Hacknowledge

Security Monitoring Services

Swiss, Simple, Efficient

Microsoft Partner

Microsoft

01

Who we are

and what we do

ABOUT US

Simple, efficient, cost effective, all-inclusive solution to monitor and detect IT security threats More than just a SOC or a SIEM

Leverage your existing security solutions/devices

Shorten the time between breach & detection

Swiss made software and hosting

ISO 27001 certification

Luxemburg
Morges (HQ), Switzerland

Hacknowledge

OUR VALUES

Independent

Hacknowledge is an independent provider of enterprise security monitoring solution.

We do not re-sell any product or service.

Fair

We believe that security monitoring can be simple and cost-effective, we will leverage your existing security solutions and devices.

Effective

We focus on efficient, secure and reliable components. We do not (re)sell magic solutions, we will not make you un-hackable.

We will help your company identify IT security threat and shorten the time between breach & detection.

Agile

Hacknowledge develops, runs and operates its own software and hardware solution

OUR SERVICES

Cyber monitoring

Offensive security

Digital forensics

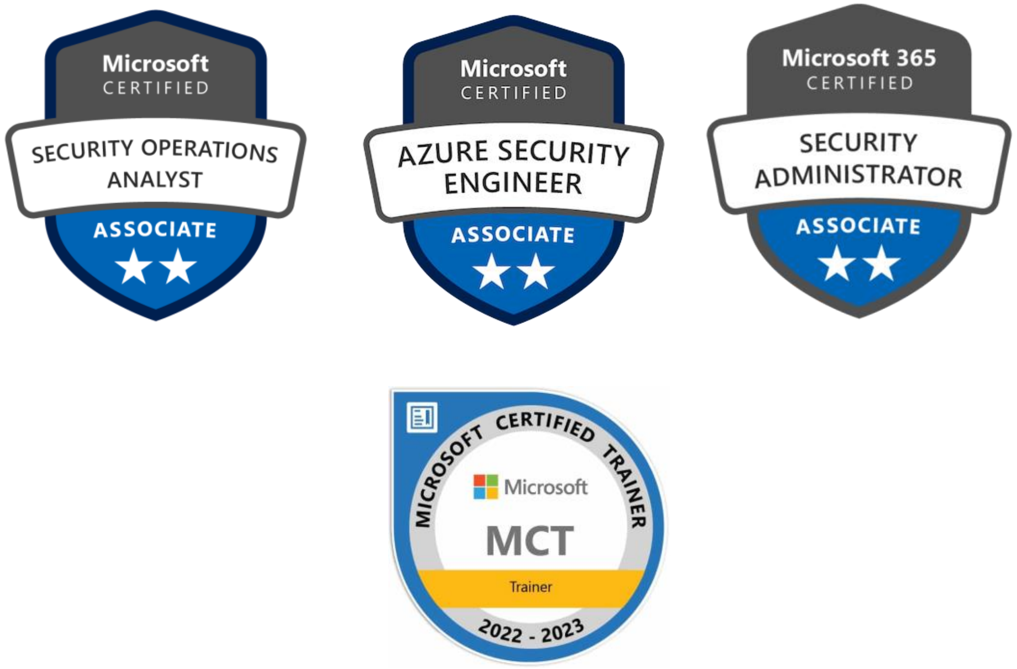
Security academy

MICROSOFT SECURITY SQUADRON

MSS SQUADRON

This is the Hacknowledge team with certified and experienced engineers who lead Microsoft Security project and Sentinel SOC deployments.

Gold
Microsoft Partner
Microsoft



02

Why do you need us?

High expertise and comprehensive tools

+100

The median number of days an organization was compromised in 2018 before the organization discovered the breach (or was notified about the breach)

Source: IBM 2020

CYBERSECURITY CHALLENGES

Expertise and staff

Each security appliance needs its own security expert to manage it properly

Budget

(Unfortunately) you do have a limited budget

A needle in a haystack

You probably realize that analysing your logs to identify security threat is as close as finding a needle in a haystack

Day to day

You probably do not have the time to pro-actively exploit the existing logs that you may already have

Leverage the existing

You may already have invested a lot in IT security… so you should leverage the existing

Share/monitor/info feed

You have to adapt your defence to the threats targeting your organisation… but those threats may be difficult to identify

