2023

GREEN CIRCLE

be aware..be secure

(All About Penetration Testing)

Preparation: (Eng_Obaida Zomot)

Reviewed By: Mohammad Alkhudari
@Jun-2023.
Green Circle
info@grcico.com

Table of content:

Penetration Testing

(introduction)

Penetration testing, often referred to as "pentesting," is a proactive security assessment technique that evaluates the security of a computer system, network, or application. It involves simulating real-world attacks on a target system to identify vulnerabilities, weaknesses, and potential entry points that malicious attackers could exploit.

Penetration testing, often referred to as "pen testing," is a cybersecurity practice that involves assessing the security of computer systems, networks, or web applications by simulating real-world attacks. The purpose of penetration testing is to identify vulnerabilities and weaknesses in a system's defenses before malicious hackers can exploit them.
During a penetration test, a skilled ethical hacker, known as a penetration tester or "pen tester," attempts to exploit security vulnerabilities in the target system. This can involve various techniques, such as network scanning, vulnerability scanning, social engineering, or attempting to bypass security controls. The goal is to uncover potential entry points that could be exploited by attackers and provide recommendations for improving the overall security posture.

Penetration testing is typically conducted in a controlled and authorized manner to ensure that the testing activities do not disrupt or harm the target systems. The results of a penetration test are compiled into a report, which outlines the vulnerabilities discovered, the potential impact they could have, and recommendations for mitigating or addressing those vulnerabilities.

Overall, penetration testing is a critical component of a comprehensive cybersecurity strategy, helping organizations identify and address security weaknesses proactively, reduce the risk of unauthorized access or data breaches, and improve their overall security defenses.

Penetration testing typically follows a defined methodology, which involves various stages:

1. **Planning and reconnaissance:** This phase involves understanding the target system, identifying potential entry points, and gathering information about the system's architecture, network infrastructure, and applications.

2. **Scanning:** In this stage, pentesters use automated tools to scan the target system or network for known vulnerabilities, open ports, and misconfigurations. This helps in identifying possible attack vectors.

3. **Gaining access:** Once potential vulnerabilities are identified, pentesters attempt to exploit them to gain unauthorized access to the system. This may involve attempting to exploit software vulnerabilities, weak passwords, misconfigurations, or social engineering techniques.

4. **Maintaining access:** Once access is obtained, pentesters try to maintain control over the compromised system, similar to what a real attacker would do. This step helps to assess the extent of damage an attacker could cause if they were to gain access.

5. **Analysis and reporting:** After completing the penetration testing activities, the pentesters analyze the results, identify security weaknesses, and document their findings. They provide a comprehensive report detailing the vulnerabilities discovered, the impact they could have, and recommendations for remediation.

(Planning and reconnaissance)

Planning and reconnaissance are critical stages in penetration testing. They involve gathering information about the target system, understanding its architecture, network infrastructure, and applications, and identifying potential entry points and attack vectors. Here's a breakdown of these stages:

1. **Define the scope:** Clearly define the scope of the penetration test, including the systems, networks, and applications to be tested. Determine the objectives, limitations, and specific goals of the test.

2. **Obtain authorization:** Ensure that you have proper authorization from the organization or individuals who own or manage the target system. Unauthorized testing is illegal and can lead to severe consequences.

3. **Information gathering:** Collect as much information as possible about the target system. This includes researching the organization, its employees, technologies used, public-facing systems, and any available documentation. Publicly available information, such as DNS records, WHOIS data, and online presence, can be useful.

4. **Network reconnaissance:** Identify the IP addresses, subnets, and network topology of the target system. Use tools like network scanners, port scanners, and network mapping tools to discover open ports, services, and devices.

