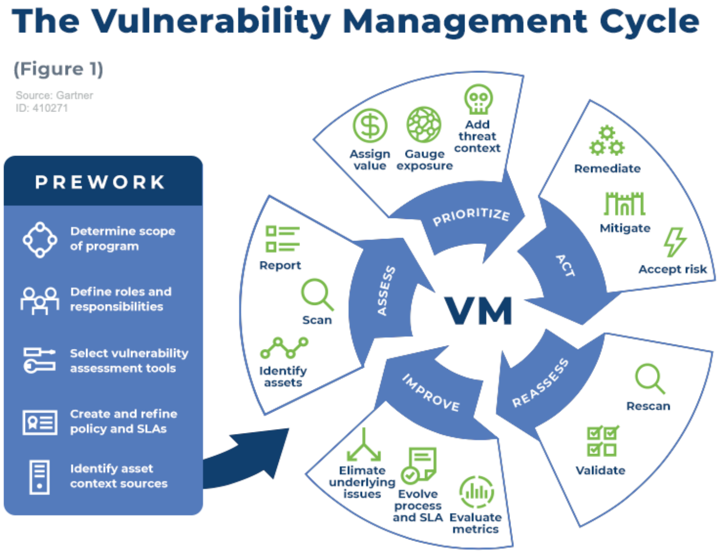
Vulnerability management

Vulnerability management is a cyclical process of identifying, assessing, remediating and reporting vulnerabilities and threats in a network. Vulnerabilities and threats require a different response depending on the type.
Vulnerability management is a strategy that organizations can use to track, minimize, and eradicate vulnerabilities in their systems. This process involves identifying and classifying vulnerabilities, so that appropriate protections or remediations can be applied.



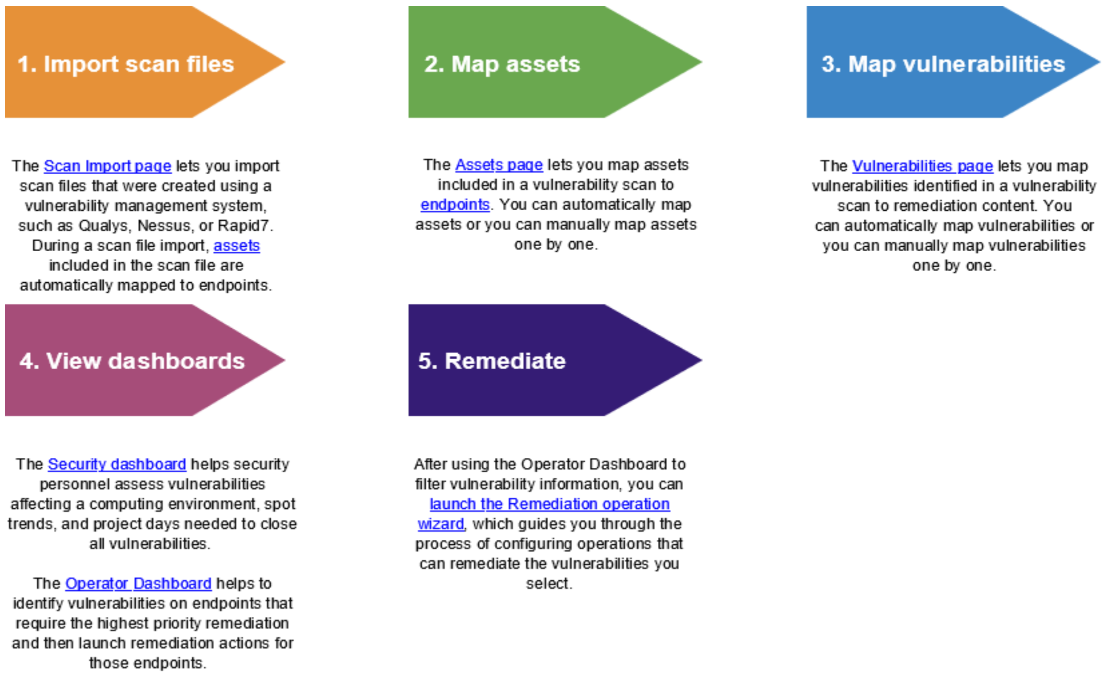
The Vulnerability Management Cycle

(Figure 1)

Source: Gartner
ID: 410271

The 4 stages of vulnerability management:

