





Redefine Digital Forensic and Incident Response

Let's set the scene



François Khourbiga

CEO and Co-Founder of Defants



Orange
Cyberdefense

MANDIANT



Top Trends in Cybersecurity, 2022

01



Attack surface
expansion

02



Identity system
defense

03



Digital supply
chain risk

04



Vendor
consolidation

05



Cybersecurity
mesh

06



Distributed
decisions

07



Beyond
awareness

[gartner.com](https://www.gartner.com)

Source: Gartner
© 2022 Gartner, Inc. All rights reserved. PR_1764850

Gartner.



McKinsey
& Company








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



September 07, 2023
9:40 PM
Jeff Seldin

Ukraine, US Intelligence Suggest Russia Cyber Efforts Evolving, Growing

Share
  





EUROPE

UK Electoral Commission targeted by 'complex cyber-attack'

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

Burak Bir | 08.08.2023 - Update : 08.08.2023



World

China sends

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**

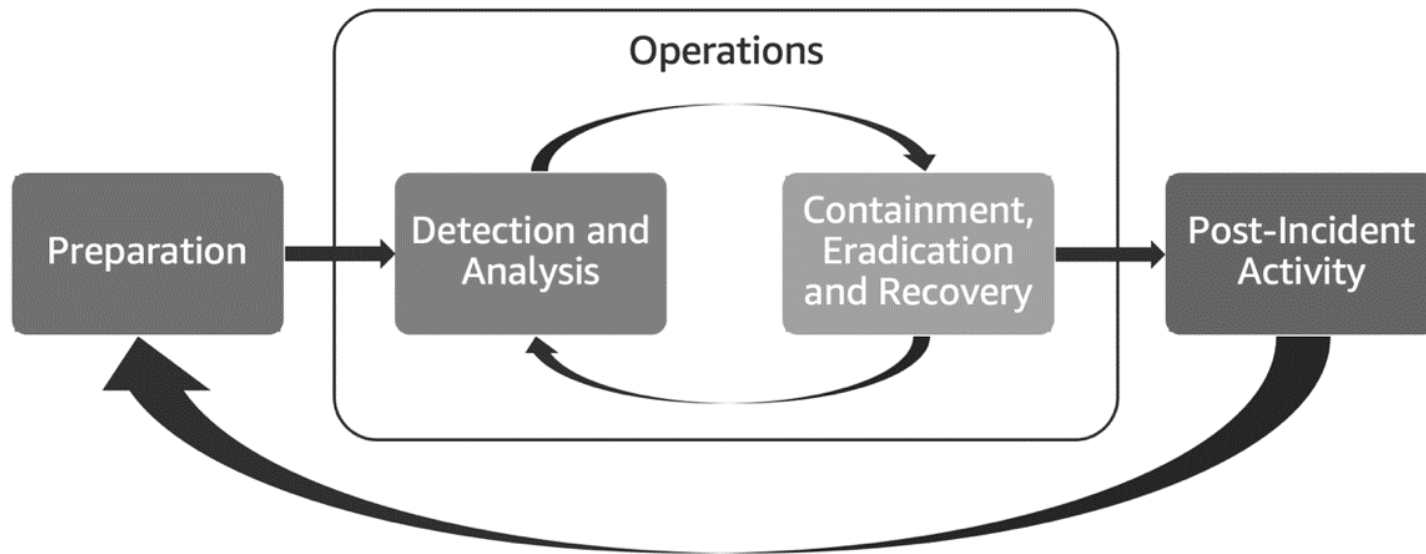


Shortage of skills

**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



KROLL



UNIX®
Unix-like Artifacts Collector (UAC)