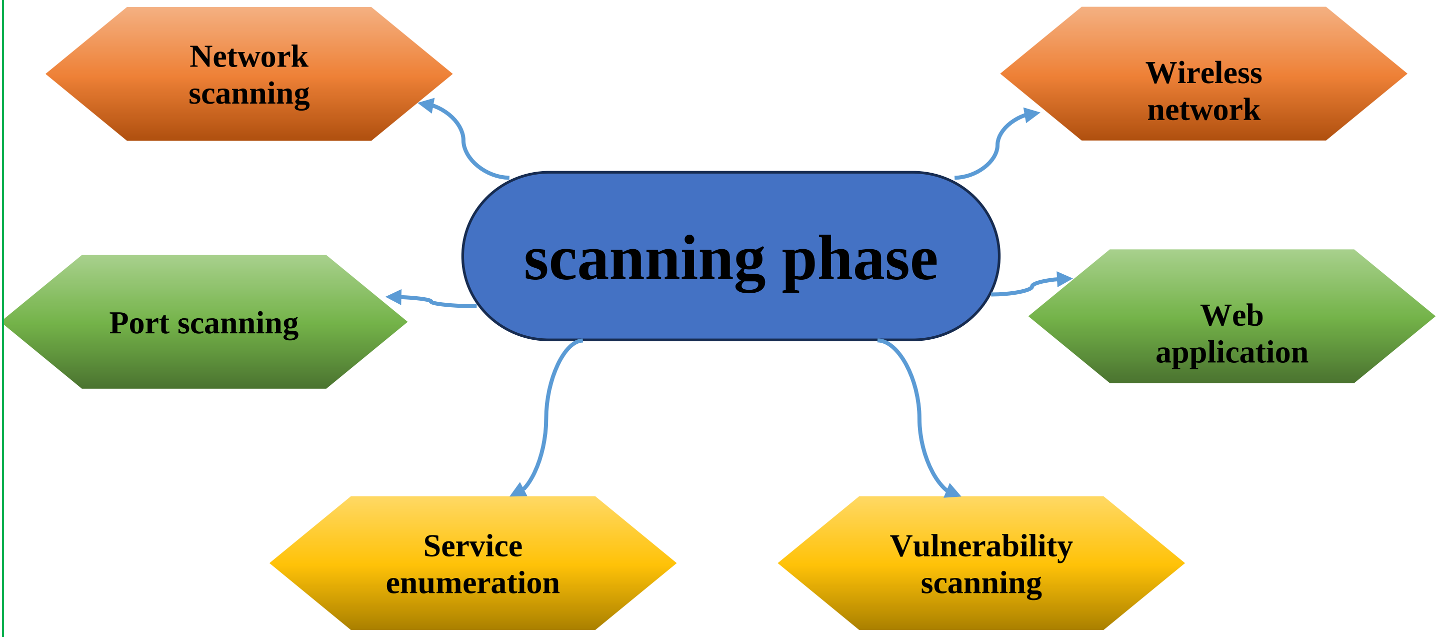
5. **Application reconnaissance:** Analyze the target's web applications, mobile apps, or any other software in scope. Identify the technologies and frameworks used, potential vulnerabilities, and known security issues. Tools like web application scanners, HTTP intercepting proxies, and code review can aid in this phase.

6. **Vulnerability assessment:** Perform vulnerability scanning to identify known vulnerabilities in the target system. Utilize automated tools like vulnerability scanners, which can help identify common weaknesses and misconfigurations.

7. **Threat modeling:** Based on the information gathered, analyze potential threats and prioritize them based on their impact and likelihood. This helps in focusing the penetration testing efforts on the most critical areas.

8. **Establish rules of engagement:** Clearly define the rules and limitations of the penetration test, including the testing schedule, test scenarios, and the boundaries of what can and cannot be tested. Ensure that any potential impact on the production environment is minimized.

(Scanning)



Scanning is an important phase in penetration testing where you perform active reconnaissance and scanning techniques to identify vulnerabilities, open ports, and potential entry points in the target system. It involves using various tools and techniques to gather more specific information about the system's security posture. Here's an overview of the scanning phase:

1. **Network scanning:** Use network scanning tools, such as Nmap or Nessus, to discover active hosts, open ports, and services running on the target network. Network scanning helps identify potential attack vectors and entry points into the system.

