COALFIRE | Arete Advisors

DATASHEET

# Incident response retainer and advisory services

## Prepare for and resolve cyber incidents quickly and effectively

A serious cyber incident is a question of "when," not "if." Cyber attacks are increasing, and organizations are at risk, regardless of their size or industry. Coalfire partners with Arete Advisors to provide an elite set of incident response advisory and retainer services. We can help you plan for security incidents before they happen and provide the expertise you need when they do occur.

### OUR APPROACH

Leveraging common frameworks like NIST Special Publication 800-61 "Computer Security Incident Handling Guide," ISO 27035, and best practices, we help you enhance your preparedness for a cyber incident.

Our experts employ investigative techniques aligned to legal requirements, ensuring chain of custody for evidence and effective identification, containment, and eradication from the cyber incident.

After the incident has been contained and eradicated, our team develops a strategy for remediating the source of the incident, investigates opportunities for improvement, works with you to implement the strategy, tests effectiveness, and finally, validates the implementation of the remediation strategy.

### OUR EXPERIENCE

Our experts have analyzed multiple types of cyberattacks over the last 20 years, including:

- **Insider threats:** The activities of former and current employees, contractors, or business associates who have inside information on the organization
- **State-sponsored attacks:** Crimes of trade secrets and other sensitive data across a range of industries
- **Destructive attacks:** Attacks intended to cause the victim organization pain by making information or systems unrecoverable
- **Protected health information (PHI) breaches:** Exposure of protected healthcare information
- **Personally identifiable information (PII) breaches:** Exposure of information used to uniquely identify individuals

### WHY COALFIRE

- **World-class expertise** – Our experts have worked hundreds of incident response cases, including some of the world's largest and most complex. They have conducted malware reverse engineering to help resolve incidents, helped organizations return to normal operations, and provided guidance on how to prevent recurring incidents.
- **Proven** – Coalfire is the trusted advisor to many law firms, government agencies, and public and private organizations.
- **Faster, high-value results** – As a technology-agnostic partner, we leverage your current investments to provide quick, effective support. Quick resolution lowers costs significantly and empowers executives to make the right business decisions.
- **One-stop-shop for preparation, response, and remediation** – We coordinate, communicate, and report on every aspect of incident response activity. We learn your environment during the preparation phase, enabling us to provide efficient support. Investigation reports include recommendations and executive- and board-level summaries.
- **Reliable operations** – Experts are available 24x7, and will contact you within one to four hours for remote assistance and in as little as 12 to 24 hours for onsite assistance.

## INCIDENT RESPONSE RETAINERS

We provide a broad set of incident response services, offered a la carte and through our incident response retainer (IRR).

| SERVICE | DESCRIPTION | STANDARD RETAINER | ENHANCED RETAINER |
|---|---|---|---|
| **Onsite or remote requirements analysis** | Interviews of key client stakeholders, operational environment assessment, and determination of any special requirements | ⬢ | ⬢ |
| **Incident response plan development** | Development of a tailored incident response plan consisting of a process overview, team organization chart, roles and responsibilities, contact lists, incident classification and categorization scheme, and incident report form template | ⬢ | ⬢ |
| **Incident response playbooks** | Development of up to four customized playbooks containing procedures and flow charts for responding to incidents you are most likely to experience | | ⬢ |
| **Status reviews and refresh** | A review of in-place materials to determine the best method to update the content | ⬢ (Annual) | ⬢ (Semi-annual) |
| **Tabletop exercise** | A session where the incident response team is assembled, given one or two distinct scenarios, and discusses actions to be taken as part of the incident response | | ⬢ |
| **Incident response hotline access** | Experts on standby 24x7 | ⬢ | ⬢ |
| **Incident response support services** | Support hours included with retainer subscription | 25 hours | 45 hours |
| **Preferred retainer rate** | Discounted hourly rate for additional incident support related to a breach – a deeper discount with the enhanced retainer | ⬢ | ⬢ |

### Incident response support includes:

- ***Incident response hotline access:*** Remote (within one to four hours) or onsite (within 12 to 24 hours) incident support related to a breach
- ***Incident triage:*** Organization and planning for incident response activities, including assistance with identifying potentially compromised hosts
- ***Incident investigation/forensics:*** Root-cause identification of the incident including memory and disk image forensic review
- ***Containment services:*** Identification and deployment of compromised host containment activities, including potential removal or segregation of compromised hosts from the environment
- ***Eradication services:*** Removal of the malicious or unauthorized infections

### Post-incident support includes:

- ***Remediation and engineering support:*** Guidance on best-practice activities and technologies to reduce the likelihood of another cyber incident

DS_IncidentResp_040318

**ENSURE YOU'RE READY FOR AN INCIDENT AND THAT YOU CAN RECOVER.**

**Learn more about Coalfire's incident response retainer and advisory services.**
**Coalfire.com | 877.224.8077**

COALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 17 years and has offices throughout the United States and Europe. **Coalfire.com**