Automation

**Time saving at scale for
tedious tasks**

Goes **Beyond** the State-of-the-Art

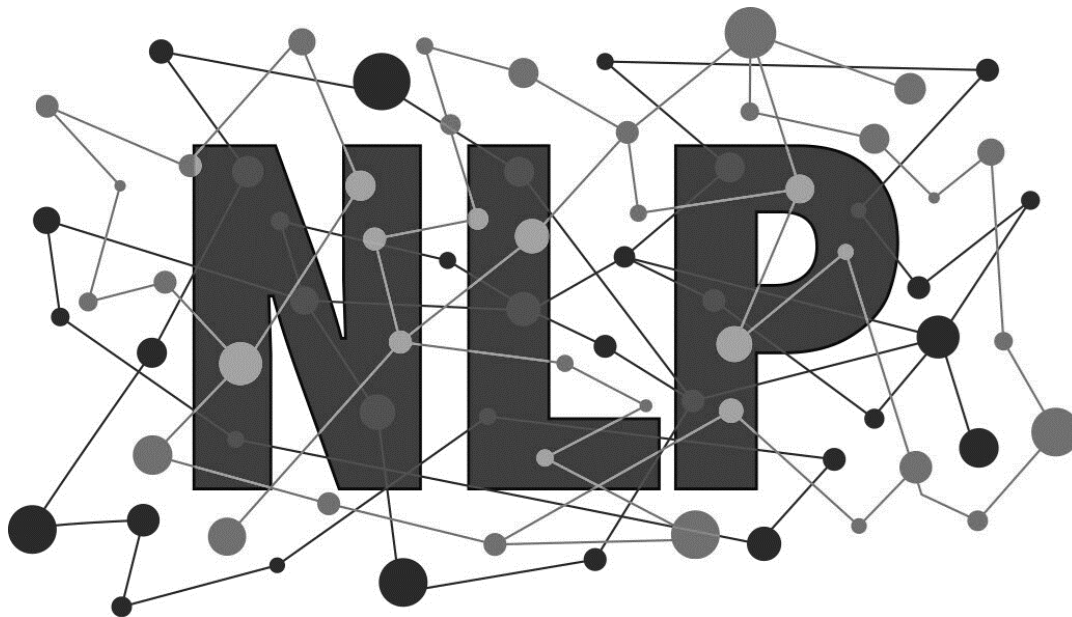




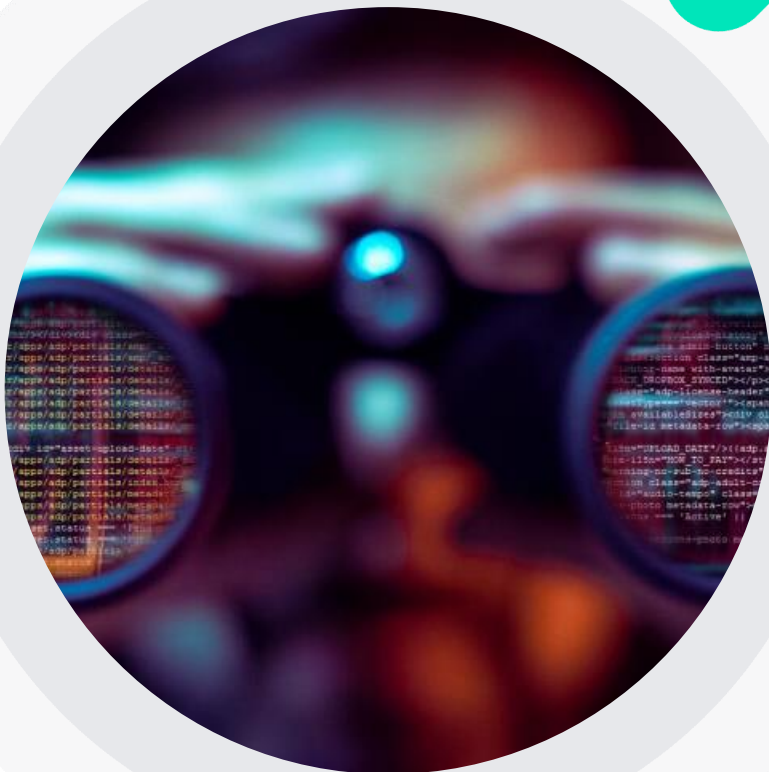
Collaboration

Share the **same process** to
include junior under the
senior's supervision

Shared Methodology Consistency and Quality



From incident response to incident anticipation