2. **Port scanning:** Conduct port scanning to determine which ports are open and listening on the target system. Port scanning tools like Nmap can help identify open ports and the services associated with them. This information helps in understanding the po scanning phasetential services that may be accessible and vulnerable.

3. **Service enumeration:** Once open ports are identified, perform service enumeration to gather more details about the running services. Tools like Nmap or banner grabbing techniques can provide information about the service versions, configurations, and potential vulnerabilities associated with each service.

4. **Vulnerability scanning:** Utilize vulnerability scanning tools, such as Nessus, OpenVAS, or Qualys, to automatically identify known vulnerabilities in the target system. These tools match the discovered services and their versions against a

database of known vulnerabilities. They generate reports that highlight the vulnerabilities, their severity, and potential remediation steps.

5. **Web application scanning:** If web applications are within the scope of the penetration test, perform web application scanning using tools like Burp Suite, OWASP ZAP, or Acunetix. These tools help identify common web application vulnerabilities like SQL injection, cross-site scripting (XSS), or insecure server configurations.

6. **Wireless network scanning:** In cases where wireless networks are part of the test, conduct wireless scanning to identify accessible networks, their encryption mechanisms, and potential weaknesses. Tools like Aircrack-ng or Kismet can assist in wireless network scanning.

Scanning provides valuable insights into the target system's vulnerabilities and helps prioritize areas for further exploitation and testing. However, it's important to conduct scanning activities responsibly, adhering to the rules of engagement and any legal or ethical

considerations. Unauthorized scanning or exploitation attempts on systems without proper authorization can have severe consequences.

(Maintaining access)

Maintaining access is a stage in penetration testing where the objective is to maintain control over a compromised system or network, simulating the actions of a real attacker. By maintaining access, penetration testers can assess the potential damage an attacker could cause and evaluate the system's ability to detect and respond to unauthorized access. Here are some key aspects of maintaining access in penetration testing:

1. **Persistence:** Establish persistence on the compromised system to ensure continued access even after the initial breach. This involves techniques like creating backdoors, installing rootkits, modifying system configurations, or creating rogue user accounts.

2. **Privilege escalation**: Attempt to elevate privileges on the compromised system to gain higher levels of access and control. This can involve exploiting vulnerabilities, misconfigurations, or weak access controls to escalate privileges from a regular user to an administrator or system-level access.

3. **Data exfiltration:** Simulate the extraction of sensitive data from the compromised system, if within the scope of the engagement. This helps assess the potential impact of a successful attack and evaluate the effectiveness of data loss prevention mechanisms.

4. **Maintaining stealth:** Actively work to avoid detection by system administrators or security monitoring tools while maintaining access. This can involve techniques like

disabling or evading security controls, hiding files or processes, and obfuscating network traffic to remain undetected.

