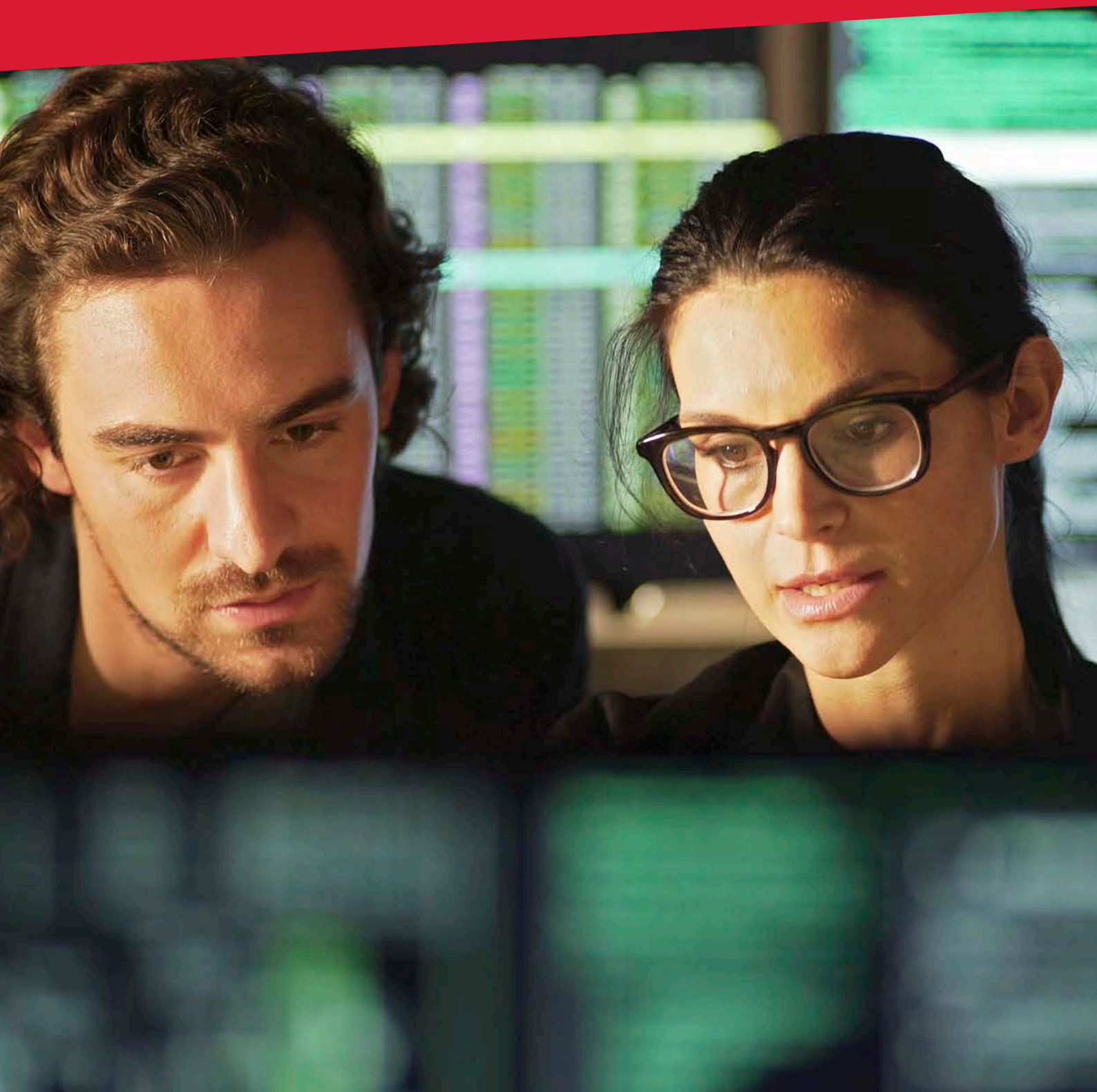
Integrity360
your security in mind

INCIDENT RESPONSE:
Be prepared for not "if" but "when"



Integrity360
your security in mind

The potential benefits of remediating an attack quickly rather than waiting weeks or months are irrefutably valuable to any modern business and make the difference between minor inconvenience and existential business impact.