**Incident
Response**

Reactive Backup Audit

**DFIR
Cyber Range**

**Compromise
Assessment**

**Threat
Hunting**

**Proactive Backup
Audit**

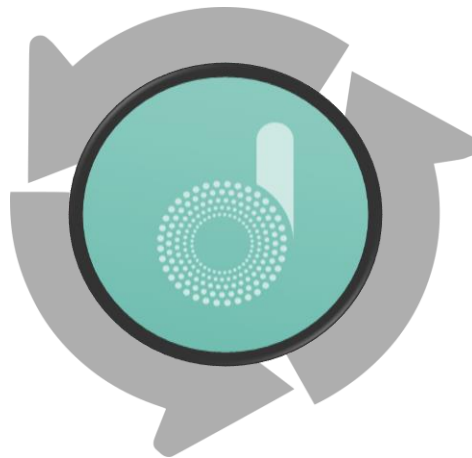
Drive DFIR to Security Operations

Modern SOC for End-Users

Enhanced security posture



Cost saving



Time saving



Access to the expertise



Enhanced security posture



Modern SOC for MSSP

Larger market
including SMEs



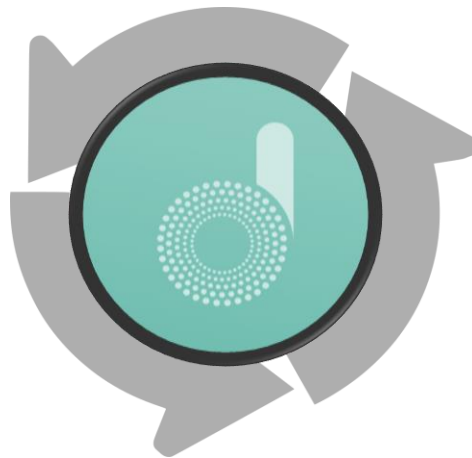
Investment
Optimization



Load balancing



Customers
included in the
project



Agile and Sovereign

Multi-domain



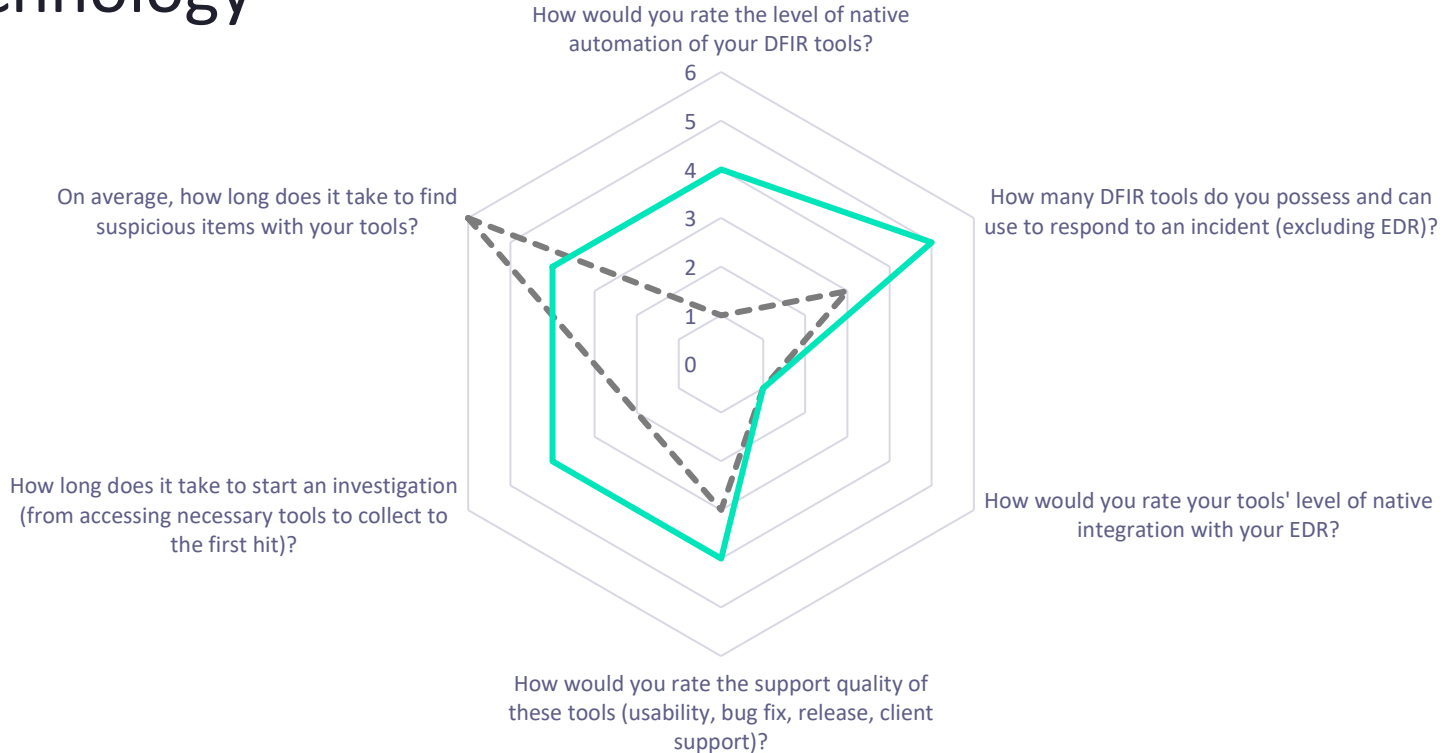
SecNumCloud



Drive DFIR to Security Operations

From 2 days to **15**
