NAVIGATING THE INCIDENT RESPONSE JOURNEY WITH HWG SABABA



HWG Sababa

HWG Sababa's SOC

24×7 monitoring, incident detection and response, intelligence and threat hunting

Team of more than 70 certified cybersecurity analysts organized in 3 levels

Millions of security events analyzed each month, 3500 cases investigated and 500 incidents resolved

100+ Incident Response projects over the past 4 years

Given the rise in global cyber threats, with **attacks up by 12%**[1] in 2023 and **dwell time down to just 8 days**[2], companies face mounting pressure to respond quickly to cyber emergencies. These emergencies present them with a unique set of challenges, including **the rapid escalation of incidents**, the complexities of **identifying and neutralising threats**, the imperative to **minimise downtime** and **operational disruptions**, and the potential for **substantial financial losses**. Moreover, the evolving nature of cyber threats demands a c**omprehensive understanding of emerging attack vectors** and **proactive measures to fortify defences**, which may exceed the capabilities of in-house teams.

In addition to the technical obstacles, enterprises must navigate **the human dimension of cyber incidents**, which can significantly impact response effectiveness and organisational resilience. Indeed, the rapid unfolding of attacks and the potential consequences of a breach can induce **heightened stress, pressure**, and **uncertainty**, impairing decision-making and intensifying the sense of urgency.



This scenario mirrors the experience of a **global enterprise**, with **numerous commercial offices** and **production facilities** across **3 continents**, along with a dedicated workforce **exceeding 5000** employees. Amidst the chaos of a cyber-attack, the company encountered major obstacles. With **daily losses soaring to € 3 million**, its capability to provide services to a **worldwide clientele of over 700 customers** was seriously compromised. Indeed, business operations were abruptly disrupted, affecting nearly all departments for several days.

Faced with the looming threat to its esteemed reputation and a shortfall in the expertise required to navigate the crisis effectively, **the company turned to HWG Sababa for assistance**. From **formulating and executing a comprehensive crisis management strategy** - including communication protocols and incident response procedures - to **implementing technical measures** to limit the damage, HWG Sababa ensured a coordinated and effective response, while also addressing the **human aspects of the emergency**. Their involvement was pivotal in empowering the organisation to handle the difficulties with confidence and resilience.

