Wikipedia
The Free Encyclopedia

Blue team (computer security)

A **blue team** is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and make certain all security measures will continue to be effective after implementation.[1]

Some blue team objectives include:

- Using risk intelligence and digital footprint analysis to find and fix vulnerabilities and prevent possible security incidents.
- Conduct regular security audits such as incident response and recovery.[2]

History

As part of the United States computer security defense initiative, red teams were developed to exploit other malicious entities that would do them harm. As a result, blue teams were developed to design defensive measures against such red team activities.[3]

Incident response

If an incident does occur within the organization, the blue team will perform the following six steps to handle the situation:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned[4]

Operating system hardening

In preparation for a computer security incident, the blue team will perform hardening techniques on all operating systems throughout the organization.[5]

Perimeter defense

The blue team must always be mindful of the network perimeter, including traffic flow, packet filtering, proxy firewalls, and intrusion detection systems.[5]

Tools

Blue teams employ a wide range of tools allowing them to detect an attack, collect forensic data, perform data analysis and make changes to thwart future attacks and mitigate threats. The tools include:

Log management and analysis

- AlienVault
- Graylog
- InTrust
- LogRhythm
- Microsoft Sentinel
- NetWitness
- Rapid7
- SolarWinds
- Splunk

Security information and event management (SIEM) technology

SIEM software supports threat detection and security incident response by performing real-time data collection and analysis of security events. This type of software also uses data sources outside of the network including indicators of compromise (IoC) threat intelligence.

See also

- List of digital forensics tools
- Vulnerability management
- White hat (computer security)
- Red team

References

1. Sypris Electronics. "DoDD 8570.1: Blue Team" (https://web.archive.org/web/20160425120250/https://www.sypriselectronics.com/information-security/cyber-security-solutions/computer-network-defense/). *Sypris Electronics*. Archived from the original (https://www.sypriselectronics.com/information-security/cyber-security-solutions/computer-network-defense/) on April 25, 2016. Retrieved July 3, 2016.
2. "What is Blue Team? | IBM" (https://www.ibm.com/topics/blue-team). *www.ibm.com*. 2023-12-14. Retrieved 2024-09-07.
3. Johnson, Rowland. "How your red team penetration testers can help improve your blue team" (https://web.archive.org/web/20160530230034/http://www.scmagazineuk.com/how-your-red-team-penetration-testers-can-help-improve-your-blue-team/article/431023/). *SC Magazine*. Archived from the original (http://www.scmagazineuk.com/how-your-red-team-penetration-testers-can-help-improve-your-blue-team/article/431023/) on May 30, 2016. Retrieved July 3, 2016.
4. Murdoch, Don (2014). *Blue Team Handbook: Incident Response Edition* (2nd ed.). reateSpace Independent Publishing Platform. ISBN 978-1500734756.

5. SANS Institute. "Cyber Guardian: Blue Team" (https://www.sans.org/cyber-guardian/blue-team). *SANS*. SANS Institute. Retrieved July 3, 2016.