- **Identify vulnerabilities** - The first stage of the management process requires identifying which vulnerabilities might affect your systems. Once you know which vulnerabilities or vulnerability types you are looking for, you can begin identifying which ones exist.
  The first stage of the management process requires identifying which vulnerabilities might affect your systems. Once you know which vulnerabilities or vulnerability types you are looking for, you can begin identifying which ones exist.
- **Evaluating vulnerabilities** - After you have identified all possible vulnerabilities in your system, you can begin evaluating the severity of the threats. This evaluation helps you prioritize your security efforts and can help reduce your risks more quickly.
  One system is the Common Vulnerability Scoring System (CVSS). This is a standardized system used by many vulnerability databases and researchers. CVSS evaluates the level of vulnerability according to inherent characteristics, temporal traits, and the specific effect of the vulnerability to your systems.
- **Remediating vulnerabilities** - With a prioritized vulnerability management plan in place, you can begin your remediation efforts. During this phase, you may also want to increase monitoring or reduce access to areas identified as at-risk. This can help prevent successful exploitation of vulnerabilities until you can apply patches or permanently increase protections to those areas.
  After vulnerabilities are addressed, make sure that you verify successful remediation. It can also help you ensure that new vulnerabilities weren't created during your remediation efforts.
- **Reporting vulnerabilities** - Reporting vulnerabilities after remediation may seem unnecessary, but it can help you improve your security and responses in the future. Having a record of vulnerabilities and when those issues were fixed shows accountability for security and is required for many compliance standards. It can also be useful when investigating future events. For example, if you find evidence that an attack has been ongoing, you can look at your patch histories to narrow down possible routes and times of entry.



The Scan Import page lets you import scan files that were created using a vulnerability management system, such as Qualys, Nessus, or Rapid7. During a scan file import, assets included in the scan file are automatically mapped to endpoints.

The Assets page lets you map assets included in a vulnerability scan to endpoints. You can automatically map assets or you can manually map assets one by one.

The Vulnerabilities page lets you map vulnerabilities identified in a vulnerability scan to remediation content. You can automatically map vulnerabilities or you can manually map vulnerabilities one by one.

The Security dashboard helps security personnel assess vulnerabilities affecting a computing environment, spot trends, and project days needed to close all vulnerabilities.

The Operator Dashboard helps to identify vulnerabilities on endpoints that require the highest priority remediation and then launch remediation actions for those endpoints.

After using the Operator Dashboard to filter vulnerability information, you can launch the Remediation operation wizard, which guides you through the process of configuring operations that can remediate the vulnerabilities you select.

Why do you need a vulnerability management process?

Vulnerabilities provide openings for attackers to enter your systems. Once inside, they can abuse resources, steal data, or deny access to services. If you do not identify and patch vulnerabilities, you are essentially leaving the doors and windows open for attackers to enter your network.
Vulnerability management programs provide structured guidelines to help you evaluate and secure your network. Rather than ignoring vulnerabilities or taking the risk of vulnerabilities being overlooked, this process can help you conduct a thorough search.

Using vulnerability management data with a next-generation SIEM

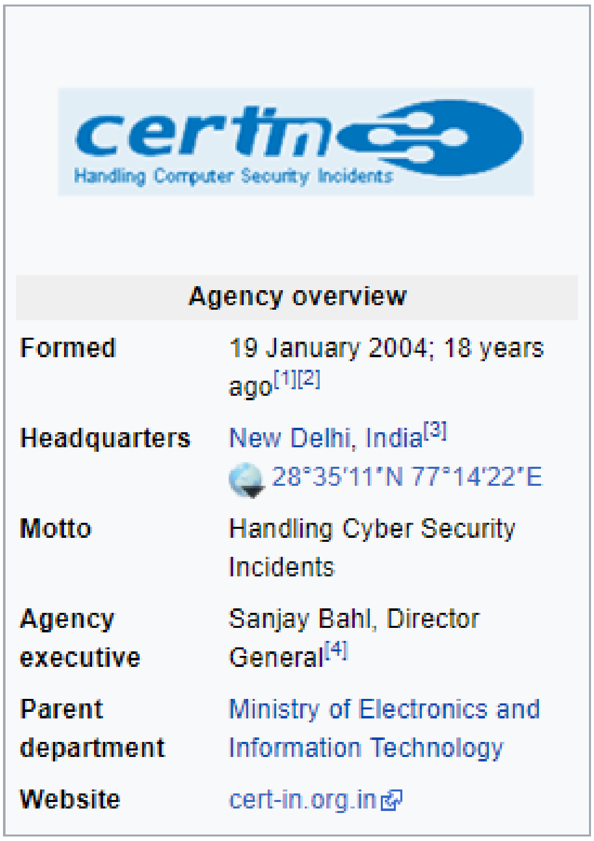
Vulnerability management log data has great value when combined with security and network logs and analysed in a next generation SIEM, such as the Exabeam Security Management Platform:
Critical assets which are vulnerable but currently unable to be patched can be added to a watch list, providing security operations teams with a clear view into any risky activities occurring on those systems.
Data from vulnerability scans can be included in Exabeam Smart Timelines, providing security analysts with an automated end-to-end picture of events.
Device information can be enriched with Exabeam’s threat intelligence data, enabling security operations teams to understand specific external threat indicators related to their environment.
The following Exabeam modules and functionality can be used to analyse and enrich data from vulnerability management tools:
Advanced analytics — using behavioral analytics to identify anomalous behavior that might indicate an attack, and correlating with threat analytics data to identify the type and source of the attack
Cloud connectors — can be used to easily collect data from a number of popular cloud-based vulnerability management solutions
Smart forensic analysis — collecting all relevant information about a security incident, across multiple users, IP addresses, and IT systems, combining it with threat intelligence data, and laying it out on an incident timeline
Incident response automation — gathering data from hundreds of tools, automatically identifying incidents, cross-referencing them with threat intelligence data, and even automatically orchestrating containment and mitigation steps
Threat hunting — using threat intelligence data combined with free exploration of internal security data to identify new and unknown threats that might be affecting your organization

