Redefine Digital Forensic and Incident Response
Let’s set the scene
François Khourbiga

CEO and Co-Founder of Defants
**Top Trends in Cybersecurity, 2022**

<table>
<thead>
<tr>
<th></th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Attack surface expansion</td>
</tr>
<tr>
<td>02</td>
<td>Identity system defense</td>
</tr>
<tr>
<td>03</td>
<td>Digital supply chain risk</td>
</tr>
<tr>
<td>04</td>
<td>Vendor consolidation</td>
</tr>
<tr>
<td>05</td>
<td>Cybersecurity mesh</td>
</tr>
<tr>
<td>06</td>
<td>Distributed decisions</td>
</tr>
<tr>
<td>07</td>
<td>Beyond awareness</td>
</tr>
</tbody>
</table>

Source: Gartner
© 2022 Gartner, Inc. All rights reserved. PL_154850
DOOR?

OH YOU MEAN A KICKING BOARD
Une cyberattaque hors norme frappe la Suisse, touchant l’armée et de nombreuses polices

Plusieurs polices cantonales, l’armée, mais aussi les douanes et l’Office fédéral de la police (Fedpol), sont concernés par le piratage de la société informatique alémanique Xplain. Cette attaque montre la vulnérabilité des prestataires IT.

UK Electoral Commission targeted by 'complex cyber-attack'

Electoral Commission says ‘hostile actors’ had first accessed its systems in August 2021

Futurs, High-tech

Strasbourg : un groupe hospitalier touché par une cyberattaque

La prise en charge des patients est maintenue, mais elle risque d’être plus longue en raison de la panne informatique causée par l’attaque.
“There needs to be a change in how #DFIR is done.”

Harlan Carvey, Senior Incident Responder, R&D
Today, Digital Forensic and Incident Response
Respond to incident

Investigating and responding to cyber incidents
Data collection

Copy of **hard drive** and **memory dump**
Tooling

Fragmented tools with non-native interaction
Shortage of skills

2/3 of organizations find challenging to respond to an incident
Incident Response Lifecycle
From response to anticipation
Triage & Collection

Leverage the Pareto’s Law
No-Code With Collection Processing Automation
Automation

Time saving at scale for tedious tasks
Goes **Beyond** the State-of-the-Art
Collaboration

Share the **same process** to include junior under the senior’s supervision.
From incident response
to incident anticipation
Incident Response

Threat Hunting

Proactive Backup Audit

Reactive Backup Audit

DFIR Cyber Range

Compromise Assessment
Drive DFIR to Security Operations
Modern SOC for End-Users

- Enhanced security posture
- Time saving
- Cost saving
- Access to the expertise
- Enhanced security posture
Modern SOC for MSSP

- Larger market including SMEs
- Investment Optimization
- Load balancing
- Customers included in the project
Agile and Sovereign

Multi-domain

SecNumCloud
Drive DFIR to Security Operations
From 2 days to **15 minutes** for expert and junior
How would you rate the level of native automation of your DFIR tools?

On average, how long does it take to find suspicious items with your tools?

How long does it take to start an investigation (from accessing necessary tools to collect to the first hit)?

How many DFIR tools do you possess and can use to respond to an incident (excluding EDR)?

How would you rate your tools’ level of native integration with your EDR?

How would you rate the support quality of these tools (usability, bug fix, release, client support)?

With Defants
Delivering report up to 2x faster
On average, how long does it take to resolve an incident?

How would you rate the ease to put in place an efficient strategy for your incident response with your existing tools?

On average, how many investigations are you currently able to carry out per year?

How would you rate the ease to follow the progress of your colleagues during an incident response?

How challenging and time-intensive is the task of converting analysts' work into a comprehensive report?

Process
MTTR and MTTC divided by 3 with load balancing and follow-the-sun
On average, what level of education do your incident response analysts have?

On average, how many years' experience do they have in DFIR?

On average, how long does training take for your analysts to be fully autonomous on your tools?

On average, how many people do you assign at most to an incident response?
Thank you for your attention

Contact us at anytime

bonjour@defants.com