Introduction to Incident Response

You never know when it's coming. You might not be prepared when it does. But every company needs to be able to respond to a cyber security incident – and do so quickly.

The rate and volume of cyber-attacks grows by the day. Cyber criminals are continuously iterating their malicious code and their methods of operation, hoping to stay one step ahead of the cyber security tactics that businesses use to protect their digital infrastructure.

At the same time, the companies that are leaning heavily on their cyber security solutions as the only tools they need to stop hackers in their tracks are forgetting about what happens when those defences fail. And when it happens, too many organisations find they are not equipped to respond. It's a trend that's leaving even huge organisations like Equifax and Marriott unable to respond, in some cases for years, to an attack once they've been breached.

Because let's be honest with ourselves: As much as we try to prevent a cyber-attack, we live in a world of 'when' and not 'if' it'll happen.

Which brings us to what happens next – incident response. The most important action to be taken after a security incident is detected are often out of reach for a lot of companies. The technical expertise required to analyse, contain, eradicate and recover from a cyber security threat isn't a resource that's ordinarily freely available.

It's why the companies that are truly proactive in defending against a cyber-attack see incident response services as a key cog in their cyber security machine. And it's no surprise that proper incident response planning is seen as a core security control in all the leading cyber security frameworks and standards.

Moving away from simply detecting a security incident and towards responding effectively to it is not an easy journey. But the potential benefits of remediating an attack quickly rather than waiting weeks or months – or worse, not knowing how it happened – are irrefutably valuable to any modern business and make the difference between minor inconvenience and existential business impact.

The Cyber Threat Landscape

The biggest threats to companies that lived on the internet used to be worms and email scamming. Now, there's phishing, malware, ransomware, cryptojacking, formjacking, trojans, spearphishing, and supply chain compromise to worry about – amongst other emerging threats.

In truth, the volume, complexity and sophistication of attacks continues to grow just as quickly as our ability to defend against them. Consider ransomware alone, where strains like GandCrab, SamSam and Ryuk have grabbed headline after headline for their highly targeted and disruptive attacks, rapidly evolving malware code and profitability for their creators.

Major corporations across the world have already begun to feel the impact of cybercriminals' evolution in tactics. The Marriott Hotel chain, for instance, saw 500 million records stolen over a four-year span where hackers had free reign of its infrastructure. British Airways saw 500,000 customer records accessed in a data breach. Both companies now face a GDPR fine totalling over €100 million.

A GROWING ATTACK SURFACE

Organisations face major hurdles in securing their digital infrastructure, whether it be from a lack of technical expertise, poor workforce awareness of cyber threats or the inability to convince the board of directors to buy-in to cyber security in general.

The attack surface for hackers to expose businesses for their lack of cyber security is only growing as companies become more interconnected than ever before. There are four attack vectors that cybercriminals are constantly looking to exploit:

EXPOSED SERVICES

Unsecured systems and services exposed to the internet make easy targets. High cloud adoption rates continue to increase exposure.

VULNERABILITIES

Vulnerability exposure still provides a key avenue for attack. Ransomware creators are rapidly adapting to take advantage of newly disclosed vulnerabilities.

PHISHING

Ever-present despite variability in effectiveness. The vast majority of campaigns employ phishing attacks in the initial phases.

MALWARE

Whether first stage for initial exploit or latter stages for persistence or lateral movement, the deployment of malware is ubiquitous across campaigns.

Challenges Facing Cyber Security

Companies are tasked with more than ever before in trying to maintain business continuity, as a digital attack could be just as damaging as a fire in a warehouse or a lawsuit from a competitor. Addressing those threats posed by cybercriminals – and many organisations' lukewarm commitment to cyber security – isn't easy for the average business.