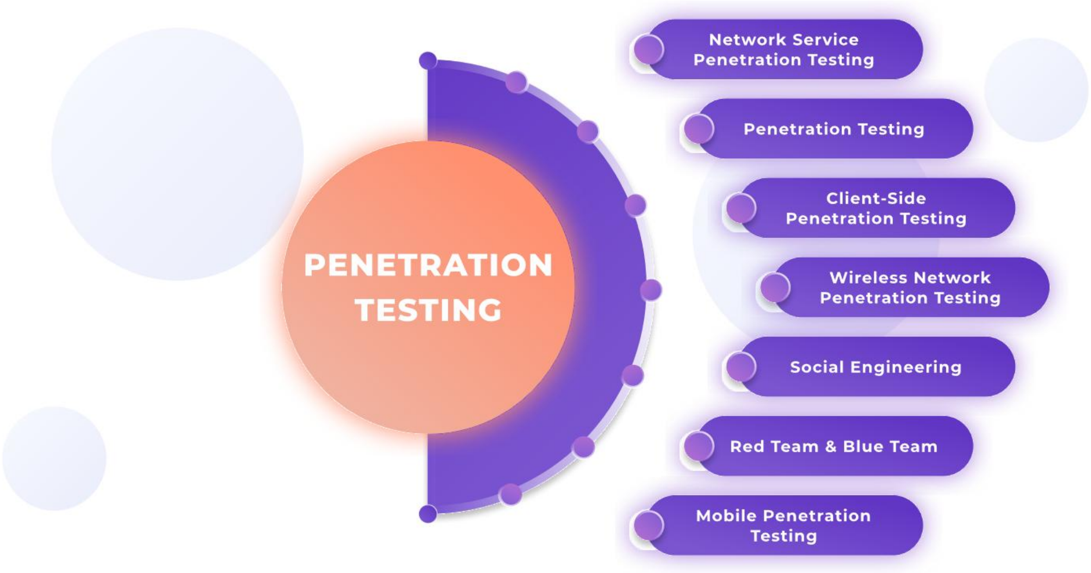
5. **Lateral movement:** Explore the possibility of moving laterally within the network to gain access to other systems or resources. This can involve exploiting vulnerabilities or weak credentials to pivot from one system to another, mimicking an attacker's lateral movement.

6. **Interaction with target environment:** Interact with the compromised system as an attacker would, performing activities that may include reconnaissance, privilege escalation attempts, data manipulation, or deploying additional tools or malware for further exploitation.

7. **Monitoring and documenting actions:** Keep track of the actions performed during the maintenance of access phase. This helps in documenting the steps taken, the level of access achieved, and the potential risks associated with the compromised system.

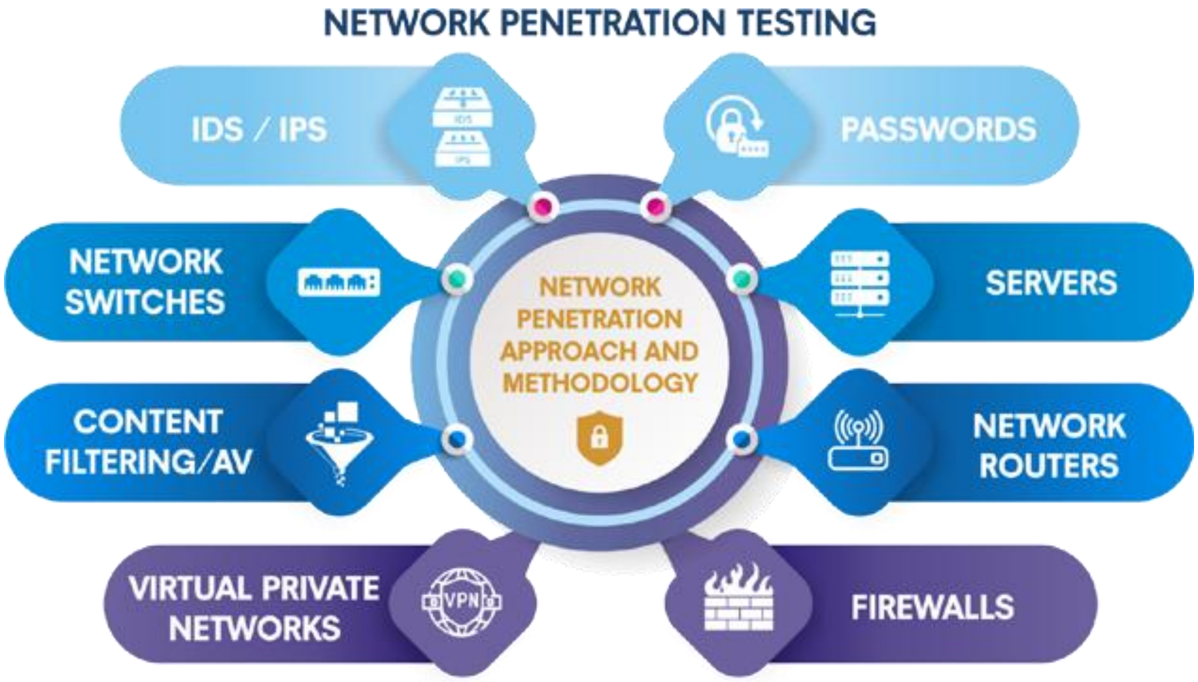
It's crucial to conduct the maintaining access phase with extreme caution and care. Penetration testers must strictly adhere to the rules of engagement and ensure that the activities do not cause any harm to the target system or network. The goal is to assess the

