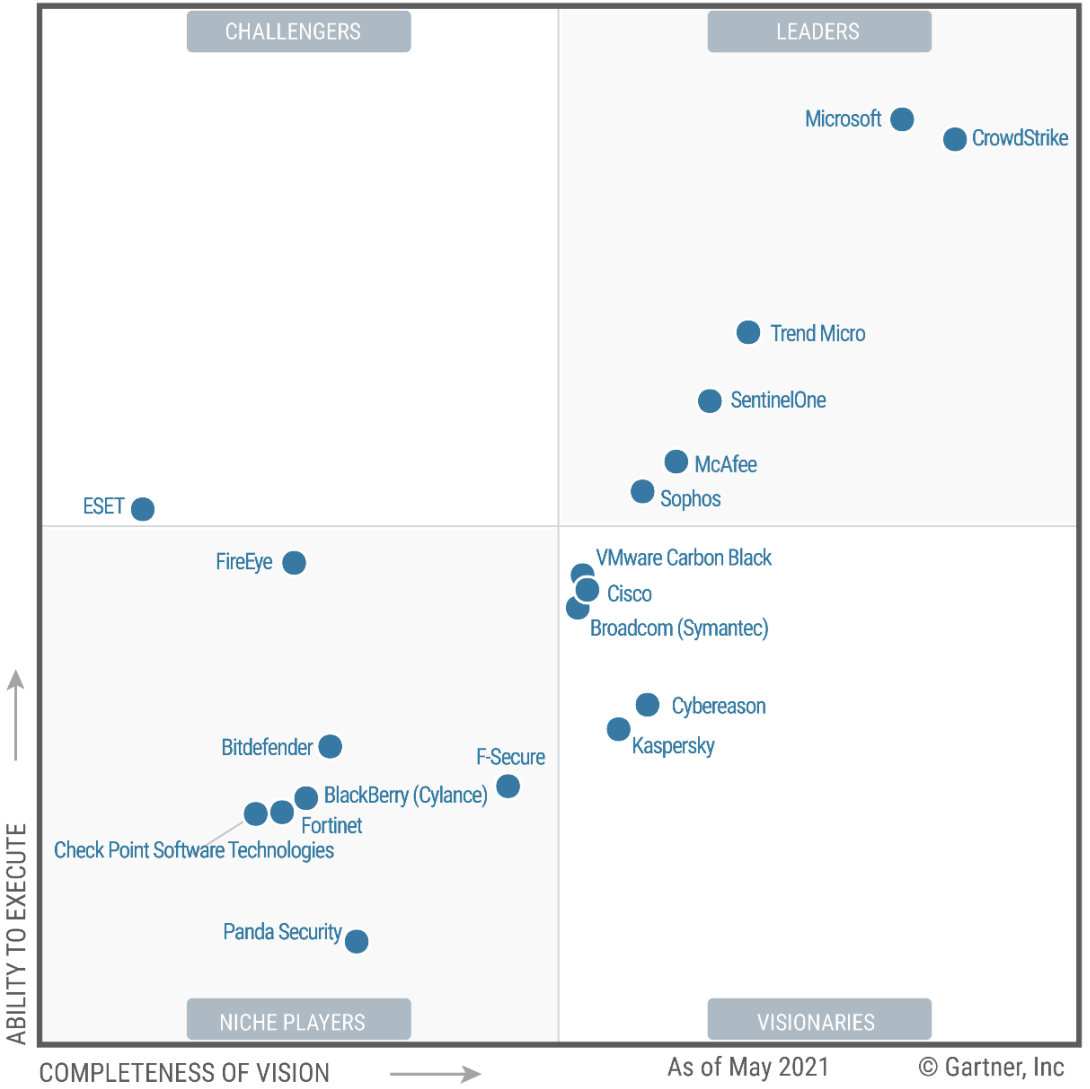
Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of **endpoint data** with rules-based automated response and analysis capabilities

May 11, 2021

> Gartner names Microsoft a Leader in the 2021 Endpoint Protection Platforms Magic Quadrant

Rob Lefferts Corporate Vice President, Microsoft 365 Security

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

Velociraptor

SOAR approach

OST

Velociraptor Use-Case

A powerful DFIR technique is searching bulk data for patterns

- Searching for CC data in process memory
- Searching for URLs in process memory
- Searching binaries for malware signatures
- Searching registry for patterns

Bulk searching helps to identify evidence without needing to parse file formats

Velociraptor Console: Search for Hosts

Velociraptor Response and Monit

Not secure | localhost:8889/app/index.html?#/search/*winattacklab*

winattacklab

Show All

sma

Client ID	Hostname	OS Version	Labels
C.a5782701aeaa25ad	Client1.winattacklab.local	Microsoft Windows 10 Enterprise for Virtual Desktops10.0.18363 Build 18363	
C.6bee654d36162481	DC1.winattacklab.local	Microsoft Windows Server 2019 Datacenter10.0.17763 Build 17763	
C.089c05507220bb47	FS1.winattacklab.local	Microsoft Windows Server 2019 Datacenter10.0.17763 Build 17763	
C.a6882b4d01bfe643	WS1.winattacklab.local	Microsoft Windows Server 2016 Datacenter10.0.14393 Build 14393	

10 25 30 50

« 0 1 › Goto Page

Note, for the lab, the forensics client is connected, too.

