Cybersecurity Incident Response and Forensic Investigation Service

- Ensures that triage starts and forensic evidence is secured
- Includes proven crisis management methodologies
- Delivers consistent and proven results

Introduction

You knew it would happen someday. And that someday has arrived. A security breach has been identified by your staff and the compromise could result in a plant or process shutdown, data theft, identity theft, or even serious damage to your company's reputation. Worse yet, you realize you do not have the internal resources or expertise necessary to investigate and determine the scope of the problem. And the CEO wants answers now!

The Emerson Lifecycle Services Cybersecurity Incident Response (IR) and Forensic Investigation Service Team is ready to provide the answers your CEO wants. Staffed with some of the best and most experienced IR talent in the business and backed by elements of Trellix world-class products and services, we respond immediately to help you through your cybersecurity crisis. Our consultants provide the expertise and tools to determine what happened and how to fix it, whether your incident has affected your firewall, VPN, or even your DeltaV™ applications.

Benefits

Ensures that triage starts and forensic evidence is secured: Our first responders identify and contain the incident, offering instant remediation when appropriate. We respond immediately and help you through your crisis.

Includes proven crisis management methodologies: As part of our holistic approach to identification, containment, and remediation, we combine the skills and experience of our IR team and DeltaV specialists with the expertise of the industry's leading malware researchers at Trellix Professional Services.

Delivers consistent and proven results: Our consultants provide the expertise and tools to determine what happened and how to fix it.

EMERSON™

Service Description

After the initial cyber-incident has been triaged and contained, the clean-up and restoration of production and control remains to be dealt with. Since time is of the essence in these situations, effective, external help is often the best remedy to augment your site staff. The Emerson Cybersecurity Incident Response and Forensic Investigation Service Team stands ready to provide you the assistance you need to recover and restore your plant to full operations.

Additionally, it is also important to determine exactly what happened, how and where the incident originated, and what remediation must be taken to ensure that this attack does not happen again. That's where our forensic experts apply state-of- the-art tools and years of forensic evaluations experience to quickly analyze the data and effectively remediate your system.

Methodology

Emerson Lifecycle Services' proven IR program methodology is thorough, relevant, modular, and adaptable. An IR program touches many groups in your organization: security, IT, legal, human resources, compliance, and others. Our thorough planning approach is more effective because it is crossfunctional and inclusive of all stakeholders. We ensure your plan is relevant to your organization because we create a custom plan for each client. Our plan methodology consists of a modular framework, allowing you to choose which components are included. We produce an IR program handbook that is easy to update so that it stays evergreen. This allows you to keep your plan current as personnel, networks, and equipment change.

The Emerson Services IR Program Development is based on a seven-step process:

1. Client interviews
2. Gap analysis
3. Creation of IR documents
4. Internal IR training
5. Dry-Run exercises
6. Management presentation
7. Plan adoption and sign-off

Emerson's proven forensic investigation methodology is compliant, consistent, focused, and confidential. We stay informed of the latest legal rulings, rules of evidence handling, and industry best practices. We use proven tools and test them often. Our forensic methodology is highly refined and constantly improving, providing you consistent results in every engagement. By keeping investigations focused and specific, we also save you time and money. Above all, we maintain strict confidentiality in our forensic engagements.

The Emerson Cybersecurity Incident Response and Forensic Investigation Services framework is based on an eight-step process:

1. Determination of investigation scope and authority
2. Creation of investigative plan
3. Staff interviews
4. Forensic acquisition of electronic data
5. Strict chain-of-custody management
6. Forensic analysis of acquired data
7. Forensic reporting and follow-up
8. Expert witness/testimony, if required

Deliverables

The typical Emerson Cybersecurity Incident Response and/or Forensic Investigation Service engagement includes:

- Initial teleconferencing of security consultant(s) to begin understanding your situation;
- Dispatch of security consultant(s) to your site, if needed;
- Collaborative incident management using proven crisis management methodologies;
- Written assessment of the security breach and recommended investigation strategy;
- Written investigative findings and recommendations for remediation;
- Written remediation report if remediation services are rendered;
- Written final report containing all details of IR engagement; and
- Close-out meeting to evaluate successes and areas of improvement documented in the final report.

Scope

A typical engagement ranges from one to four weeks depending on the scope of the investigation. During the investigation, assessment and containment phases, we collaborate with you to determine if additional services are needed for remediation. A comprehensive report of findings is provided at the end of the engagement.

These services are offered on a non-Emergency approach, in other words, Emerson's Lifecycle Services cybersecurity incident response and forensics investigation services are valuable to complement an existing emergency incident response customers might already have with other service providers.

Other Related Cybersecurity Services

- Cybersecurity Policies and Procedures Site Development Service
- Incident Response Plan Development Service
- Cybersecurity Assessment Service
- Integrated Patch Management Service
- Backup and Recovery Service
- Cybersecurity Remediation Service
- Other DeltaV Cybersecurity Application Solutions include:
  - Endpoint Security For DeltaV Systems
  - Application Whitelisting For DeltaV Systems
  - Security Information And Event Management for DeltaV Systems
  - Network Security Monitor For DeltaV Systems
  - Threat Monitoring Solutions for DeltaV Systems

Ordering Information

Description	Model Number
Cybersecurity Incident Response and Forensic Investigation Services	Contact your Local Emerson Services Representative

Contact Us
www.emerson.com/contactus

EMERSON