# Calian Digital Forensics and Incident Response (DFIR) Retainer

Calian's cyber investigation team delivers advanced digital forensics and incident response (DFIR) services to respond to evolving cyber threats. Drawing on expertise in endpoint and mobile forensics, ransomware, breaches, data exfiltration and more, the team combines threat intelligence with tailored methodologies to identify threat actor, techniques and indicators of compromise.

Calian's DFIR team is aligned with Microsoft detection and response team (DART) methodology, ensuring precision and compliance with industry-leading standards. The team takes an integrated defence approach, combining security insights with defensive operations, and is empowered by Microsoft's extended security stack to deliver a holistic security strategy.

Calian incident response services are seamlessly integrated with Calian's MXDR and SOC services or available as a stand-alone service. The team conducts in-depth investigations across the cloud, endpoints and infrastructure, to contain and manage cybersecurity incidents.

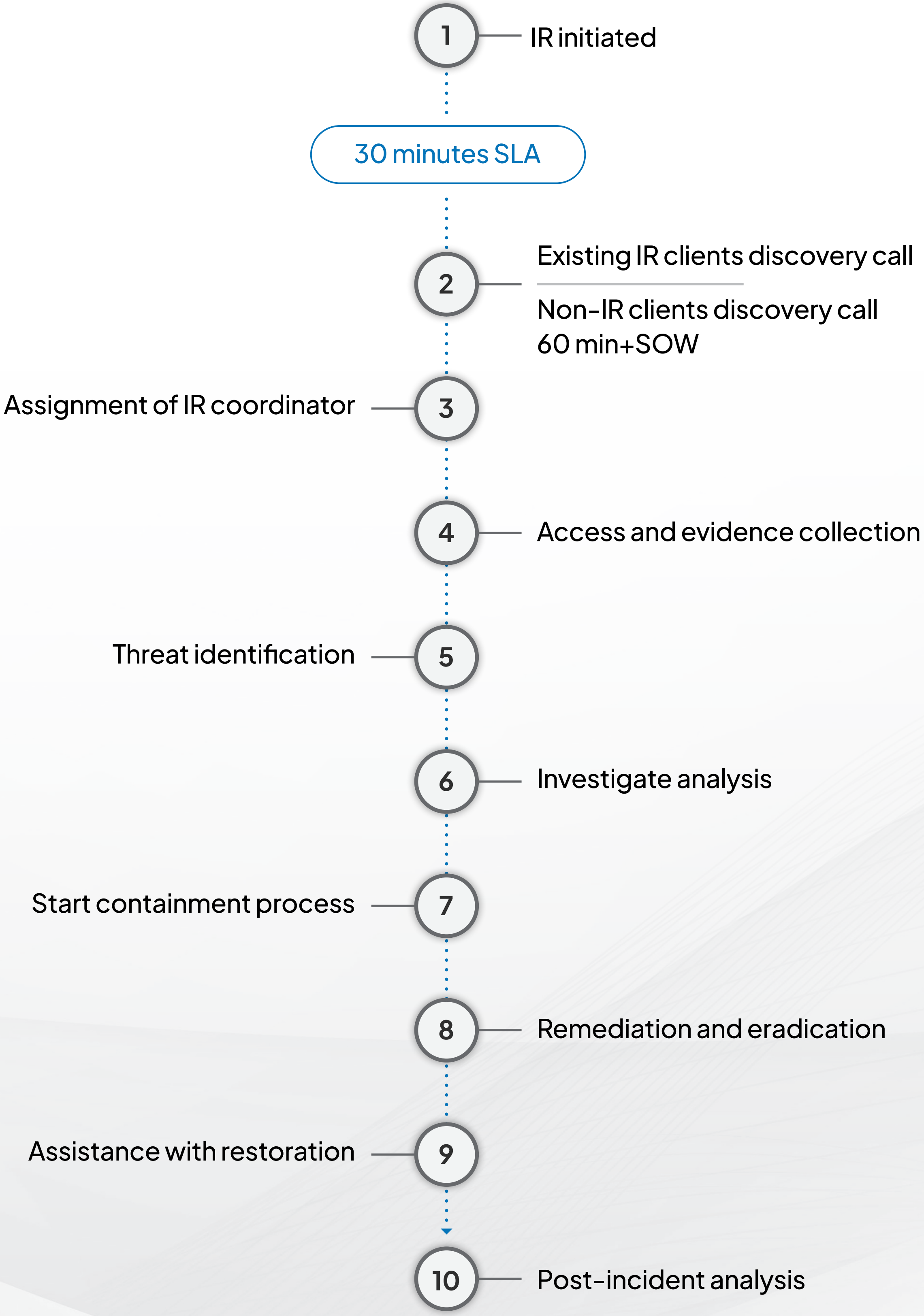
## Why your organization needs an incident response retainer?