(types penetration Testing)


PENETRATION TESTING
Network Service Penetration Testing
Penetration Testing
Client-Side Penetration Testing
Wireless Network Penetration Testing
Social Engineering
Red Team & Blue Team
Mobile Penetration Testing

1. **Network Service Penetration Testing.**
2. **Web Application Penetration Testing.**
3. **Wireless Network Penetration Testing.**
4. **Social Engineering.**
5. **clintent side Penetration Testing.**
6. **Wireless Security Assessment.**
7. **Red Team Testing.**
8. **Mobile Penetration Testing.**

(Network Penetration Testing)



Network penetration testing, also known as network security testing or infrastructure testing, focuses on evaluating the security of a network infrastructure. It aims to identify vulnerabilities and weaknesses in network devices, protocols, configurations, and associated systems. The goal is to assess the overall security posture of the network and identify potential entry points for unauthorized access or attacks. Here's an overview of network penetration testing:

1. **Network reconnaissance:** Gather information about the target network, including IP ranges, network topology, DNS information, and publicly available information. This helps in understanding the network layout and potential entry points.

2. **Network scanning:** Conduct network scanning to identify active hosts, open ports, and services running on the network. This includes using tools like Nmap, Nessus, or OpenVAS to discover potential vulnerabilities, misconfigurations, or weak points in network devices and services.

3. **Vulnerability assessment:** Utilize vulnerability scanning tools to identify known vulnerabilities in network devices, such as routers, switches, firewalls, and intrusion

detection systems (IDS). The goal is to detect weaknesses that can be exploited to gain unauthorized access or disrupt network operations

4. **Exploitation:** Once potential vulnerabilities are identified, attempt to exploit them to gain unauthorized access to network devices or systems. This can involve exploiting weak passwords, misconfigurations, known vulnerabilities, or weak access controls.

5. **Privilege escalation:** If access is obtained to a network device or system, attempt to escalate privileges to gain higher levels of access and control. This includes exploiting vulnerabilities or weak configurations to elevate privileges and access sensitive information or perform unauthorized actions.

