



# CERT Development

EFFECTIVE RESPONSE

Emergency!!!

## Effective Response



## Effective Response

- Well funded, organized attackers threaten your network
- IT attacks can result in:
  - Loss of data
  - Disruption of services
  - Defacement of public Internet resources
- Business results of these attacks can be:
  - Loss of revenue
  - Loss of public confidence
  - Release of sensitive data
  - Loss of intellectual property or intelligence
  - Damage to brand

### Traditional, Preventative Approach to IT Security

**Prevent:** Implement preventative security in line with best practices

**Mitigate:** If an incident occurs, restore from backup and resume operation

#### The Problem

- Root cause and ultimate impact of incidents remains largely unknown
- Management left to guess as to the overall risk to the business from IT Security incidents
- Dedicated attackers remain undetected, and their damage unknown



## CERT Defined

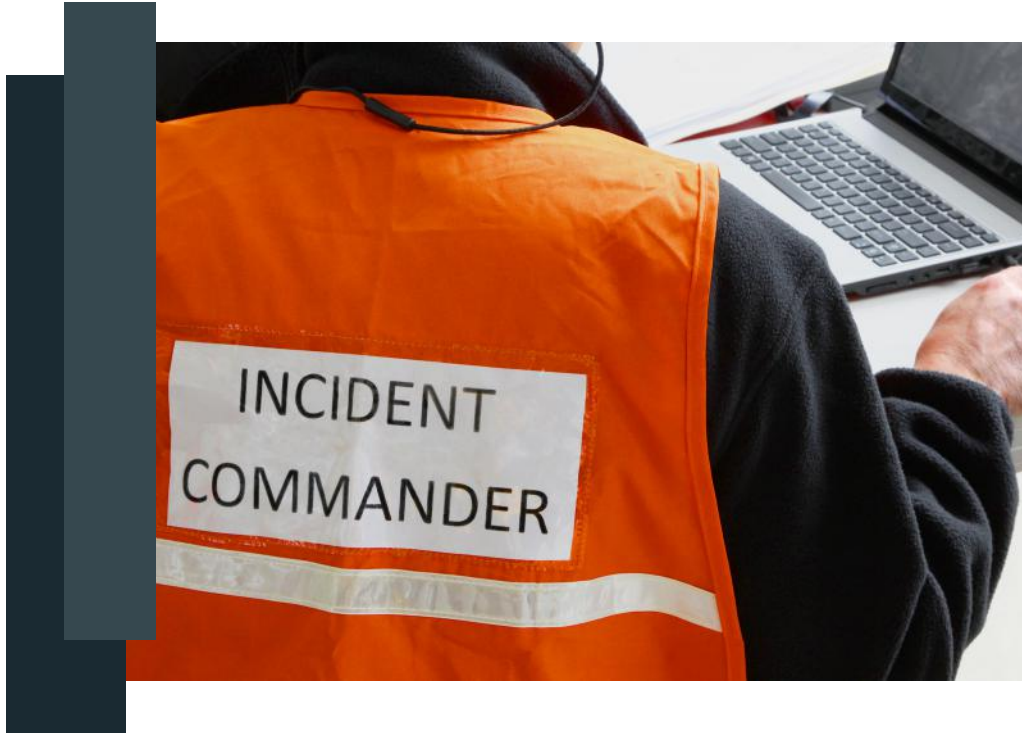
A *Computer Emergency Response Team (CERT)* or *Security Incident Response Team (SIRT)* is a unit within an information security group that is responsible for investigating and reporting on suspected information security incidents.

A CERT responds to reports of possible incidents from a Security Operations Center (SOC) and/or from users

A CERT is a second or third-tier response group that handles technical investigations into incidents



## IT Security Cycle



- CERT completes the IT Security and Risk Management Cycle
- Events are proactively investigated
- Results are used to dynamically adjust security efforts
- Impact and risk can more accurately be measured

### Reasons for a CERT

- Minimize the negative impact of security incidents
- Promote compliance with IT usage policies
- Track and understand incidents to aid in future prevention and detection
- Provide advisories to IT security and IT user base about new and potential threats
- Quantify loss and risk from security incidents
- Detect and deter advanced threats

