Ciscos approach to cybersecurity

Ciscos CSIRT

Computer security incident response team

Receive, review and respond to security incident reports

Security playbook

One of the best ways to prepare for a security breach is to prevent it

Organizations should provide guidance on:

- How to identify the cybersecurity risk to system, asets, data and capabilities

- the implementation of safeguards and personnel training

- flexible response plan that minimizes the impact and dmg. in the event of breach

- security measures and processes that need to be put in place in the aftermath

Tools for incident detection and prevention

SIEM

- **Security information and event management**

- system collects and analyzes security alerts, logs and other real-time and historical   
 data from security devices in the network to facilitate early detec. of cyber attacks

DLP

- **Data loss prevention**

- system is designed to stop sensitive data from being stolen from or escaping a   
 network

- it monitors and protects data in three different states:  
 data in use   
 data in motion  
 data at rest

IPS

- **can block or deny traffic based in a positive rule or signature match**

IDS  
 - **scans data against a database of rules or attack signatures, looking for malicious   
 traffic**