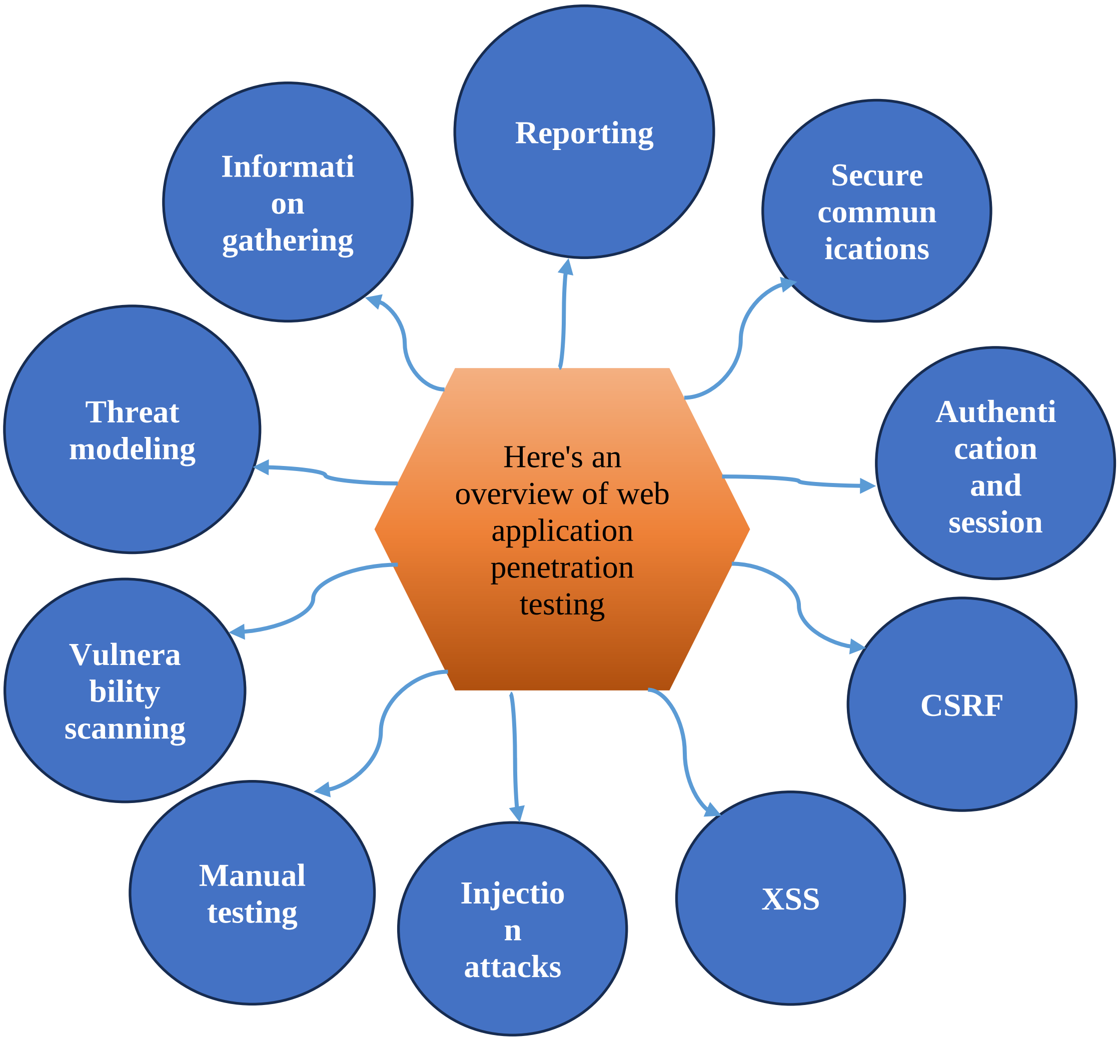
6. **Network traffic analysis:** Analyze network traffic to identify potential security risks, such as unencrypted or insecure protocols, suspicious network activities, or unauthorized data transfers. Tools like Wireshark or tcpdump can be used for network packet analysis.

7. **Firewall and intrusion detection testing:** Assess the effectiveness of firewalls and intrusion detection systems (IDS) by attempting to bypass or circumvent them. This includes testing rule sets, filtering mechanisms, and intrusion detection capabilities to determine if they can effectively detect and prevent unauthorized access attempts.

8. **Reporting:** Document the findings, including identified vulnerabilities, their impact, and recommended remediation steps. Provide a comprehensive report outlining potential risks and suggestions for improving the network's security.

Network penetration testing helps organizations identify weaknesses in their network infrastructure and take proactive measures to enhance security. It assists in preventing unauthorized access, protecting sensitive information, and ensuring the integrity and availability of network resources.