## CERT Capabilities



- Root cause analysis, to understand where security failures occurred, so that they can be corrected
- Generate alerts and advisories to users of IT systems
- Notify SOC staff of new threats to aid detection efforts
- Notify IT staff of potential security vulnerabilities
- Provide metrics to assess loss and risk from incidents
- Report critical findings or failures to management



## Tools



A variety of tools will be needed to support a CERT

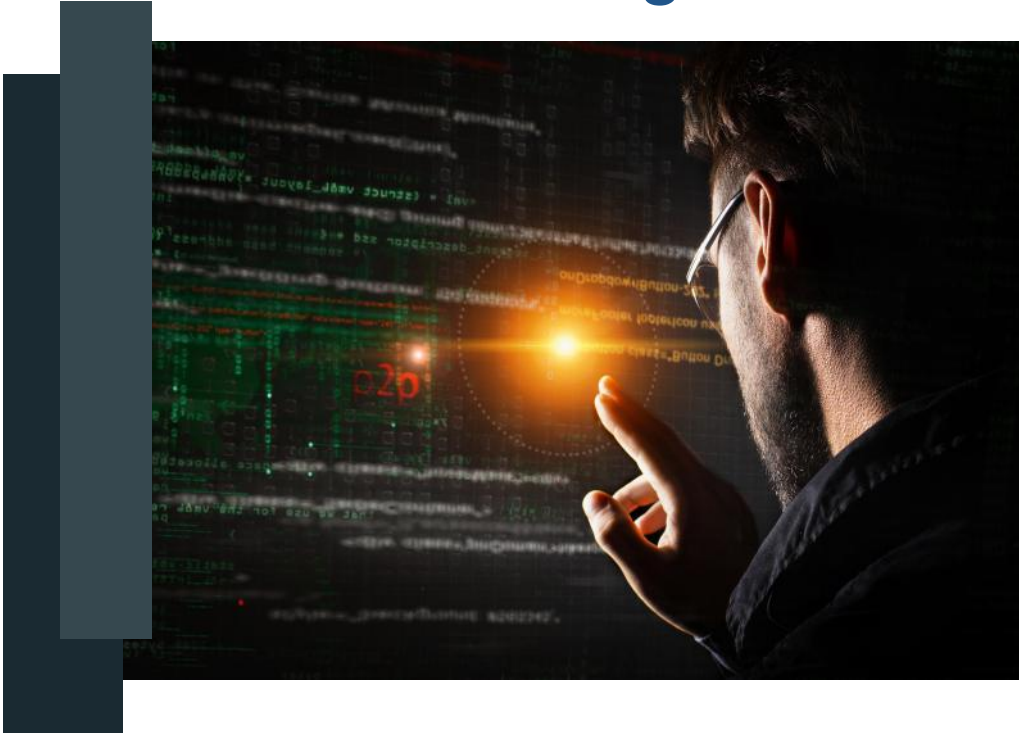
- Centralized Logging
- Automated Detection
- Intelligence Feed System
- Incident Tracking System
- Network Monitoring
- Enterprise Forensic System

### **Policies and Procedures**


- Must be repeatable, remain nimble so as to enable rapid response, be forensically sound, maintain defensible evidence, and be in line with relevant standards
- Should adopt relevant requirements from ISO 17025, ISO 27035 and organizational policies and procedures
- Should define clear authorizations and reporting lines to ensure correct distribution of sensitive material

An icon representing training, showing three stylized human figures with a line graph above them.

## Training



Training will be required in a number of disciplines for all team members

- Network Fundamentals
  - Incident Handling
  - Log Analysis
  - Network Monitoring
  - Malware Analysis
  - Forensic Collection and Analysis
  - Penetration Testing
- 
- A dark grey rectangular redaction box covering text at the bottom of the page.



## Summary

- Today's attackers are investing in stealing your data
  - You must invest in protecting it
  - Modern IT Security must be **PROACTIVE** not merely **PREVENTATIVE**
  - Implementing a CERT to investigate anomalies on your network is the most effective way to address the current and future threats
  - Feedback from a CERT provides quantifiable data to identify and assess risks to your organization, allowing informed business decisions
- 