OST

Velociraptor Console: Access to connected Client

Velociraptor Response and Monit

Not secure | localhost:8889/app/index.html?#/host/C.a5782701aeaa25ad/detailed

winattacklab | Show All | Client1.winattacklab.local connected | sma

- Home
- Hunt Manager
- View Artifacts
- Server Events
- Server Artifacts
- Notebooks
- Host Information
- Virtual Filesystem
- Collected Artifacts
- Client Events

VFS | Collected | Overview | VQL Drilldown | Shell

ttacklab.local (C.a5782701aeaa25ad) @ 2021-05-13 10:44:42.344784975 +0000 GMT

ildTime	Labels	Hostname	OS	Architecture	Platform	PlatformVersion	KernelVersion	Fqdn	ADDomain
21-04-T22:11:10Z	[]	Client1	windows	amd64	Microsoft Windows 10 Enterprise for Virtual Desktops	10.0.18363 Build 18363	10.0.18363 Build 18363	Client1.winattacklab.local	winattacklab.local

50 Showing rows 1 to 1 of 1 1

Select a client and the lower part of the menu becomes active. It's always client dependent

OST

Velociraptor Console: Access Virtual File System of Client

Not secure | localhost:8889/app/index.html?#/vfs/C.a5782701aeaa25ad/file/

winattacklab | Show All | Client1.winattacklab.local connected | sma

- file
  - A:
  - C:
  - D:
  - E:
- ntfs
  - \\.\C:
  - \\.\D:
- registry
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_CONFIG
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_PERFORMANCE_DATA
  - HKEY_USERS
- artifacts
  - Generic.Client.Info
  - System.VFS.ListDirectory

C:	0	d---------	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z
D:	0	d---------	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z
E:	0	d---------	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z	0001-01-01T00:00:00Z

Please select a file or a folder to see its details here.

2021-05-13T12:25:09.204Z

OST

Velociraptor & YARA

- **YARA** is a powerful keyword scanner
- Uses rules designed to identify binary patterns in bulk data
- YARA is optimized to scan for many rules simultaneously.
- Velociraptor supports YARA scanning of bulk data (via accessors) and memory.

yara() and proc_yara()

YARA

yara

The pattern matching swiss knife for malware researchers (and everyone else)

{ } YARA in a nutshell

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

View project in GitHub

Download Latest release

Read the Documentation

Ask for help at YARA's group

Send Bug Report

Contact the author:

OST

YARA example: Drive-by attack (analyzed using Velociraptor)

You suspect a user was compromised by a drive by download (i.e. they clicked and downloaded malware delivered by mail, ads etc).

You think the user used the **Edge** browser but you have no idea of the internal structure of the browser cache/history etc.

Write an artifact to extract potential URLs from the Edge browser directory (also where is it?)

Step 1: Figure out where to look

```
LET edge = SELECT Pid FROM pslist()
WHERE Name =~ "Edge"
LIMIT 2

SELECT * FROM foreach(row=edge,
    query = {
     SELECT * FROM handles(pid=Pid)
     WHERE Type = 'File' AND Name =~ "User"
     LIMIT 500
   })
```

OST

Looks like somewhere in C:\Users\<name>\AppData\Local\Microsoft\Edge**

Show 10 entries

Pid	Type	Name
9276	File	\Device\HarddiskVolume4\Users\test\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\BrowserMetrics-5EBCA82E-243C.pma
9276	File	\Device\HarddiskVolume4\Users\test\AppData\Local\Microsoft\Edge\User Data\SmartScreen\local\cache
9276	File	\Device\HarddiskVolume4\Users\test\AppData\Local\Microsoft\Edge\User Data\SmartScreen\local\download_cache
9276	File	\Device\HarddiskVolume4\Users\test\AppData\Local\Microsoft\Edge\User Data\ShaderCache\GPUCache\index
9276	File	\Device\HarddiskVolume4\Users\test\AppData\Local\Microsoft\Edge\User Data\ShaderCache\GPUCache\data_2
9276	File	\Device\HarddiskVolume4\Users\test\AppData\Local\Microsoft\Edge\User Data\ShaderCache\GPUCache\data_2
9276	File	\Device\HarddiskVolume4\Users\test\AppData\Local\Microsoft\Edge\User Data\Default\Visited Links

OST

Step 2: Recover URLs

We don't exactly understand how Edge stores data but we know roughly what a URL is supposed to look like!