HWG Sababa

[1]Clusit Report 2024

[2]2023 Active Adversary Report for Tech Leaders

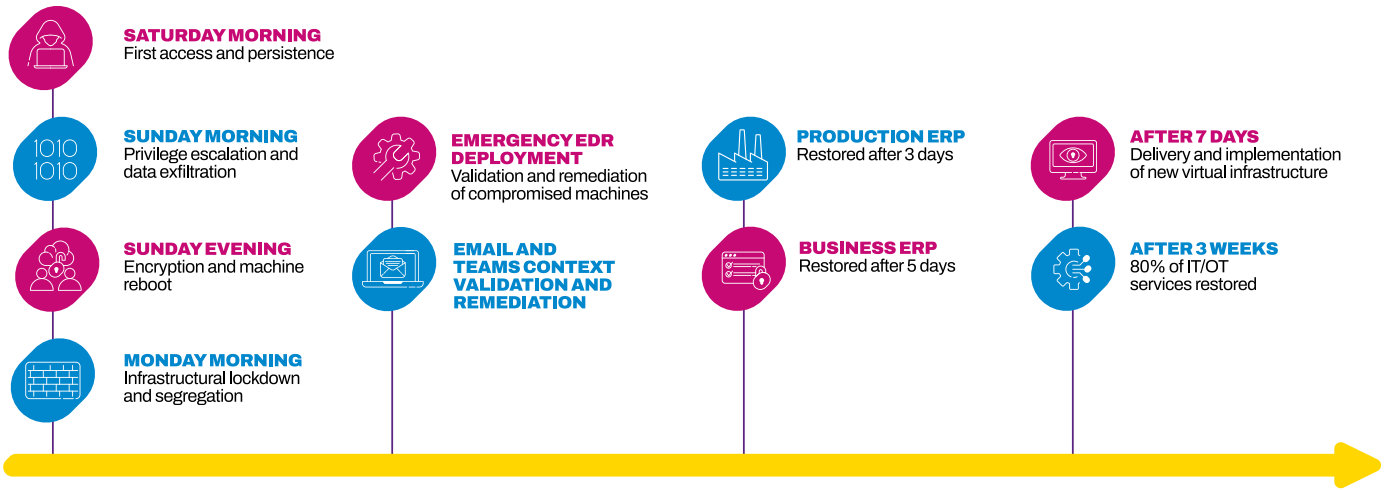
REVEALING THE BREACH

The incident began with an unexpected restart of the virtual machines. As the malfunction persisted, the internal IT department recognized the critical nature of the situation and reached out to HWG Sababa for assistance.

In the initial response, HWG Sababa immediately deployed **two specialists from the Defence Center** to assist the company in managing the incident. Together, they initiated a **forensic investigation**, aiming to uncover the attack's origins and progression. Right away, a significant revelation emerged: the attackers entered the network through a **VPN channel**, sidestepping the need for brute-force tactics. Exploiting a **compromised service user account**, they gained unauthorised access, setting the stage for their malicious activities.

The attackers' sophisticated capabilities enabled them to reach a primary target – the **Domain Controller**. By taking control of this critical node and conducting targeted enumeration activities, they discovered **other misconfigured accounts**, some of which held elevated privileges. With these powerful keys in hand, the attackers released a **wave of malware**, including Mimikatz, which eluded detection by the organisation's antivirus system. Aside from this system-disrupting activity, they orchestrated a **data exfiltration to a Russian IP address**. After completing the exfiltration and preparing their disruption tools, they initiated an **encryption campaign on both host machines and the virtual environment.**

THE STAGES OF INCIDENT MANAGEMENT AND RESPONSE



Infrastructure lockdown and segregation.

Upon HWG Sababa's immediate involvement in the incident, quick action was taken to issue emergency containment directives. This encompassed a **comprehensive lockdown of both on-premise and cloud-based infrastructure** by disabling Internet access, as well as the i**mplementation of east-west segregation**, thus creating isolated subsets of the infrastructure. This approach facilitated the analysis, containment, and recovery operations without disrupting services that were not impacted and could be restarted quickly.

Active Directory Validation.

Following the initial containment measures, a **careful validation of the Active Directory environment was undertaken**. Every user account was scrutinised to ensure the absence of any **unauthorised administrators** established by the attacker.
This verification process facilitated the **successful reactivation of email functionality within one day from the initial emergency call.**

EDR and Compromise Assessment.

In parallel with the onsite investigation, HWG Sababa's experts quickly **provided and deployed cutting-edge EDR licences**, replacing the less effective antivirus solution. Collaborating closely with the organisation, they successfully deployed **over 3,000 licences across both virtual and physical servers within a week**, aiming to cleanse the infrastructure and enhance coverage against potential re-infections. Designed to halt any future outbreaks before they could escalate, this solution proved instrumental in fortifying defences.

Meanwhile, leveraging **Compromise Assessment**, HWG Sababa's Defence Center remotely analysed **machines showing evident signs of compromise to assess their health status**. This proactive measure aimed to identify affected machines necessitating backup restoration, where feasible, while also identifying those deemed secure for reintegration into production.

Restoring Core Services.

Drawing insights from the Compromise Assessment and the deployed EDR licences, HWG Sababa's specialists started crafting **guidelines for service restoration.** Priority was given to core services, following a structured order of importance, with a focus on tasks that could be **quickly accomplished and produced immediate benefits.** Starting with the corporate ERP systems, one was restored within 3 days, while the other was reestablished within 5 days.

Onsite Expertise.

By the end of the first week, a virtualized systems specialist was sent to the customer site. With vast expertise and essential hardware, he set up a **customized virtual infrastructure for machine rebuilding and remediation**. Moreover, throughout the latter half of the second week, another expert was assigned to guide the **rebuilding and restoration process of the network**, maintaining strict adherence to the latest cybersecurity principles.