At a high level, organisations need to be able to:

- ✔ Reduce exposure
- ✔ Detect and prevent attacks
- ✔ Be prepared for incidents

Most businesses account for the first two with the implementation of next-generation tools like email and web filtering, firewalls, endpoint, antivirus, EDR tools and SIEM. The third item on the checklist sometimes escapes companies because of how complex a response to a cyber-attack can become, or a false belief that there is such thing as 100% security.

Because there isn't a one-size-fits-all or a plug-and-play solution for incident response, companies must ask themselves the following questions when evaluating their current abilities:

INCIDENT RESPONSE CHALLENGES

SECURITY

- If we were breached, who would we contact?
- Could we support a major incident?
- Do we have the capability to investigate the incident?

RISK MANAGEMENT

- Can we contain an incident in the shortest time possible?
- How do we ensure the incident impact is fully eradicated?

COMPLIANCE AUDIT

- Are we compliant?
- Can we quickly demonstrate compliance?
- Can we detect and react to changes affecting compliance?

What Is Incident Response And Why Is It Important?

Incident response refers to a company's ability to investigate, diagnose, contain and remediate a security incident and navigate its consequences.

To be effective, it must take place in the quickest time period possible. The longer the attacked dwells inside your environment, the more damage they can do.

It can make the difference between a company recovering seamlessly from an incident or never recovering at all.

Incident response has grown so important and influential that it has become one of the core reasonings behind the introduction of the TIBER-EU framework, which uses Red Team assessments to evaluate European financial institutions' ability to detect, respond to and remediate a cyber-attack.

Apart from the idea that incident response has earned its right in any board-level discussion on cyber security, its importance is also tied to the simple fact that businesses must be able to respond to a cyber-attack if they want to avoid suffering its three negative impacts: reputational risk, legal risk and financial risk.

Why Use Incident Response?

Within the industry, it's seen as a core component of any well-thought-out cyber security strategy. Incident response is an aspect of compliance for the following major cyber security frameworks:

- ✔ **NIST PR.IP-9**
- ✔ **CIS CSC 19**
- ✔ **COBIT 5 APO12.06, DSS04.03**
- ✔ **ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1**
- ✔ **ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3**
- ✔ **NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17**

HOW MATURE IS YOUR INCIDENT RESPONSE CAPABILITY?

Below you'll find a look at what an effective incident response strategy and team is capable of.

1

NON EXISTENT

No incident response plan in place

2

INITIAL / AD-HOC

Incident response plan documented, however not tested or rolled out across all the relevant stakeholders

3

DEFINED AND REPEATABLE

Incident response plan in place, defined team roles and responsabilities. IR specialist skills or retainer in place

4

MANAGED

Incident response plan in place with defined roles, responsabilites and skills in place. Occasional dry-run

5

OPTIMISED

Plan in place and well understood with all roles and skills in place. Regular fire drills and continuous improvement loop.

Integrity360's Incident Response Service

Intergrity360 leverages an array of next-generation technology and expert cyber security specialists to deliver incident response. The service assists your organisation in responding to a suspected security incident in a time-efficient and productive manner. Our model runs on a staged approach, which stops the active threat by applying proprietary tools and processes to quickly evaluate the environment and remedy the situation. These stages are:

1 Preparation

Integrity360 incident response specialists meet with the client to discuss the scope of the incident and establish a communication matrix for escalation.

2 Detection and Analysis

Assist in the deployment of assessment tools. Conduct log analysis from the clients systems and environment in an effort to determine the root cause of the incident.

3 Containment and Eradication

Collaborate with the client in containing the incident, and restoring the business to normal operational standard.

4 Post-Incident Activity

Our incident response team produce a technical report detailing the incident while a briefing of management, board and any other key personnel takes place.

The service empowers companies to react to security incidents that threaten their business continuity despite not potentially having the skills or resources on-site. By combining the use of the client's own logs and systems with leading analysis and diagnostic tools and the security expertise of a dedicated Security Operations Centre and on-the-ground support, organisations can cut containment from months to just a matter of days or hours and minutes rather than weeks or months.

Integrity360's incident response service provides:

Enhanced incident response

Retain visibility and control by availing of best-practice processes and tools and leveraging experience from the front lines of cyber security.