Yara is our sledgehammer !

```
rule URL {
  strings: $a = /https?:\\/\\/[a-z0-9\\/+&#:\\?.-]+/i
  condition: any of them
}
```

OST

Step 3: Let’s do this!

```
LET Globs = 'C:/Users/*/AppData/Local/Microsoft/Edge/**'
LET YaraRule = "rule URL {
    strings: $a = /https?:\\/\\/[a-z0-9\\/+&#:\\?.-]+/i
    condition: any of them
    }"

SELECT * FROM foreach(row={
   SELECT FullPath FROM glob(globs=Globs)
}, query={
   SELECT str(str=String.Data) AS Hit,
          String.Offset AS Offset,
          FileName FROM yara(files=FullPath, rules=YaraRule)
})
LIMIT 100
```

OST

Step 3: Results

Show 10 entries

Search:

Hit	Offset	FileName
https://assets.msn.com/bundles/v1/edgeChromium/latest/10.4d61ec8d15ed1bd48876.js	24	C:\Users\test\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\8436d9ca-9c01-4a31-9c3e-96fd6e6f5a9f\5d4c8d6643ca68f7_0
https://assets.msn.com/bundles/v1/edgeChromium/latest/10.4d61ec8d15ed1bd48876.js	24	C:\Users\test\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\8436d9ca-9c01-4a31-9c3e-96fd6e6f5a9f\5d4c8d6643ca68f7_1
https://assets.msn.com/bundles/v1/edgeChromium/latest/12.6a2f64876121d9765d26.js	24	C:\Users\test\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\8436d9ca-9c01-4a31-9c3e-96fd6e6f5a9f\69a2d3fdc5c3b46d_0
https://assets.msn.com/bundles/v1/edgeChromium/latest/12.6a2f64876121d9765d26.js	24	C:\Users\test\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\8436d9ca-9c01-4a31-9c3e-96fd6e6f5a9f\69a2d3fdc5c3b46d_1
https://assets.msn.com/bundles/v1/edgeChromium/latest/3.b37991b6e6355482318d.js	24	C:\Users\test\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\8436d9ca-9c01-4a31-9c3e-96fd6e6f5a9f\249f651f139086c2_0
		C:\Users\test\AppData\Local\Microsoft\Edge\User Data\Default\Service

OST

Wazuh Open Source SIEM

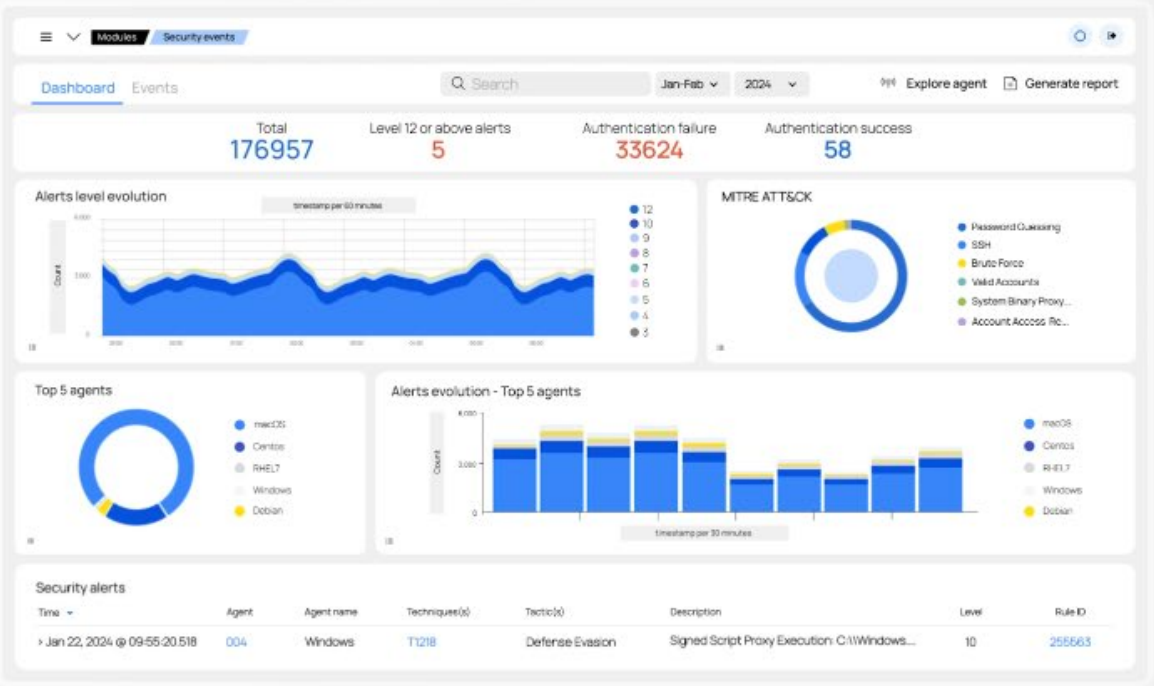
wazuh.