CERT

CERT: Computer Emergency Response Team
(CERT-IN)

It is the nodal agency to deal with cyber security threats like hacking and phishing. It strengthens security-related defence of the Indian Internet domain.

CERT-In (the Indian Computer Emergency Response Team)



Agency overview

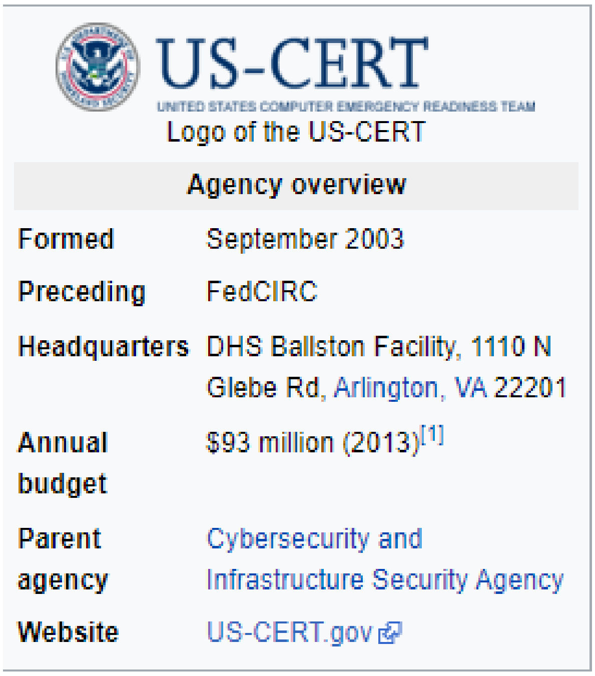
Formed	19 January 2004; 18 years ago[1][2]
Headquarters	New Delhi, India[3] 28°35′11″N 77°14′22″E
Motto	Handling Cyber Security Incidents
Agency executive	Sanjay Bahl, Director General[4]
Parent department	Ministry of Electronics and Information Technology
Website	cert-in.org.in

In December 2013, CERT-In reported there was a rise in the cyber-attacks on Government organisations like banking and finance, oil and gas and emergency services. It issued a list of security guidelines to all critical departments. It liaisons with Office of National Cyber Security Coordinator, National Security Council and National Information Board in terms of the nation's cyber security and threats.

CERT-In (the Indian Computer Emergency Response Team) is a government-mandated information technology (IT) security organization. The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

US CERT United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team is an organization within the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency. Specifically, US-CERT is a branch of the Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center.



Logo of the US-CERT

Agency overview	
Formed	September 2003
Preceding	FedCIRC
Headquarters	DHS Ballston Facility, 1110 N Glebe Rd, Arlington, VA 22201
Annual budget	$93 million (2013)[1]
Parent agency	Cybersecurity and Infrastructure Security Agency
Website	US-CERT.gov

DHS's first Director of the National Cyber Security Division created the United States Computer Emergency Readiness Team (US-CERT) in September 2003 to protect the Internet infrastructure of the United States by coordinating defense against and responding to cyber-attacks.

US-CERT is the 24-hour operational arm of the NCCIC which accepts, triages, and collaboratively responds to incidents, provides technical assistance to information system operators, and disseminates timely notifications regarding current and potential security threats, exploits, and vulnerabilities to the public via its National Cyber Awareness System (NCAS).

Threat Analysis and information sharing

This feature is involved with reviewing, researching, vetting and documenting all Computer Network Defense (CND) attributes which are available to US-CERT, both classified and unclassified.

Digital analytics

This feature conducts digital forensic examinations and malware artifact analysis (reverse engineering) to determine attack vectors and mitigation techniques, identifies possible threats based on analysis of malicious code and digital media, and provides indicators to mitigate and prevent future intrusions

Operations

This feature informs the CND community on potential threats which allows for the hardening of cyber defense, as well as, develops near real-time/rapid response community products.

Communications

This feature supports NCCIC information sharing, development, and web presence. It is responsible for establishing and maintaining assured communications, developing and disseminating information, products, and supporting the development and maintenance of collaboration tools.

International

This feature partners with foreign governments and entities to enhance the global cybersecurity defense posture. It supports bilateral engagements, such as CERT-to-CERT information sharing/trust building activities, improvements related to global collaboration, and agreements on data sharing standards.