FIELD EFFECT

Incident Response

Minimize business impact with accelerated expert-led response

When incidents occur, you want to recover as quickly and effectively as possible. Working with a trusted incident response (IR) partner ensures you have the expertise and skillset to confidently recover.

With Field Effect incident response services, you can count on our cybersecurity analysts to help you navigate your breach and to deliver accelerated and trusted response services so you can get back to business. Combining decades of IR experience with proven methodologies and innovative technology, we deliver accelerated and expert-led investigations to efficiently respond to threats and protect you against future attacks.

Our team has a proven track record defending many of the largest and most secure networks in the world. This depth of experience provides a perspective into incidents that others may miss. We work as an extension of your team throughout the incident response journey to:

RESPOND FASTER

Leveraging Field Effect MDR, we gain immediate visibility into your environment and can assess the ongoing breach. This insight enables us to react to any ongoing malicious activity by containing and blocking threats as they occur.

UNDERSTAND THE THREAT

A key aspect of incident response is understanding what occurred and why and how it occurred. Field Effect's world-class investigators conduct detailed forensic analysis to determine root cause, threat actor techniques and whether sensitive data has been breached.

RECOVER WITH CONFIDENCE

Our team will work with you to ensure your best path to recovery is achieved and all indicators of malicious activity have been contained. For peace of mind, we monitor your environment for 90 days to protect you from possible return attacks.

NAVIGATE OPERATIONAL IMPLICATIONS

Navigating an incident is always complex and unpredictable. In addition to containment, mitigation, and recovery, your dedicated IR case manager will provide guidance around operational implications such as cyber insurance, legal, communications, and more.

STRENGTHEN YOUR ENVIRONMENT

After your recovery, Field Effect MDR will help you proactively identify high risk vulnerabilities and attack vectors that threat actors are likely to exploit. This enables you to proactively improve your attack surface and prevent future attacks.

Key benefits:

- ✓ Expert-led recovery
- ✓ Innovative technology
- ✓ Proven methodologies
- ✓ 90 day post-incident monitoring and response
- ✓ Reporting suitable for legal and insurance purposes

Incident response services

While no two incidents are identical, there are three main response types which cover most scenarios. The specific course of action for each case will be determined during an initial scoping call with the Field Effect Incident Response team. Note that each IR package includes three months of ongoing monitoring and protection to prevent repeat attacks and to highlight other vulnerabilities which require remediation.

	Package	Description	Response elements
01	**Comprehensive Incident Response**	This is the most common package and includes in-depth analysis of the incident and reporting as required by you, your business, and/or third-party stakeholders such as insurance and legal firms. This includes investigation of forensic data and logs from systems determined to be the best source of information to identify and understand the threat. The 90-day Field Effect MDR deployment aids in containing the threat and recovering securely.	[X] Prepare [√] Identify [√] Contain [√] Investigate [√] Eradicate [√] Recover
02	**Cloud Account Incident Response**	This package is applicable for a cloud business email breach. It provides an in-depth analysis of the incident with a comprehensive report suitable for legal and insurance purposes. This includes thorough analysis of suspected compromised accounts and other applicable data sources determined necessary for the investigation. The 90-day monitoring of your organization's cloud email services allows us to contain the threat as you return to business as usual.	[X] Prepare [√] Identify [√] Contain [√] Investigate [√] Eradicate [√] Recover
03	**Standard Incident Response**	This package is applicable when a compromise has occurred, and some containment and resolution steps were already taken. By leveraging Field Effect's MDR platform, dedicated cybersecurity breach management and our cybersecurity analysts, this package will ensure the appropriate steps are being taken to provide protection and secure recovery of the environment.	[X] Prepare [X] Identify [X] Contain [√] Investigate [√] Eradicate [√] Recover

Reach Out:

If suspect you or one of your clients is experiencing a breach, please reach out as soon as possible:

fieldeffect.com/report-an-incident
forensics@fieldeffect.com
+1 (800) 299-8986