Platform ⌄ Cloud Documentation Services ⌄ Partners ⌄ Blog Company ⌄ Install Wazuh Log in

The Open Source Security Platform

Unified XDR and SIEM protection for endpoints and cloud workloads.

Install Wazuh Free Cloud Trial

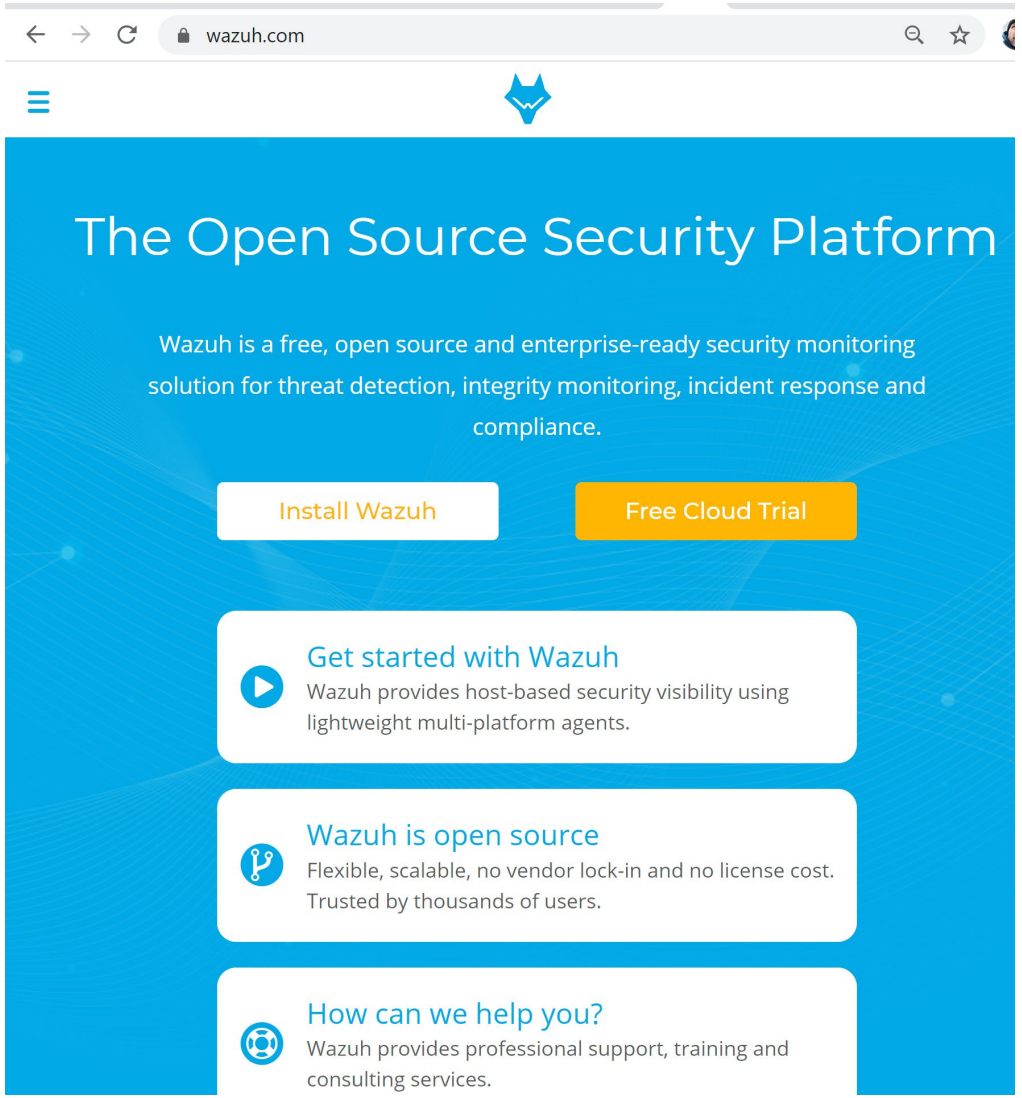


OST

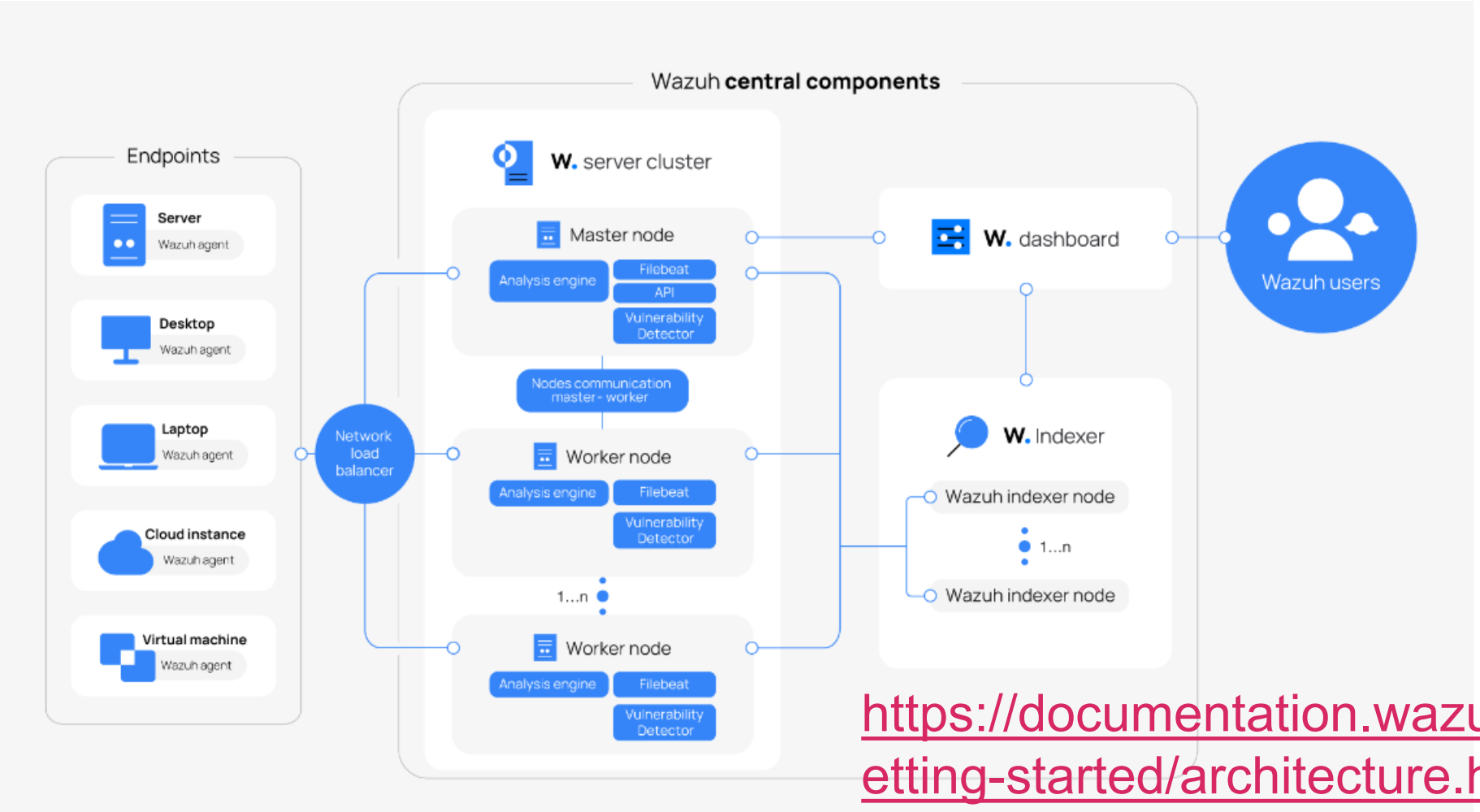
Wazuh

Wazuh is an open source security platform that focuses on infrastructure monitoring, security risk detection and incident response in the sense of a SIEM and EDR (Endpoint Detection & Response).

The so-called **Wazuh agent** is installed on the machines to be monitored and communicates with the **Wazuh manager**, which is installed on a server. To ensure that the data is clearly represented, it is further sent to components of Elastic Stack and displayed in a dashboard using Kibana. Translated with www.DeepL.com/Translator (free version)