03

Our solution

Introduction and benefits

Hacknowledge concept

All in one service to help your team focus on actionable events

FROM NOISE to RELEVANT THREATS

Logs

An SME with 200 event sources (PC, servers, etc.) can produce around **43 millions logs per day**

Events

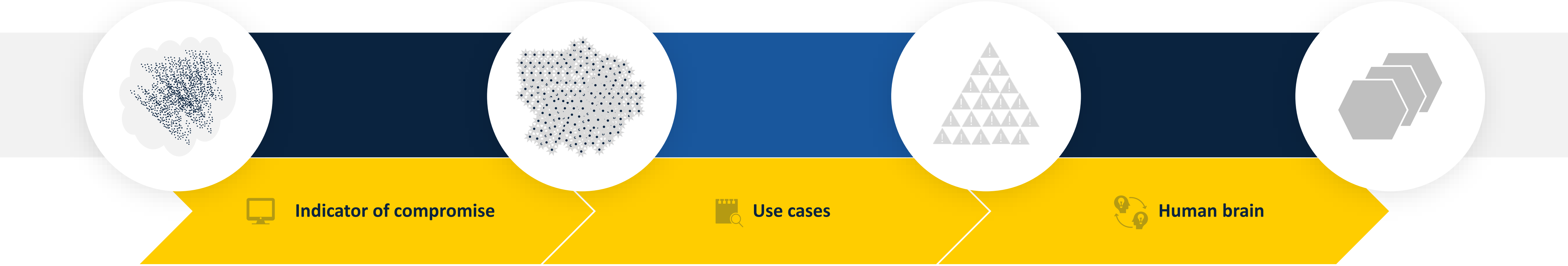
We select the relevant logs to reduce that number to **a few thousands of events per day**

Alerts

We aggregate the events to identify suspicious phenomena, and reduce the noise to **less than hundred alerts per month**

Incidents

Our security engineers qualify the alerts in order to report you only the most relevant incidents limited to a **few units per month** (but as much as required…)



Indicator of compromise

Use cases

Human brain

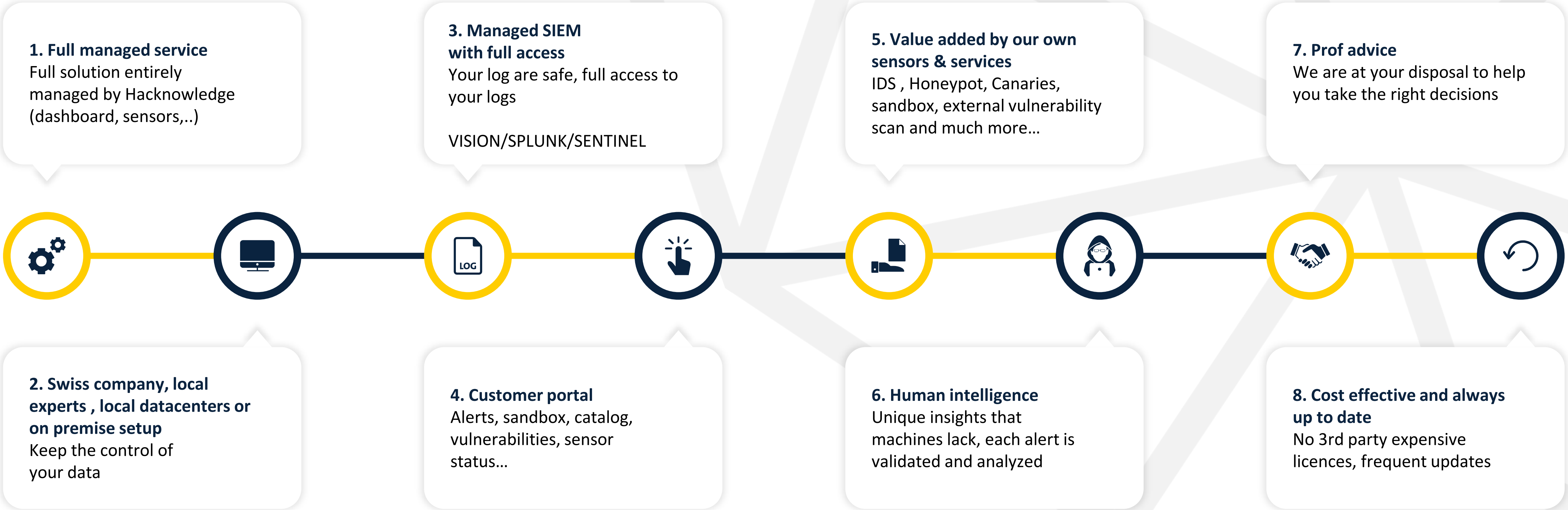
WE AIM AT

- Generating strong signals
- By better exploiting your logs and those generated by our sensors
- Covering your on promise or cloud based services
- Leveraging the use of your existing devices
- While monitoring threats targeting your company