An incident response retainer is a critical investment for organizations seeking to enhance their cybersecurity posture and mitigate the potentially devastating impacts of cyber incidents. By securing an incident response retainer, organizations gain immediate access to a team of specialized cybersecurity experts who understand your environment through the onboarding process and can swiftly respond to and contain threats, reducing the time between detection and action. This rapid response is crucial in minimizing damage, downtime and associated costs during a cyber crisis.

## Calian's incident response approach

- **Live system analysis:** Real-time investigation of active systems to capture volatile data and detect ongoing threats.
- **Postmortem forensics:** Meticulous examination of compromised systems to uncover hidden evidence and reconstruct attack timelines.
- **Network forensics:** In-depth investigative analysis of network traffic to trace attack vectors to correlate with other forensic evidence.
- **Mobile forensics:** Advanced techniques to recover data from a wide range of mobile devices, including smartphones and tablets.
- **Compliance with industry standards:** Calian adheres to the NIST SP 800-61r2 incident response lifecycle and follows Microsoft DART best practices ensuring compliance and industry-leading standards.
- **Integration with MXDR and SOC:** Calian's DFIR services are supported by Microsoft security technologies that boost the effectiveness of incident response and overall cybersecurity posture.

## Incident response customer journey



1 IR initiated

30 minutes SLA

2 Existing IR clients discovery call

Non-IR clients discovery call
60 min+SOW

3 Assignment of IR coordinator

4 Access and evidence collection

5 Threat identification

6 Investigate analysis

7 Start containment process

8 Remediation and eradication

9 Assistance with restoration

10 Post-incident analysis

## Incident response report

After an incident, our team delivers a comprehensive incident response report. The report includes a chronological timeline of events, a detailed description of the attack vectors used, the extent of the Incident, and the specific actions taken to contain the threat based on the evidence available during the investigation. This report not only aids in your internal review and improvement processes but also serves as a valuable document for compliance, insurance claims and potential legal proceedings.

Incident response investigation report key components:

- **Executive summary:** A concise overview of the incident, key findings and high-level recommendations.
- Investigative timeline: A detailed timeline illustrating key events, methodologies and findings from the incident. This includes artifacts of interest that support or refute investigative hypotheses.
- **Recommendations:** Expert guidance on enhancing security measures and effectively mitigating risks to prevent future incidents.

## Why choose Calian?

When a cyber incident strikes, you need more than just technical expertise. You need a trusted partner who understands the stress and uncertainty you and your organization are facing. We help you navigate the complex landscape of cyber incidents, translating technical complexities into clear action plans, and providing the confidence you need to make critical decisions. With Calian, you're never alone when facing a cyber crisis.

### Industry expertise:

- Trusted expert specialists with deep knowledge of advanced threats and evolving attack patterns, experience recovering some of the most complex infrastructures in the world.
- A cyber investigation team that also functions as a cyber threat intelligence unit, leveraging expertise in every investigation.
- Calian's cyber investigation team, with over 25 years of experience in digital forensics, incident response, and threat intelligence, using methodologies aligned with Microsoft DART team best practices to ensure precision and compliance with industry-leading standards.
- Proven expertise across a wide range of security incidents, from benign threats to global ransomware-related outages.

### Complete NIST compliance:

Calian adheres to the NIST SP 800-61r2 incident response lifecycle and Microsoft DART methodology, ensuring precision and adherence to industry standards.

### Four key stages of NIST IR lifecycle:

1. **Preparation:** Developing capabilities to address incidents effectively.
2. **Detection and analysis:** Identifying threats, analyzing attack vectors and determining the scope of incidents.
3. **Containment, eradication and recovery:** Stopping threats, removing malicious actors and restoring systems to a secure state.
4. **Post-incident activity:** Leveraging lessons learned to enhance defences and reduce future risk.

### Timely response:

- Rapid support to minimize operational disruptions and mitigate damage during active incidents.

### Custom solutions:

- Tailored strategies for organizations of all sizes and industries.
- Collaboration with other Calian and client teams to ensure thorough investigations, threat remediation and restoration services.
- Integration with Calian's offensive security team to enhance the investigation of complex threats.
- Proactive and pre-emptive cyber programs that align to your organizational needs moving forward.

## Ready to get started? Contact our team

**In the event of a suspected cyber incident, immediate action is crucial:**
You can reach us 24/7 via our dedicated toll-free hotline 1 (833) 485-3760.

For less urgent matters or to initiate a retainer agreement, email us at incidentresponse.calianitcs@Calian.com.

Our rapid response team is always on standby, ready to spring into action and provide immediate support. Whether you're facing an active threat or strengthening your security posture, we're just a call or email away.

calian.com/itcs
For more information, contact: itcs@calian.com

calian.com | info@calian.com | 1.877.225.4264 |

**Service:**
Incident Response Retainer

**Duration:**
Annual Contract
**Service Level:** 24/7 service