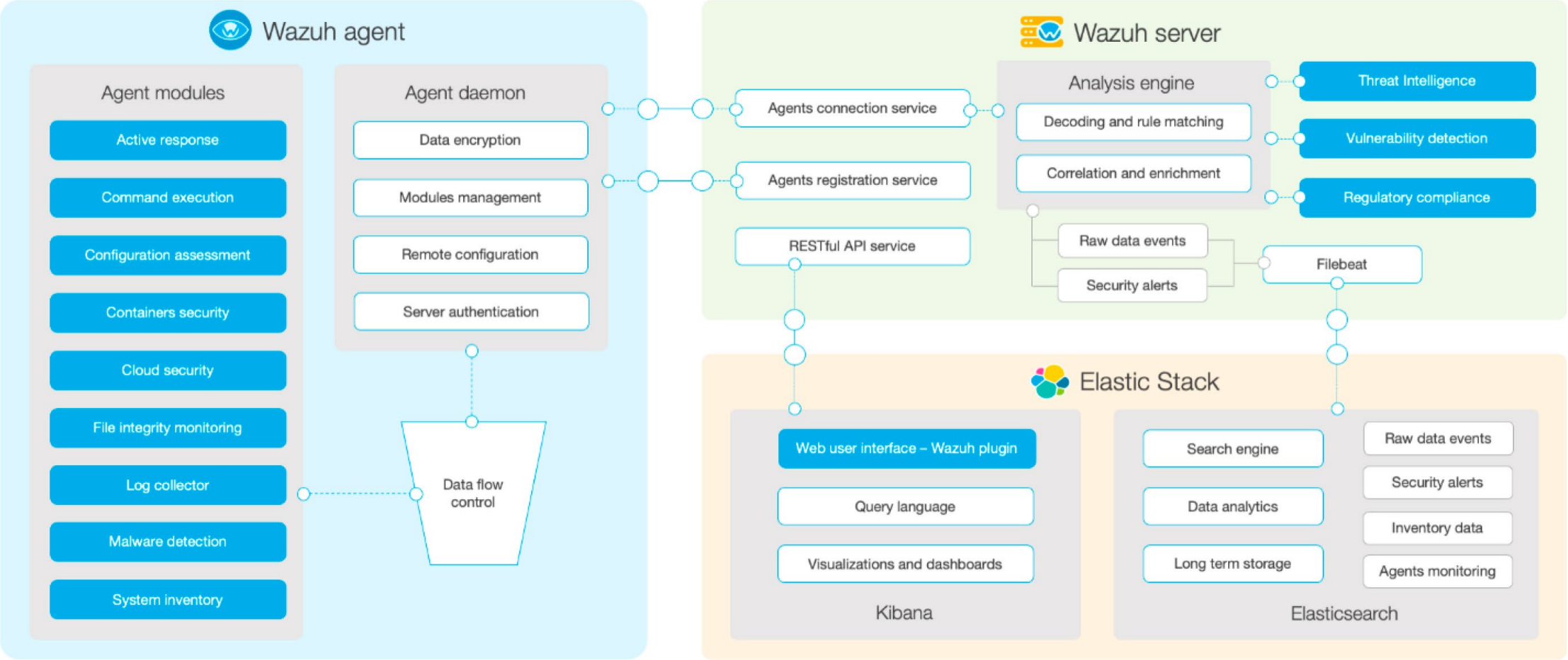


Wazuh Architektur

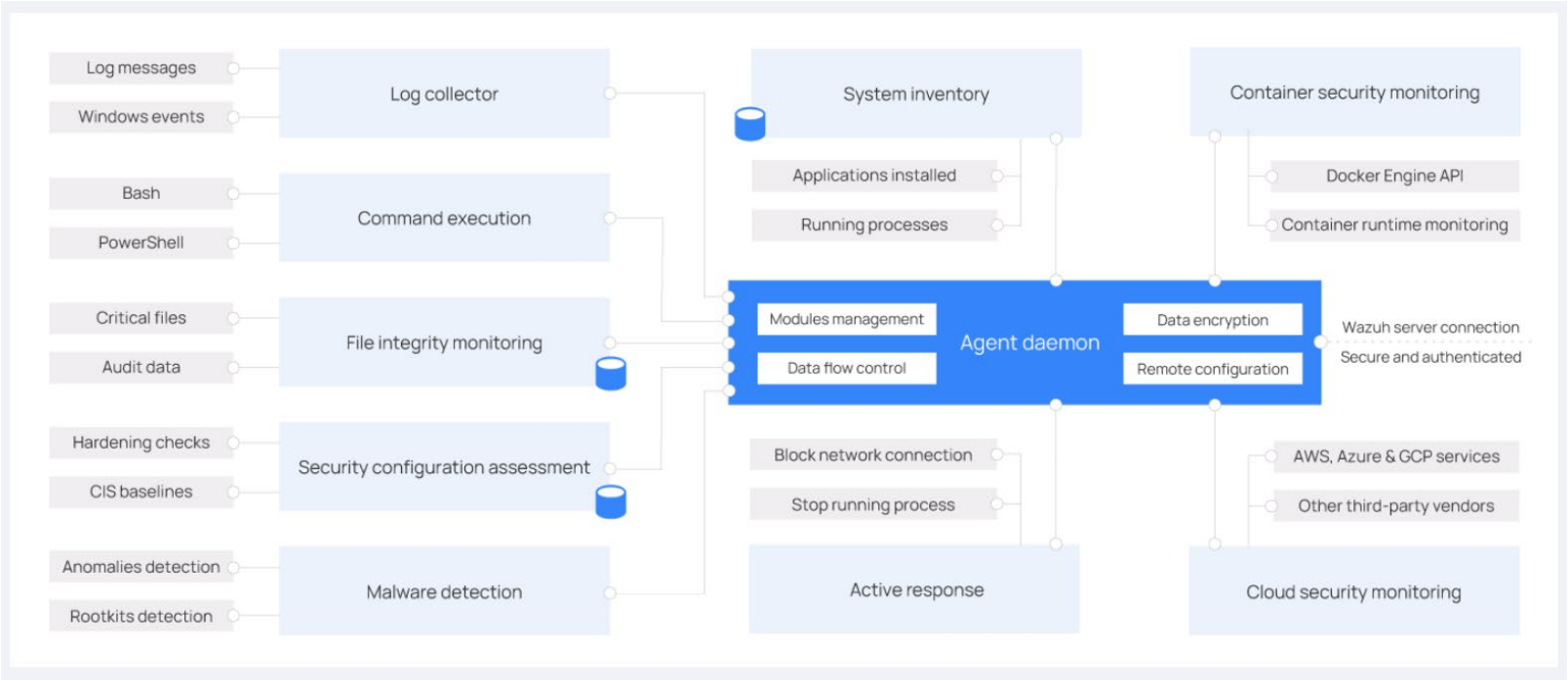


https://documentation.wazuh.com/current/getting-started/architecture.html

Wazuh Architektur



Wazuh Agent



- Agent Functionality
  - Integrity Monitoring
  - Log Collection
  - Open-SCAP
  - Configuration Assessment
  - Inventory
  - Docker Monitoring
  - Cloud Monitoring

https://documentation.wazuh.com/current/getting-started/components/wazuh-agent.html

CIRT / CSIRT

OST

CSIRT in Europe Map 2021

OST

CSIRT in CH List 2021 (582 Entries for Europe)

GovCERT.ch	CIIP, Government, National	Not member	Accredited	Member	govcert.admin....
NesCERT	Commercial Organisation	Not member	Not listed	Member	nestle.com/
NestleSOC	Commercial Organisation	Not member	Not listed	Member	nestle.com/
RIC-CSIRT	Commercial Organisation	Not member	Listed	Member	csirt.richemont...
CERT-Post	Commercial Organisation, Financial	Not member	Accredited	Member	post.ch
OS-CERT	Commercial Organisation, Service Provider Customer Base	Not member	Accredited	Member	open.ch/
UBS CIFI	Financial	Not member	Not listed	Member	ubs.com