YOU ARE BUYING

- Qualified and actionable alerts
- Visibility through dashboard and reports
- Access to expertise
- Full managed service
- Access to various solutions and features: IDS, vulnerability management, sandbox, awareness, pen-testing, honeypots, etc.

HACKNOWLEDGE SOC FEATURES



1. Full managed service
Full solution entirely managed by Hacknowledge (dashboard, sensors,..)

2. Swiss company, local experts , local datacenters or on premise setup
Keep the control of your data

3. Managed SIEM with full access
Your log are safe, full access to your logs

VISION/SPLUNK/SENTINEL

4. Customer portal
Alerts, sandbox, catalog, vulnerabilities, sensor status…

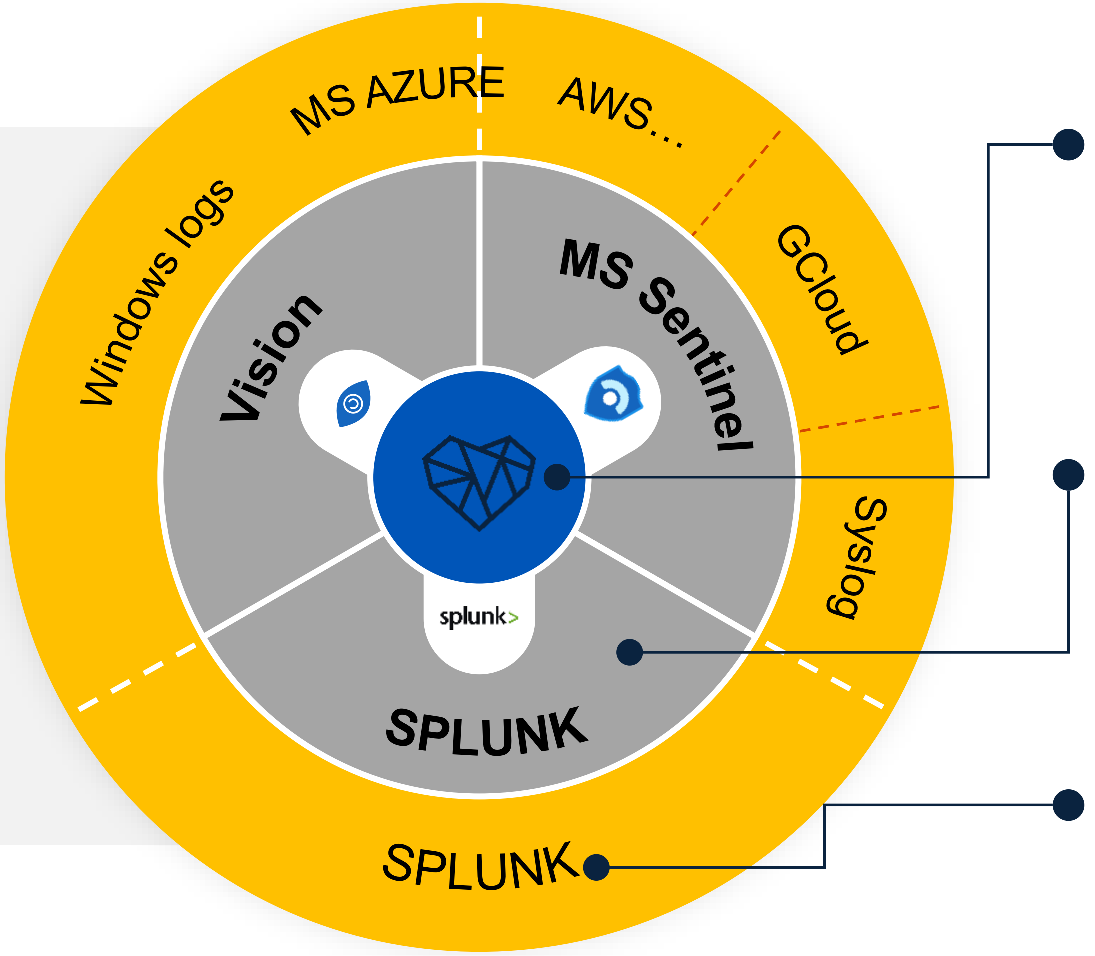
5. Value added by our own sensors & services
IDS , Honeypot, Canaries, sandbox, external vulnerability scan and much more…