(Web Application Penetration Testing)



Web application penetration testing, also known as web application security testing, focuses specifically on assessing the security of web applications. It involves identifying vulnerabilities, weaknesses, and potential entry points in web applications that could be exploited by malicious attackers. The goal is to evaluate the application's security posture, identify vulnerabilities, and provide recommendations for improving its security. Here's an overview of web application penetration testing:

1. **Information gathering:** Gather information about the target web application, including its URL, technologies used, functionality, and any available documentation. Understand the application's architecture, user roles, and data flows.

2. **Threat modeling:** Analyze the web application to identify potential threats and attack vectors. Understand the application's attack surface, such as input fields, authentication mechanisms, session management, and data handling processes.

3. **Vulnerability scanning:** Utilize automated web vulnerability scanning tools, such as Burp Suite, OWASP ZAP, or Acunetix, to identify common vulnerabilities like SQL injection, cross-site scripting (XSS), security misconfigurations, or insecure direct object references. These tools crawl through the application, testing for known vulnerabilities.

4. **Manual testing:** Perform manual testing to identify complex vulnerabilities and logic flaws that may not be detected by automated scanners. This includes testing for business logic vulnerabilities, authentication and authorization issues, session management flaws, and insecure data storage.

5. **Injection attacks:** Test for various injection vulnerabilities like SQL injection, command injection, or LDAP injection. Attempt to manipulate input fields or parameters to execute unintended commands or gain unauthorized access.

6. **Cross-Site Scripting (XSS):** Verify if the application is vulnerable to XSS attacks. Test for reflected or stored XSS by injecting malicious scripts into input fields or URLs to execute arbitrary code in users' browsers.
7. **Cross-Site Request Forgery (CSRF):** Test for CSRF vulnerabilities, where an attacker tricks authenticated users into performing unintended actions. Create malicious requests that mimic legitimate actions to validate if the application is vulnerable.

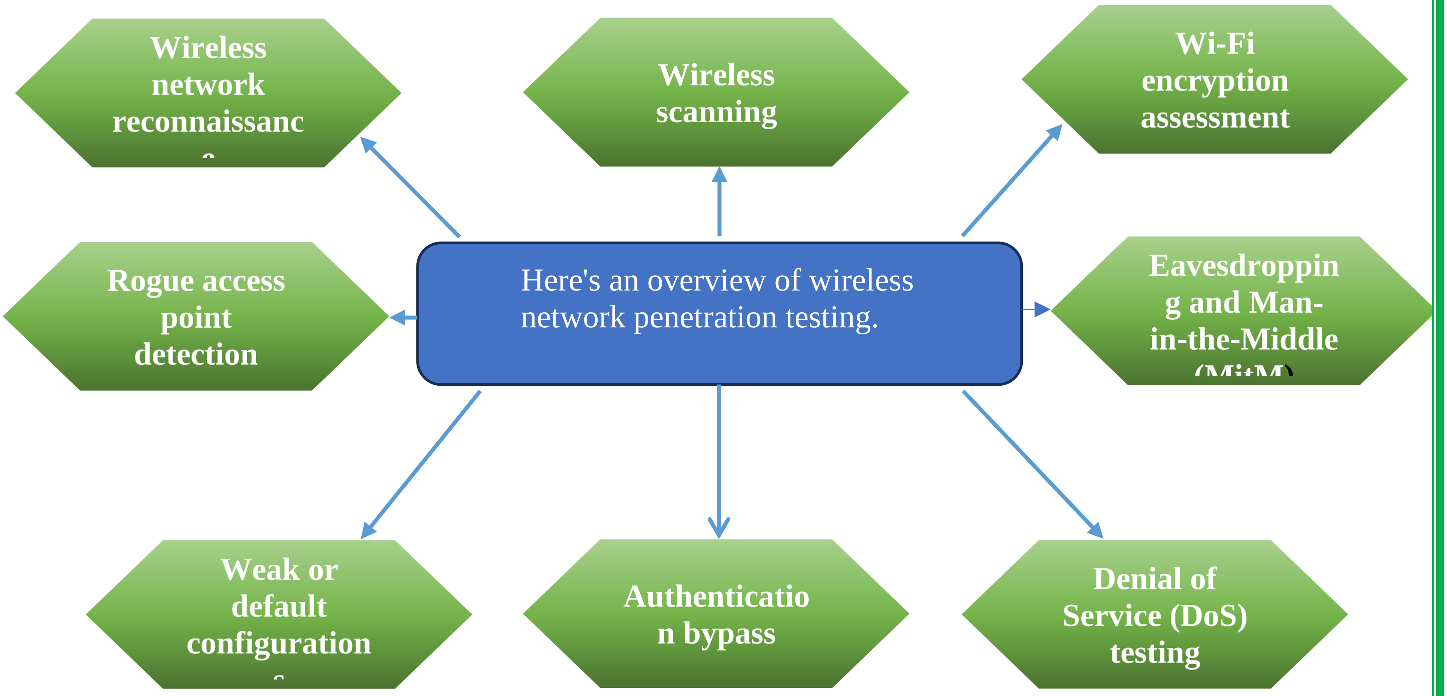
8. **Authentication and session management:** Assess the effectiveness of authentication mechanisms, password policies, and session management controls. Test for weak passwords, session fixation, session hijacking, or session replay attacks.

