Smart probes at the center of your cybersecurity operations: concrete cases and feedbacks
Intro.

Smart probes: the best answer to a fast-changing environment
Smart probes at the center of your cybersecurity operations

• **Massive digital and IT transformations** (cloud technology, more and more threats at a worldwide scale...),

• Cybersecurity has become a **key issue** for all types of organizations,

• The needs for **efficient detection solutions** is growing fast,

• Passive smart probes are **easy to install** and can **monitor the whole Information System**.
Part 1.
Smart probes: smart and secure
An innovative detection to ensure optimal protection

<table>
<thead>
<tr>
<th>Innovations on information capture</th>
<th>Innovations on analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGFLOW feature</td>
<td>CODEBREAKER feature</td>
</tr>
<tr>
<td>Capturing information to track threats with a farsighted technology.</td>
<td>Real-time files analyses with 16 engines.</td>
</tr>
<tr>
<td>Retro-analysis of suspicious files.</td>
<td></td>
</tr>
<tr>
<td>MALCORE feature</td>
<td>RETROACT feature</td>
</tr>
<tr>
<td>Understanding attacks in real-time with a high and unrivalled analysis level. Maintaining a high level of pressure on suspects.</td>
<td></td>
</tr>
</tbody>
</table>
Advanced persistent threats (APT) detection

Discovery

Initial breach

Persistence and final phase

**CODEBREAKER**
Shellcodes, ROPchains...

**MALCORE + RETROACT**
Malwares

**SIGFLOW**
Network traffic and payloads
Part 2.
Smart probes integration in a restricted environment
How do smart probes integrate in a restricted environment?
How do smart probes integrate in a restricted environment?
Key issues on smart probes integration in a restricted environment

Smart probes integration in a restricted environment (Security Incident Detection Service Providers) is a way to deeply think about intrusion detection and all related topics.

**Top 3 elements are:**

1. Logs and storage issues
2. Roles and networks isolation
3. Probes access and supervision
1. Logs and storage issues

→ **How many probes** can a management appliance deal with?
→ **For how long** can information can be stored?
→ **How many logs** can be stored?
→ …

All these questions **might be raised** before the integration.
But can be difficult to answer… **for many reasons**:

→ **Lack of information** on bandwidth
→ **No forseeing on network flows classification** (web requests, DNS, files server…)
→ **How to determine storage duration** without this information?
→ …
1. Logs and storage issues

Probes and the management appliance can adjust quickly to all types of situations. They can be configured to have more or less logs if needed.
1. Logs and storage issues

In intrusion detection, storage figures can quickly become exponential!

Some elements need to be taken into account:
→ Is there a SIEM (Security Information and Event Management)?
→ Is it relevant to store information locally?
→ Is it relevant to store everything? Alerts only? All metadata?

1 probe with an average 100Mbps traffic = 1GB to 150GB of metadata/day
1 probe with a 10Gbps traffic = 100GB to 15TB of metadata/day
2. Roles and networks isolation

Restricted environments inflict a strict access management and networks separation. The used term is **dedicated administration network**. Feedbacks on the French Military Planning Act restrictions implementation.

- **Operator**: consults alerts, IOC search, forensics
- **System Administrator**: creates roles, manages rights, configures probes and management appliance
- **Local Administrator**: consults alerts and system logs, enables/disables information feedbacks
- **Auditor**: consults alerts, consults probes logs
2. Roles and networks isolation

The operator: can consult alerts, configure other signatures...
2. Roles and networks isolation

The local administrator: can configure some probes’ options

The auditor: can consult logs.
3. Probes access and supervision

The system administrator must ensure everything is operational.
3. Probes access and supervision

Probes access in a restricted environment needs to be strictly monitored.

→ The operators management interface is physically separated from the others,
→ Double authentication with certificate,
→ Users login historic,
→ Strengthened administrators and operators actions tracking.
Thanks for your attention!

Any questions?