6. Human intelligence
Unique insights that machines lack, each alert is validated and analyzed

7. Prof advice
We are at your disposal to help you take the right decisions

8. Cost effective and always up to date
No 3rd party expensive licences, frequent updates

VARIOUS SET-UP POSSIBLE



SOC HK

SIEM

Log collector

HOW WE DO IT

Our sensors

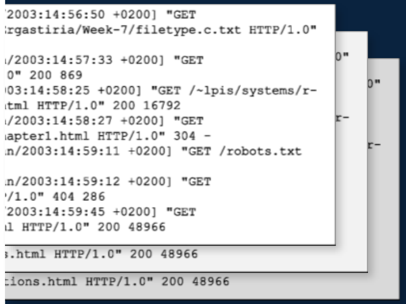
As many as needed to increase granuarity and enhance detection capabilities

Several features

Passive devices

Managed by Hacknowledge

Updated every day



```
2003:14:56:50 +0200] "GET
rgastiria/Week-7/filetype.c.txt HTTP/1.0"

/2003:14:57:33 +0200] "GET
0" 200 869
03:14:58:25 +0200] "GET /~lpis/systems/r-
tml HTTP/1.0" 200 16792
/2003:14:58:27 +0200] "GET
apter1.html HTTP/1.0" 304 -
n/2003:14:59:11 +0200] "GET /robots.txt

n/2003:14:59:12 +0200] "GET
/1.0" 404 286
2003:14:59:45 +0200] "GET
l HTTP/1.0" 200 48966
s.html HTTP/1.0" 200 48966
tions.html HTTP/1.0" 200 48966
```

Your logs and devices

To decrease the likeliness of false positives

Exploit the full audit trail

Leverage the use of your existing device/solutions

Detect lateral movements

Correlation

Better detection

SENSORS COMPONENTS

Our Sensors

- Custom development
- Optimized
- Hardware or virtual
- Managed by Hacknowledge
- Many interfaces

Sensor’s characteristic

- 4 x SFP+ 10 Gbs interfaces
- 6x 1Gbs copper interfaces
- 8 cores processors
- 16G Ram-Disk (all logs are cached and managed in RAM to extend SSD life)

CITRIX XenServer

Microsoft

vmware

KVM

Log collector

- Push / Fetch
- Cache and filter
- Local correlation
- Enrichment and tech partnerships

IDS

- Span , tap , rspan
- Managed by Hacknowledge
- Different feeds
- CIRCL, FIRST, Commercial, Gov...

