FIELD EFFECT

Incident Response

Identify, isolate, and resolve — with experts at your side.

No one wants to suffer a security incident, and most don't want to believe it can happen to them. The unfortunate reality is that it can happen to any organisation, large or small, and the results can be devastating if not appropriately and expediently managed and resolved.

An incident is any unauthorized access or attempted access to system(s), and/or a breach of security policy with intent to negatively impact system integrity or availability.

The specifics can vary from situation to situation, but often involve theft of intellectual property or sensitive data, financial crime, denial of service, or a variety of destructive attacks. In any case, the most important result for an organization is to quickly get business running, with as little damage as possible.

What to do in case of an incident

DO's

- Take a breath and try to remain calm. We will help you through this!
- Reach out as quickly as possible.
- Decide who are the stakeholders that need to be involved.
- Send an email to forensics@fieldeffect.com as soon as possible to get started on the response and resolution, in order to minimize any damage.
- Consider chain of custody requirements (ask us if you're not sure).
- Focus on this order of operations: Identify, Recover, Protect (Field Effect works on your behalf through each step).

DONT's

- Wait. Even if you just suspect an incident is happening, reach out.
- Try to cover any tracks. This isn't a blame game, and these actions can slow down the time to recovery.
- Talk about the incident outside of the direct stakeholders.

How Field Effect resolves the incident

There are four major work phases of Incident Response support that the Field Effect Incident Response team provides:

- Issue Identification
- Root Cause Analysis
- Issue Elimination and Reporting
- Confirmation of Incident Neutralization

Throughout the entire lifecycle of the incident, the Field Effect team will provide support via phone, email and via status updates. You will also have access to a dedicated portal to view our AROs reporting, providing clear Actions, Recommendations, and Observations to follow based on your cyber security situation.

Phase	Actions and deliverables from the field effect team
Issue Identification	▪ Immediately deploy the technology required to begin analysis ▪ Acquire the data needed for analysis ▪ Identify the nature of the incident ▪ Perform initial containment steps
Root Cause Analysis	▪ Perform required analysis on appropriate forensic data, including partition, file system, operating system artifact, application artifact, and file analysis ▪ Look for evidence of sensitive data loss ▪ Tailor the threat monitoring based on the tools and techniques used by the attacker(s)

Issue Elimination and Reporting	▪ Provide a comprehensive report suitable for regulatory and/or statutory requirements for data loss for data loss and notification, including an Executive Summary with key findings.
	  ▪ Detailed findings of the forensics analysis and root cause
	  ▪ Detailed narrative, providing deeper understanding of the incident
	▪ A walk through of the report with the Field Effect team to ensure understanding and answer any questions
	▪ If there is not third-party insurance or legal involvement, a briefer summary can be provided
	▪ Provide detailed steps to resolve the issue and prevent it from happening again

Confirmation of Incident Neutralization	▪ Continue monitoring appropriate network(s) and/or cloud services to determine that there is no ongoing exposure, and to and to ensure there are no delays or urgent follow-up activities required ▪ Provide insight and resolution detail of all security risks discovered during monitoring ▪ Monitor to prevent future threat

Types of Incident Response

While no two incidents are exactly the same, 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.

Each Field Effect Incident Response includes three months of ongoing Convalence monitoring and protection, to ensure that the threat has been neutralized, and to highlight other vulnerabilities which require remediation.

Packages	Description	What's included
Comprehensive Covalence Incident Response	This is the most common package and includes an 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 forensic analysis of the disk or system determined to be the best source of forensics information, and analysis of the associated and relevant log(s). It may also include broad assessment of other relevant disks and logs. Finally, it includes three months of ongoing Covalence monitoring, detection, and response to ensure the threat is neutralized and to monitor for and address other threats or vulnerabilities. These findings are provided in easy to follow and actionable alerts in the form of AROs (actions, recommendations, and observations).	✕ Prepare ✓ Identify ✓ Contain ✓ Investigate ✓ Eradicate ✓ Recover
Cloud Account Covalence 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 account activity. It also includes three months of ongoing Covalence Cloud monitoring, detection, and reporting to ensure the threat is neutralized and to monitor for and address other threats or vulnerabilities. These findings are provided in easy-to-follow and actionable alerts in the form of AROs (actions, recommendations, and observations).	✕ Prepare ✓ Identify ✓ Contain ✓ Investigate ✓ Eradicate ✓ Recover

Packages	Description	What's included
Standard Covalence Incident Response	This package is applicable when some resolution steps have already been taken, and the analysis required is broad instead of deep. The aim is to ensure appropriate recovery steps have been/are being taken, and to provide protection and vulnerability assessment to monitor for and protect from further damage from the incident. The specific activities and deliverables may differ case to case, and Field Effect will work with you as appropriate to review and validate remediation action(s) taken, to highlight gaps, and to highlight other areas of vulnerability. It may include high-level analysis of the associated and relevant log(s). It also includes three months of ongoing Covalence monitoring, detection, and reporting to ensure the threat was neutralized, and to monitor for and address other threats or vulnerabilities. These findings are provided in easy to follow and actionable alerts in the form of AROs (actions, recommendations, and observations).	✕ Prepare ✕ Identify ✕ Contain ✓ Investigate ✓ Eradicate ✓ Recover

Field Effect Contact

New and existing clients can directly connect with Field Effect using the methods listed below to report an incident. Whether during business hours or not, you can expect a timely response to these critical incidents.

Contact Method	Contact Information
Web Form	https://fieldeffect.com/report-an-incident/
Email	forensics@fieldeffect.com
Phone	+1 (800) 299-8986

Start securing your business today.

Email:
letschat@fieldeffect.com

Phone:
Canada + United States
+1 (800) 299-8986

United Kingdom
+44 (0) 800 086 9176

Australia
+61 1800 431418