**🛡️ The Role of CSIRT in an Organization**

**(Computer Security Incident Response Team)**

**Level:** Beginner | **Category:** Incident Handling / Cyber Defense

**🧠 What is CSIRT?**

CSIRT stands for **Computer Security Incident Response Team**.  
It’s a **special team** in an organization that **responds to cybersecurity incidents** like hacking, malware, phishing, etc.

Think of it like the **emergency squad** for computer-related attacks!

**🔍 Why is CSIRT Needed?**

Organizations get attacked all the time.

A CSIRT helps:

* 🔒 **Protect sensitive data**
* 🛠️ **Fix breaches quickly**
* 📢 **Communicate clearly** during incidents
* 📄 **Maintain evidence** for legal use
* 📊 **Prevent future attacks**

**👨‍💼 What Does CSIRT Do? (Main Roles)**

| **Role** | **What it Means** |
| --- | --- |
| **🕵️ Detection** | Spotting signs of attack or suspicious behavior |
| **🚨 Response** | Taking quick actions (block, isolate, alert) |
| **🔍 Investigation** | Finding out how the attack happened |
| **🧪 Containment** | Stopping the attack from spreading |
| **🔧 Recovery** | Restoring systems, cleaning malware |
| **📂 Reporting** | Writing reports for management or legal teams |
| **📚 Lessons Learned** | Improving defenses after incidents |

**🧰 Example Scenario: CSIRT in Action**

1. Alert from firewall: “Unusual login from Russia”
2. CSIRT investigates → finds malware on server
3. They isolate the server from network
4. Remove malware and recover system from backup
5. Log everything for legal and future reference
6. Train staff to avoid phishing (if that was the cause)

✅ Quick action = less damage = better protection

**🧩 FIRST.org and CSIRT**

**FIRST** = Forum of Incident Response and Security Teams

It’s a **global organization** that connects and certifies CSIRTs.

* Provides **best practices**
* Supports **international cooperation**
* Helps new CSIRTs become **trusted and professional**

👉 You can check out their resources at [https://www.first.org](https://www.first.org/)

**🧠 Summary Table**

| **Topic** | **Description** |
| --- | --- |
| **CSIRT** | A team that responds to cyberattacks |
| **Goal** | Detect, respond, investigate, recover |
| **Works with** | SOC, IT, Legal, Management |
| **Supported by** | FIRST.org for global standards |