Honeypots

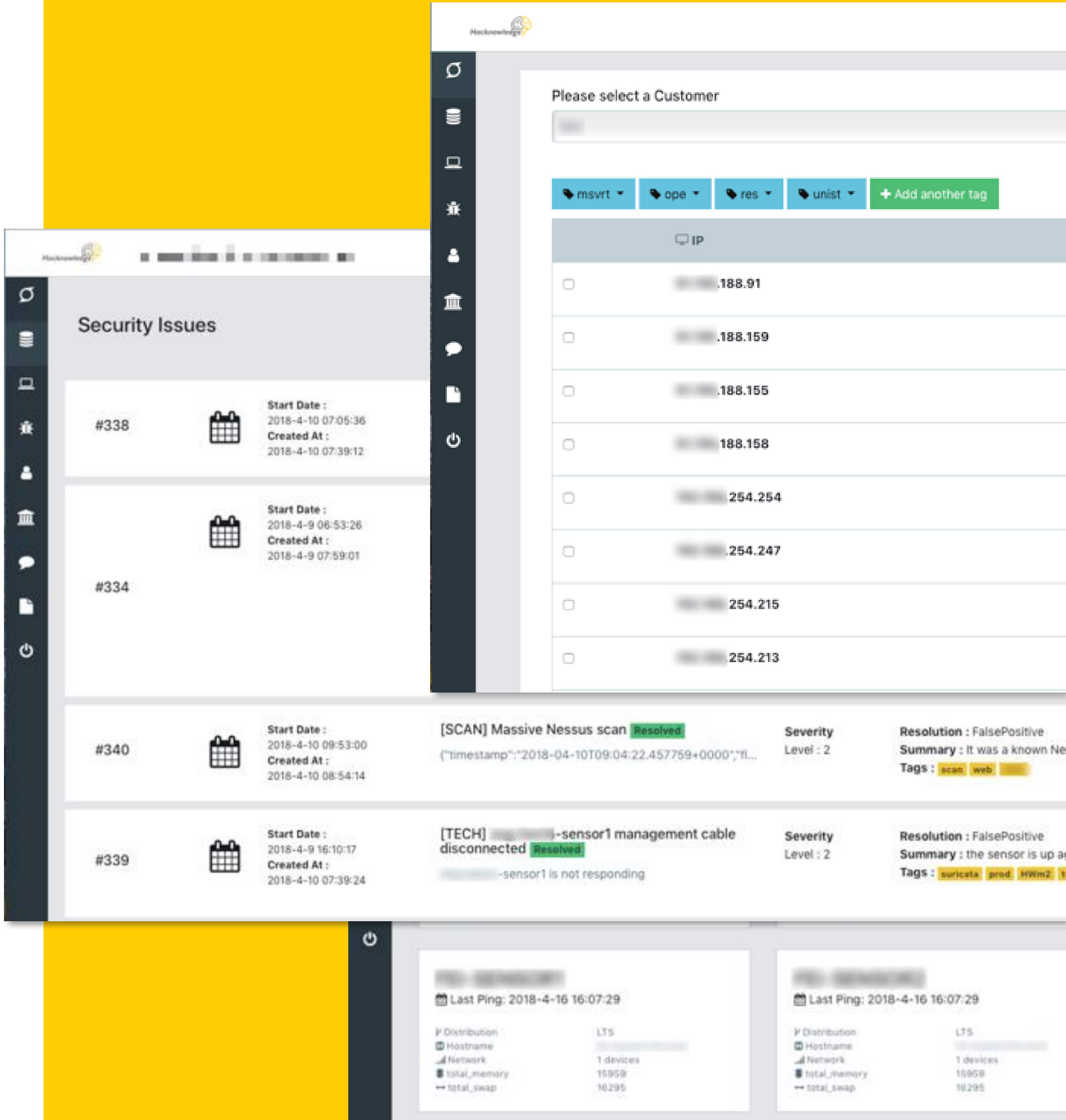
- As many as needed
- Low or high interaction
- Different services : file, web, VOIP, DB,..

Vulnerability scanning

- Launched from sensor
- Provides you with visibility
- Helps to prioritize and understand alerts

CUSTOMER PORTAL

- All security alerts and status
- Sensors status and characteristics
- Discovered vulnerabilities on systems with tag and severity filter
- Access to a sandbox for files and URL analysis
- Portal users creation and management
- Secure file exchange environment
- … and many more



Please select a Customer

□	IP
□	[redacted].188.91
□	[redacted].188.159
□	[redacted].188.155
□	[redacted].188.158
□	[redacted].254.254
□	[redacted].254.247
□	[redacted].254.215
□	[redacted].254.213

Security Issues

#338
Start Date : 2018-4-10 07:05:36
Created At : 2018-4-10 07:39:12

#334
Start Date : 2018-4-9 06:53:26
Created At : 2018-4-9 07:59:01

#340
Start Date : 2018-4-10 09:53:00
Created At : 2018-4-10 08:54:14
[SCAN] Massive Nessus scan Resolved
{"timestamp":"2018-04-10T09:04:22.457759+0000","fl...
Severity Level : 2
Resolution : FalsePositive
Summary : It was a known Ne
Tags : scan web [redacted]

#339
Start Date : 2018-4-9 16:10:17
Created At : 2018-4-10 07:39:24
[TECH] [redacted]-sensor1 management cable disconnected Resolved
[redacted]-sensor1 is not responding
Severity Level : 2
Resolution : FalsePositive
Summary : the sensor is up a
Tags : suricata prod HWm2

[redacted]
Last Ping: 2018-4-16 16:07:29
Distribution LTS
Hostname [redacted]
Network 1 devices
total_memory 15959
total_swap 16295

[redacted]
Last Ping: 2018-4-16 16:07:29
Distribution LTS
Hostname [redacted]
Network 1 devices
total_memory 15959
total_swap 16295

RECURRENT REPORTING

Executive
Summary

Hacknowledge Proposal

Page [illegible] of 30

Executive summary

AUGUST
Report – sample

Latest period summary

Executive summary

This reports covers the period 01-08-2016 to 31-08-2016. No major critical alert has been raised during this last period; several low severity alerts were raised and have been correctly addressed by CUSTOMER security and network teams; several security vulnerabilities should be fixed as soon as possible.