THE FINAL MILE

Within three weeks, the company had successfully regained stability, with **75% to 80% of critical services smoothly restored**. However, overcoming the final 20% presented the most difficult challenge, demanding intensified efforts from IT departments, as energy levels diminished. Despite the significant progress made, it is precisely in this phase that the most unpredictable obstacles typically arise, moving the finish line further.

"Throughout our entire collaboration with the CIO and CISO, we tackled technical challenges and deliberated on operational decisions that are unique to the Incident Response context. Few are ever fully prepared for such scenarios. Incident Response should always be recognized as a complete crisis where the primary challenge is to navigate, manage, and ultimately overcome moments of uncertainty in resolution, while maintaining unwavering lucidity. Our extensive experience in incident management and the dedicated professionals we engaged enabled the CIO, CISO, and IT teams to effectively handle and respond to the crisis without losing sight of the ultimate goal or succumbing to exhaustion. These efforts were deeply appreciated.",

explained Raffaele Fazio, Head of Defence Center at HWG Sababa.

Indeed, recovering from a cyber crisis requires not only technical measures but also **attending to the human element**. Dealing with such emergencies can be stressful, but having a trusted cybersecurity player by your side can provide reassurance that you're not alone in facing the challenge. Here HWG Sababa played a key role in **offering clear guidance, answering questions**, and **providing ongoing support** to individuals and stakeholders who may be feeling overwhelmed or uncertain about how to navigate the recovery process, especially within the last mile.

"After resolving the incident, our commitment persisted. We remained fully dedicated to supporting them in fortifying their cybersecurity posture, mitigating future risks, and safeguarding against similar incidents. Through strategic planning and collaborative efforts, we are working hand in hand to build a proactive defence strategy against evolving cyber threats.",

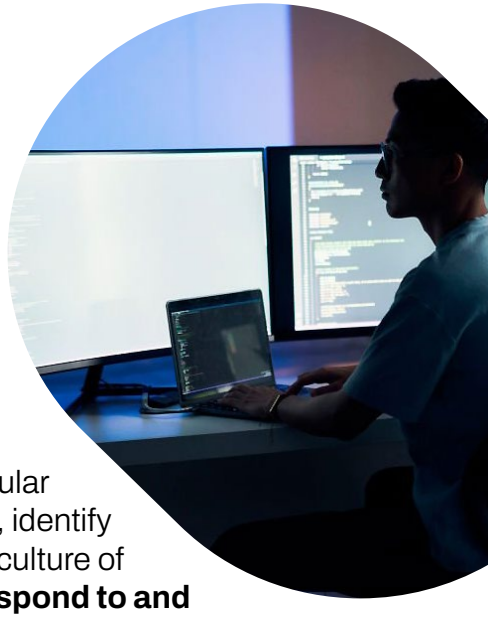
continued Raffaele Fazio, Head of Defence Center at HWG Sababa.

LESSONS LEARNED

1. Proactively develop and implement an Incident Response plan

Insights gleaned from this experience underscore the critical need for organisations to **proactively develop and implement comprehensive Incident Response plans**. This ensures a unified and efficient response during cyber emergencies, where every passing hour presents a valuable opportunity to navigate challenges and mitigate financial, reputational, and operational impacts.

2. Continuous review and updating of strategies



But that's not all – it's crucial for organisations to **regularly review and update their strategies** based on insights gained from real-world incidents. This proactive approach ensures that they remain **agile and adaptive in the face of evolving cyber threats**. By continuously learning from past experiences and adjusting their tactics accordingly, companies can strengthen their resilience and readiness to effectively mitigate future risks.

3. Prioritise ongoing training

Ultimately, it's fundamental to **prioritise ongoing training and exercises to ensure preparedness among staff at all levels**. Regular simulations of cyber emergencies help validate response procedures, identify gaps, and enhance coordination among stakeholders. By fostering a culture of preparedness, organisations can bolster their ability to **effectively respond to and recover from cyber incidents**, ultimately minimising the impact on their operations and interested parties.

Take proactive steps to protect against potential cybersecurity incidents.

Reach out to us to develop a tailored Incident Response plan: **contacts@hwgsababa.com**

HWG Sababa

Follow us on:

HWG Sababa

www.hwgsababa.com