Strengthened business continuity

Access to a 24x7x365 Security Operations Centre and a defined response Service Level Agreement (SLA) helps to avoid single points of failure within organisation.

Deep skills on demand

Add scarce deep and broad technical skills to rapidly assess the incident and provide detection on how to analyse and contain the situation.

Cost-efficient option

Opportunity cost savings result from economies of scale in resourcing, processes and tools, as well as the ability to repurposes costs that aren't incurred.

Deliverables and Benefits of Incident Response Service

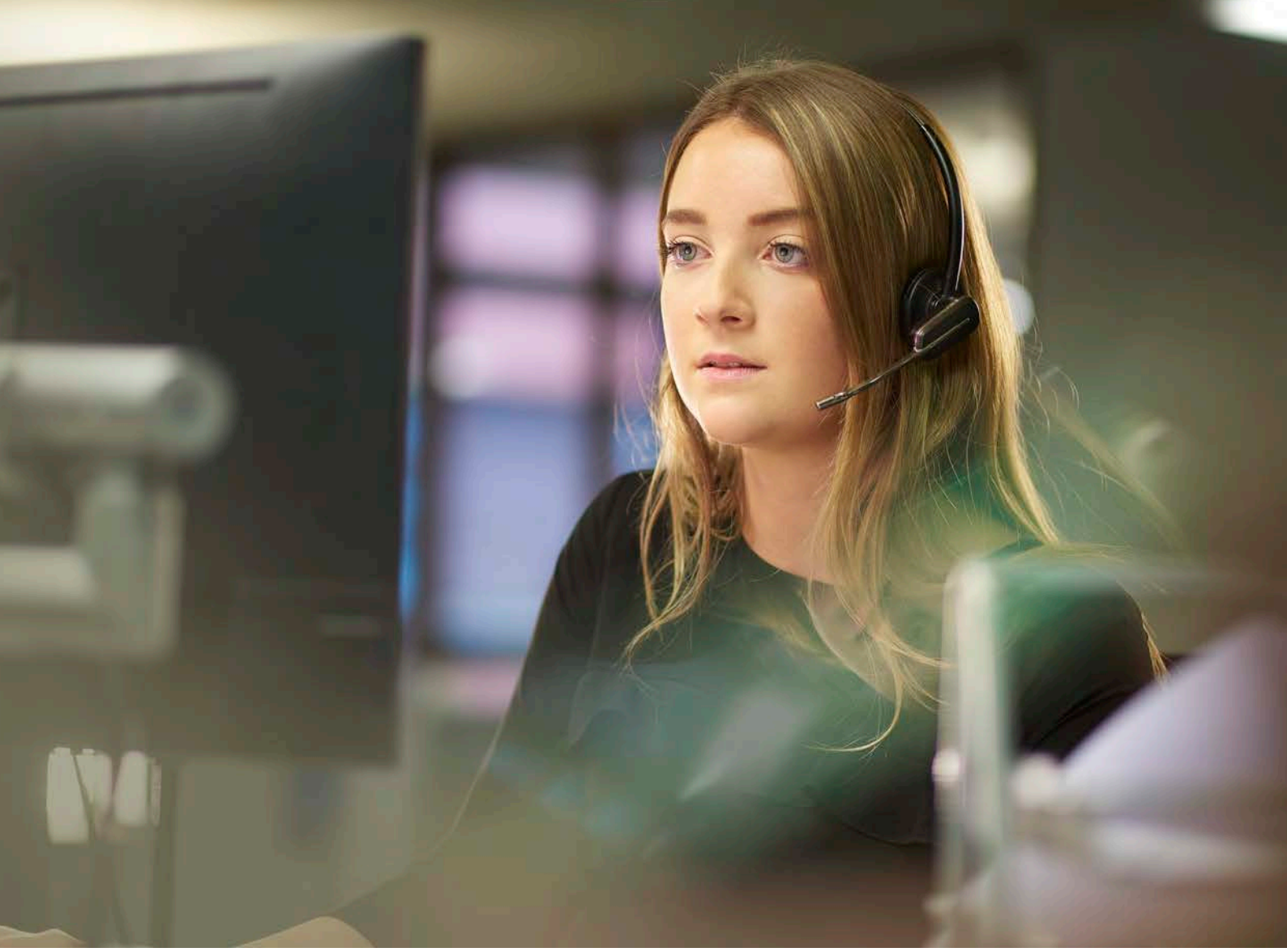
Apart from gaining access to highly skilled cyber security specialists and the backing of a state-of-the-art 24x7x365 Security Operation Centre, clients also receive a number of deliverables under a standard incident response retainer. These deliverables include:

- Incident Response Preparedness Assessment
- Investigative support and direction for every unique incident.
- Malware and log analysis.
- Containment and remediation planning and assistance.
- Regular status reporting and project management-related activities.
- Forensic investigation, acquisition of electronic data and adherence to strict chain-of-custody procedures, where required.
- Reporting and presentations associated with our findings and recommendations.

Integrity360's incident response service is broken down into two standard retainers. They allow organisations access to experienced incident response experts who can quickly recognise and contain a threat.

FEATURES	No retainer - On Demand IR	40 hours IR retainer	80 hours IR retainer	120 hours IR retainer
Prepaid hours	None	40	80	120
Additional hours rate	On-demand rate	40 Hr Retainer rate	80 Hr Retainer rate	120 Hr Retainer rate
Minimum additional hour blocks	20	10	10	10
Minimum hours per incident	none	none	none	none
Response Time 24x7*	Best efforts	2 hours	2 hours	2 hours
Incident Response Preparedness Assessment	No	Included	Included	Included
Unused hours apply to other services	No	Yes	Yes	Yes

*Notwithstanding the response time SLA, average response time is under 15 minutes.



At a high level, the service provides companies with more resources, specialised services and managerial skills to deal with security incidents – not to mention the in-depth perspective on how to remediate them.

Apart from that, clients gain access to malware experts who can add to the decision-making perspective and proprietary tools and proven methodologies to respond more quickly. On top of it all, the service provides strategic malware, forensic and log analysis reporting personnel to educate internal teams where needed.

Other service benefits include:

Timeliness: Guaranteed availability of an experienced incident response expert in the event of a compromise or suspected breach.	**Productivity:** Speed up investigations to contain them within days and reduce response times while still clearing tasks and objectives.
Skillset: Improve incident response capabilities and reduce exposure to attacks and breaches with dedicated personnel	**Resourcing:** Demonstrate compliance and improve policy enforcement with skilled staff you can bring on at a moment's notice.
Experience: Skilled specialists from a variety of disciplines paired with a communication matrix allow for enhanced visibility and clearer decision-making.	**Value:** Repurpose the hours not used to improve other areas of the cyber security strategy while also staying prepared in the event of a security incident.

Why work with Integrity360

Security incidents continue to plague companies across the world, fanning flames at their business continuity and putting their reputation and ability to operate at risk.

Integrity360's incident response specialists have years of experience with the real-world threat landscape. The incident response service plays a key role in ensuring that a company can safely go about their day-to-day routine knowing that if the unexpected takes place, a skilled team is waiting in the wings to contain and remediate.

Through detailed log analysis, the implementation of next-generation cyber security tools and an acute handle on the cyber-threat landscape, Integrity360 experts can quickly detect, identify and contain a security incident.

Contact an Integrity360 advisor today to learn how you can elevate your company's risk posture by emailing us at info@integrity360.com or visiting integrity360.com for more information.

Integrity360
your security in mind

HEAD OFFICE
3rd Floor, Block D, The Concourse,
Beacon Court, Sandyford, Dublin 18.
+353 (0)1 293 4027

UK OFFICE
90 Long Acre, Covent Garden,
London, WC2E 9RZ
+44 2033 973414

NEW YORK OFFICE
260 Madison Avenue, 8th Floor
Manhattan, 10016
+1 212 461 3286

info@integrity360.com
www.integrity360.com

Integrity360

your **security** in mind