We consider the overall security level as good

AUGUST

LEVEL: GOOD (7/10)
We have not identified any critical problem; A possible brute-force attack has been identified, we consider the overall security level as good

EXPOSURE: GOOD (7/10)
No critical company data found on the Internet.
A twitter message has been identified as a potential threat for the company.
Several employees are using their professional email addresses for personal purposes.

4 ALERTS
Low: Unknown VPN generating too many useless logs (configuration problem)
Low: Possible brute force (password lost by one of your users)
Medium: 2 workstations infected by a malware (problem solved)
Low: Download of a hacking tool (source identified)

10 VULNERABILITIES
Vulnerability scan has reported 10 different vulnerabilities affecting the following components:
- vmware server (patch missing)
- Oracle servers
- Windows server 2003

Hacknowledge Proposal

Page 5 of 30

Vulnerabilities & priorities

Technical report

Sensors status

All sensors are running fine.

We do not see any overload or disk problem.

Alerts for the last period 1/08/16 to 31/08/16

●●○○
Virus & malwares: communication with known C&C server

What: During the latest period, 2 of your workstations have initiated connection with known C&C servers (y.y.y.y & z.z.z.z); security team has been alerted and has reinstalled those workstation. We consider the problem has solved.

When: 15th of August 2016, 16h36 GMT+1

How many: 2

How often: 1

Impacted systems: workstationA (x.x.x.x), workstationB (x.x.x.x)

Possible solutions: It would be interesting to have the possibility to correlate the network antivirus log (vendorA) with the antivirus logs (vendorB), the use a sandboxing solution would also lower this risk

Data:

Hacknowledge Proposal

Page 7 of 30

Exposure on the internet

●●○○
VPN Ipsec: numerous Phase1 errors

What: DeviceA & DeviceB firewall-vendor devices are generating a lot of phase-1 VPN ipsec errors trying to establish a VPN with 3 specific IP addresses that seems to belong to Oracle. Customer has been notified and was not aware of those VPN

How many: 157 820/msg per day

How often: every day

Impacted systems: DeviceA & DeviceB

Possible solutions: Customer is investigation the need of those VPN. Meanwhile, those message will not be sent by our sensors anymore

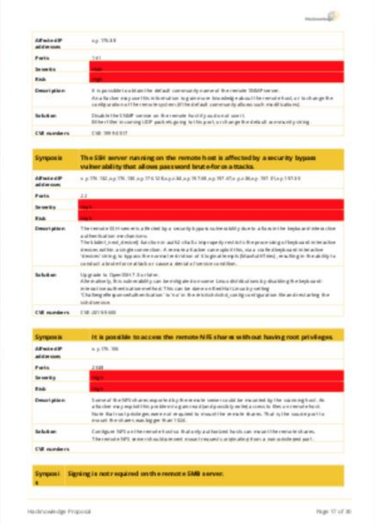
Data:

Quick Values for remip

Hacknowledge Proposal

Page 8 of 30

Relevant security news



Affected IP addresses	x.y.176.3.8
Ports	161
Severity	High
Risk	High
Description	It is possible to obtain the default community name of the remote SNMP server. [illegible]
Solution	Disable the SNMP service on the remote host if you do not use it. [illegible]
CVE numbers	CVE-1999-0517

Synopsis	The SSH server running on the remote host is affected by a security bypass vulnerability that allows password brute-force attacks.
Affected IP addresses	[illegible]
Ports	22
Severity	High
Risk	High
Description	[illegible]
Solution	Upgrade to OpenSSH 7.0 or later. [illegible]
CVE numbers	CVE-2015-5600

Synopsis	It is possible to access the remote NFS shares without having root privileges.
Affected IP addresses	x.y.176.186
Ports	2049
Severity	High
Risk	High
Description	[illegible]
Solution	Configure NFS on the remote host so that only authorized hosts can mount the remote shares. [illegible]
CVE numbers	

Synopsis	Signing is not required on the remote SMB server.