VTCERT	Financial	Not member	Re-Listing Pending	Not member	vontobel.ch
SWITCH-CERT	Financial, NREN, National	Not member	Certified	Member	switch.ch/cert/
NCSC.ch	Government	Not member	Not listed	Member	ncsc.admin.ch/...
ISPIN-CERT	ICT vendor customer base	Not member	Not listed	Member	ispin.ch
PMI CERT	Industrial sector	Not member	Not listed	Member	pmi.com
CC-SEC	ISP Customer Base	Not member	Listed	Member	cablecom.ch/
KS-CERT	ISP Customer Base	Not member	Not listed	Member	Public website not available
Swisscom CSIRT	ISP Customer Base	Not member	Listed	Member	swisscom.ch/e...
CERN CERT	NREN	Not member	Listed	Not member	cern.ch/security
ETHZ-NSG	NREN	Not member	Re-Certification Candidate	Not member	www1.ethz.ch/...

OST

Terminology

«CERT»: Computer Emergency Response Team

- Trademark
- Imprecise

«CSIRT»: Computer Emergency Security Incident Response Team

- More precise
- Free to use

However, the terms CERT and CSIRT are used synonymously in daily life.

OST

Definition CSIRT

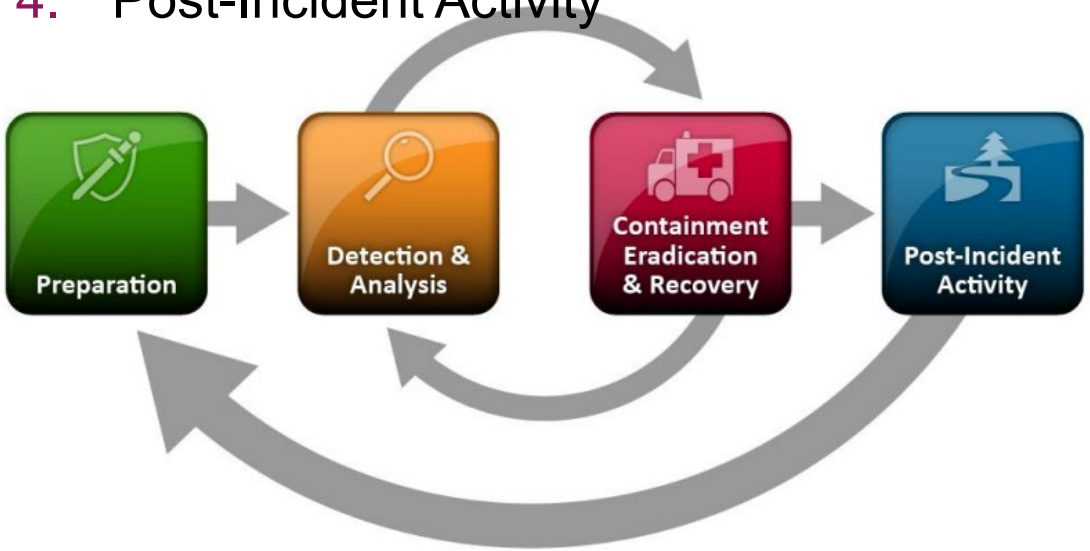
“A CSIRT is a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches.”