minutes
for expert and
junior

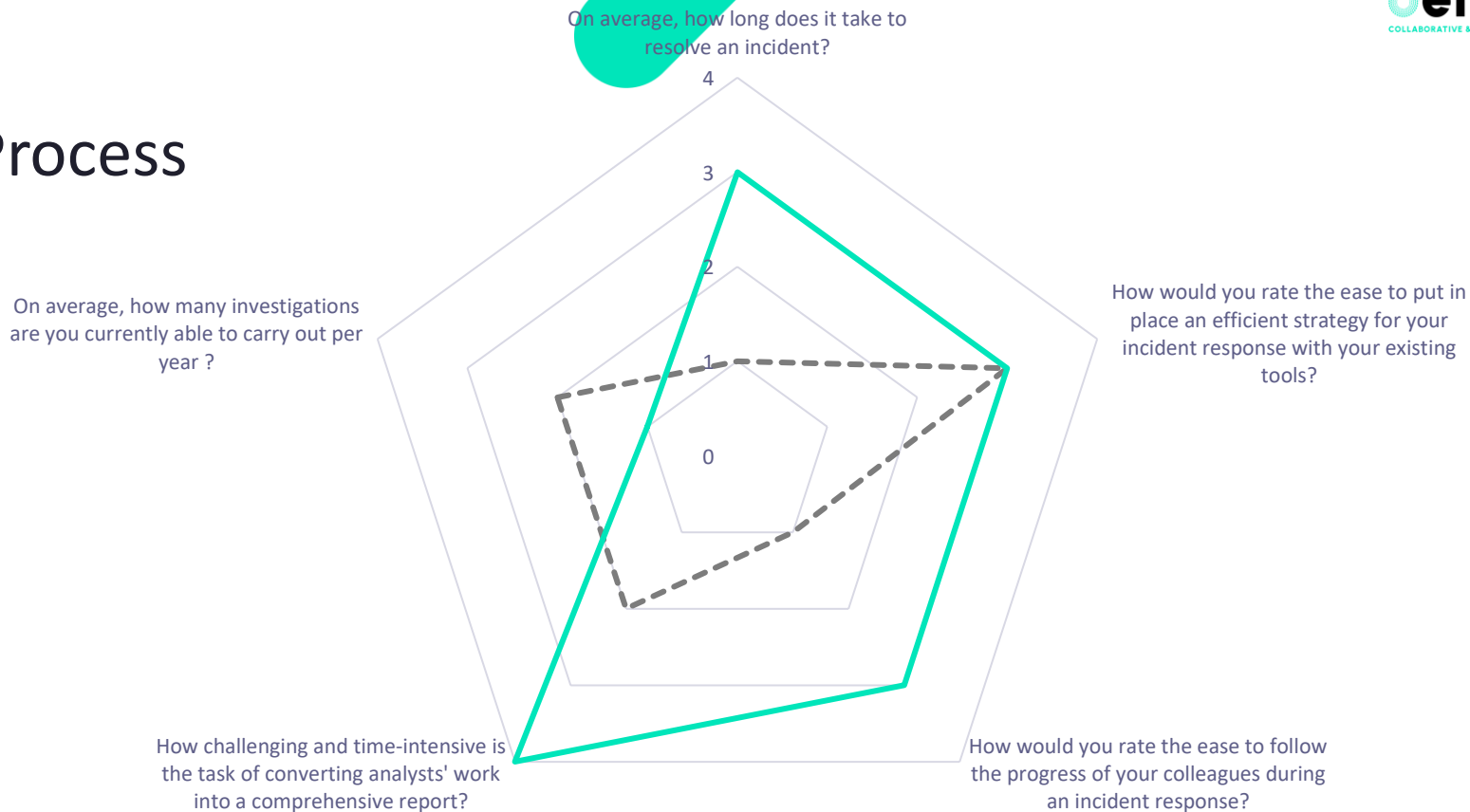
Technology




**Delivering report
up to **2x faster****

Process

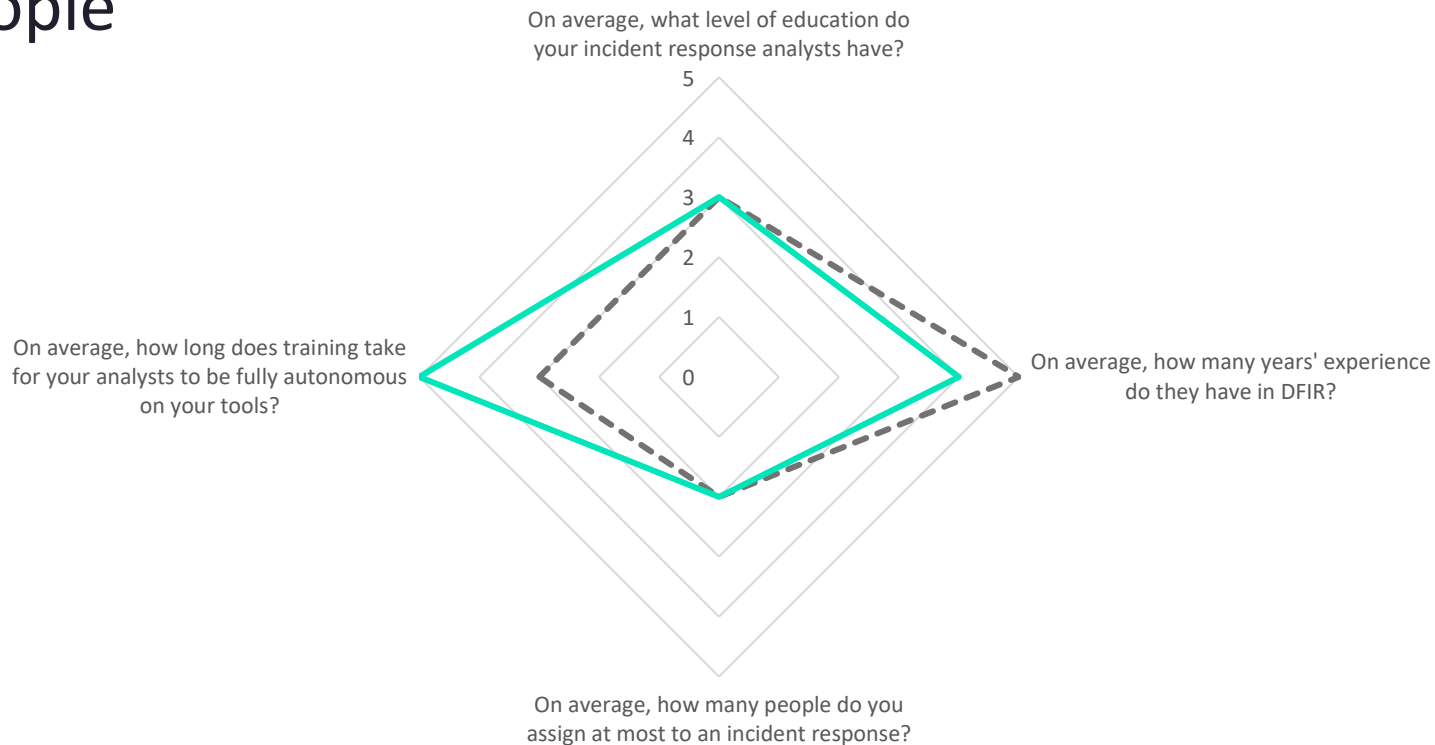
— With Defants





MTTR and MTTC
divided by 3 with
load balancing and
follow-the-sun

People



Thank you for your attention

Contact us at anytime

bonjour@defants.com