Hacknowledge Proposal

Page 17 of 30

And more

OTHER **FEATURES**

OTHER FEATURES AND SERVICES

01 Keyword monitoring (threat intel)

02 Canaries

03 Sandbox

04 Managed EDR

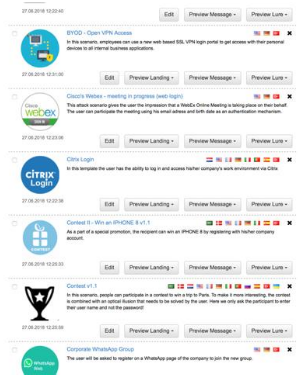
05 Vulnerability management

06 Pentesting

07 Phishing tests

08 User awareness content & sessions

09 Incident response



27.06.2018 12:22:40

BYOD - Open VPN Access

In this scenario, employees can use a new web based SSL VPN login portal to get access with their personal devices to all internal business applications.

27.06.2018 12:31:00

Cisco's Webex - meeting in progress (web login)

This attack scenario gives the user the impression that a WebEx Online Meeting is taking place on their behalf. The user can participate the meeting using his email adress and birth date as an authentication mechanism.

27.06.2018 12:23:06

Citrix Login

In this template the user has the ability to log in and access his/her company's work environment via Citrix

27.06.2018 12:22:38

Contest II - Win an IPHONE 8 v1.1

As a part of a special promotion, the recipient can win an IPHONE 8 by registering with his/her company account.

27.06.2018 12:25:33

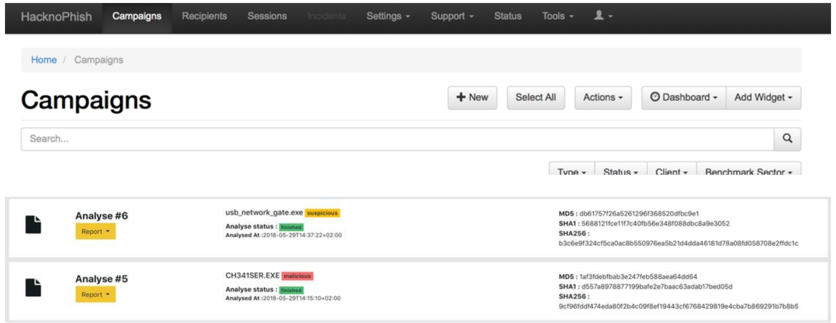
Contest v1.1

In this scenario, people can participate in a contest to win a trip to Paris. To make it more interesting, the contest is combined with an optical illusion that needs to be solved by the user. Here we only ask the participant to enter their user name and not the password!

27.06.2018 12:25:59

Corporate WhatsApp Group

The user will be asked to register on a WhatsApp page of the company to join the new group.



Campaigns

Analyse #6

usb_network_gate.exe suspicious
Analyse status : finished
Analysed At :2018-05-29T14:37:22+02:00

MD5 : db61757f26a5261296f368520dfbc9e1
SHA1 : 5688121fce11f7c40fb56e348f088dbc8a9e3052
SHA256 :
b3c6e9f324cf5ca0ac8b550976ea5b21d4dda46181d78a08fd058708e2ffdc1c

Analyse #5

CH341SER.EXE malicious
Analyse status : finished
Analysed At :2018-05-29T14:15:10+02:00

MD5 : 1af3fdebfbab3e247feb588aea64dd64
SHA1 : d557a8978877199bafe2e7baac63adab17bed05d
SHA256 :
9cf96fddf474eda80f2b4c09f8ef19443cf6768429819e4cba7b869291b7b8b5

04

Pricing

and options

PRICING MODEL

CAPEX

Setup - One time fee

OPEX

Yearly fee including everything

SIMPLE

+

PREDICTABLE

Thank you!
Questions?

(See you soon)

Hacknowledge

Hacknowledge SA
Rue de Lausanne 35A
1110 Morges
Switzerland
+41 21 519 05 01

Hacknowledge Lux SA
9 Rue du Laboratoire
1911 Luxembourg
Luxembourg
+352 20 30 15 86

hacknowledge.com