-- ENISA

Incident Response: Industry Standard Processes

NIST

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity



Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

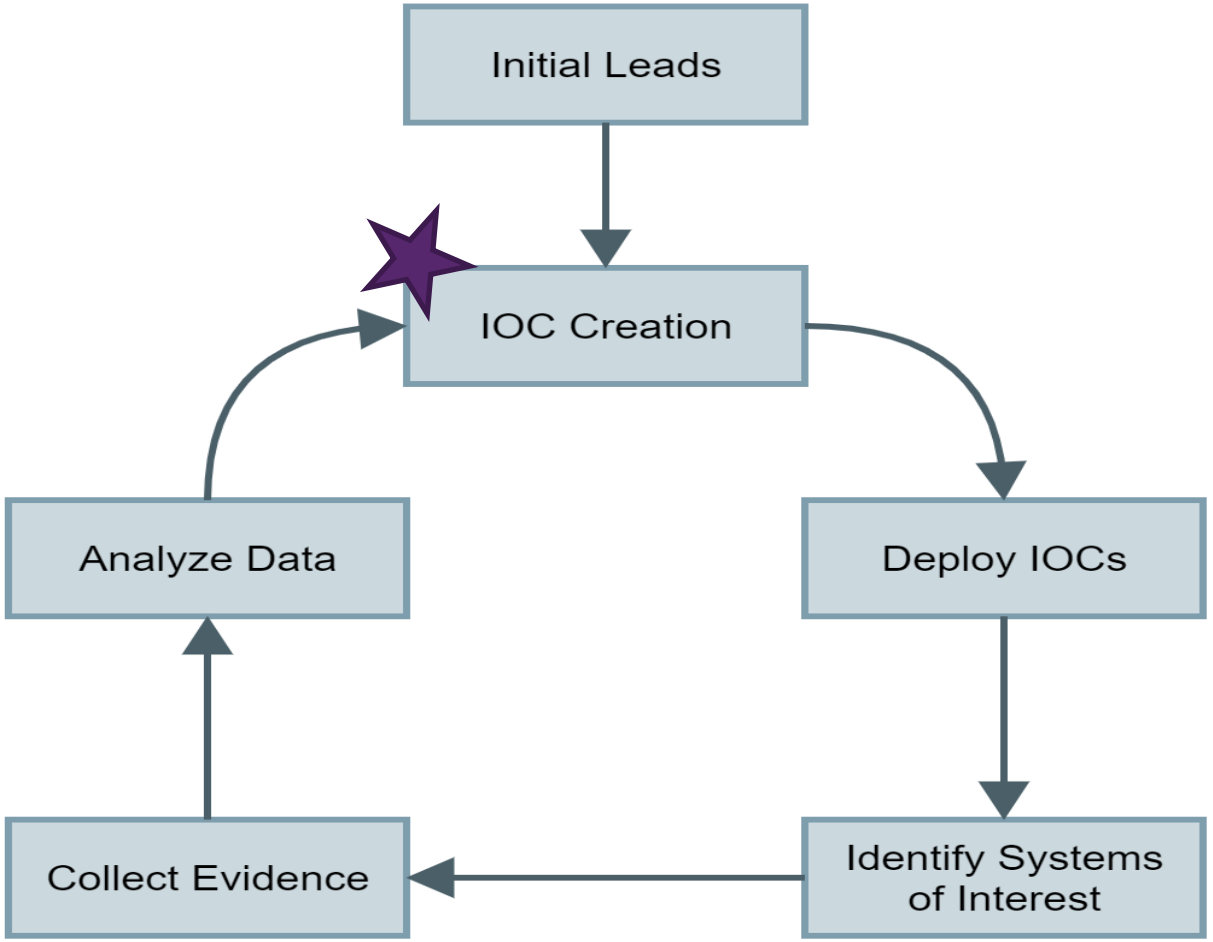
SANS

1. **P**reparation
2. **I**dentification and Scoping
3. **C**ontainment / Intelligence Development
4. **E**radication / Remediation
5. **R**ecovery
6. **L**essons Learned / Threat Intel Consumption

Source: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-3[illegible]

OST

Incident Response: Indicator of Compromize (IOC)



OST

Incident Response: Indices of Compromize (IOC)

IOC Creation

Indicators of Compromise (IOCs) define characteristics of an incident in a **structured manner**. They have the goal to describe, communicate and find artifacts related to incidents.

Format

- Host-based IOC formats (no formerly accepted standard yet):
  - YARA - http://virustotal.github.io/yara/
  - STIX, TAXII https://oasis-open.github.io/cti-documentation/ (formerly Mitre's CybOX)
  - Mandiant's OpenIOC - https://github.com/mandiant/OpenIOC_1.1, www.openioc.org
- Network-based IOC formats:
  - Snort rules https://www.snort.org/rules_explanation

OST