9. **Secure communications:** Evaluate the implementation of secure communication protocols (e.g., HTTPS) and the proper handling of sensitive data, such as credit card information or personal identifiable information (PII).

10. **Reporting:** Document the findings, including vulnerabilities discovered, their impact, and recommended remediation steps. Provide a comprehensive report to the organization, outlining potential risks and suggestions for improving the security of the web application.

Web application penetration testing helps identify and address vulnerabilities in web applications, ensuring the security and integrity of user data, preventing unauthorized access, and protecting against potential attacks. It's important to conduct web application penetration testing with proper authorization and follow ethical guidelines to ensure the security of the tested applications.

(Wireless Network Penetration Testing)


Wireless network reconnaissanc
Wireless scanning
Wi-Fi encryption assessment
Rogue access point detection
Here's an overview of wireless network penetration testing.
Eavesdroppin g and Man-in-the-Middle
Weak or default configuration
Authenticatio n bypass
Denial of Service (DoS) testing

Wireless network penetration testing, also known as wireless security testing, focuses on assessing the security of wireless networks, including Wi-Fi networks. It involves identifying vulnerabilities, weaknesses, and potential entry points in wireless networks that could be exploited by unauthorized individuals. The objective is to evaluate the security posture of the wireless network and provide recommendations for improving its security. Here's an overview of wireless network penetration testing:

1. **Wireless network reconnaissance:** Gather information about the target wireless network, including SSID (network name), encryption protocols, wireless devices, and network topology. Understand the network's layout, access points, and potential entry points.

2. **Wireless scanning:** Conduct wireless scanning to identify active wireless networks, available access points, and their characteristics. Use tools like Kismet, Airodump-ng, or NetStumbler to discover wireless networks, channels, signal strengths, and associated devices.

3. **Wi-Fi encryption assessment:** Evaluate the encryption mechanisms used by the wireless network, such as WEP, WPA, or WPA2. Test the strength of the encryption by attempting to crack weak encryption keys or exploit vulnerabilities in the encryption protocols.

4. **Rogue access point detection:** Test for the presence of rogue access points, which are unauthorized devices that mimic legitimate access points to deceive users and capture sensitive information. Scan for unauthorized access points and validate their legitimacy.

5. **Weak or default configurations:** Assess the security configurations of wireless devices, such as access points and routers. Test for weak or default administrative credentials, insecure wireless configurations, or weak encryption settings.

6. **Authentication bypass:** Test the effectiveness of authentication mechanisms used in the wireless network. Attempt to bypass authentication controls or exploit vulnerabilities to gain unauthorized access to the network.

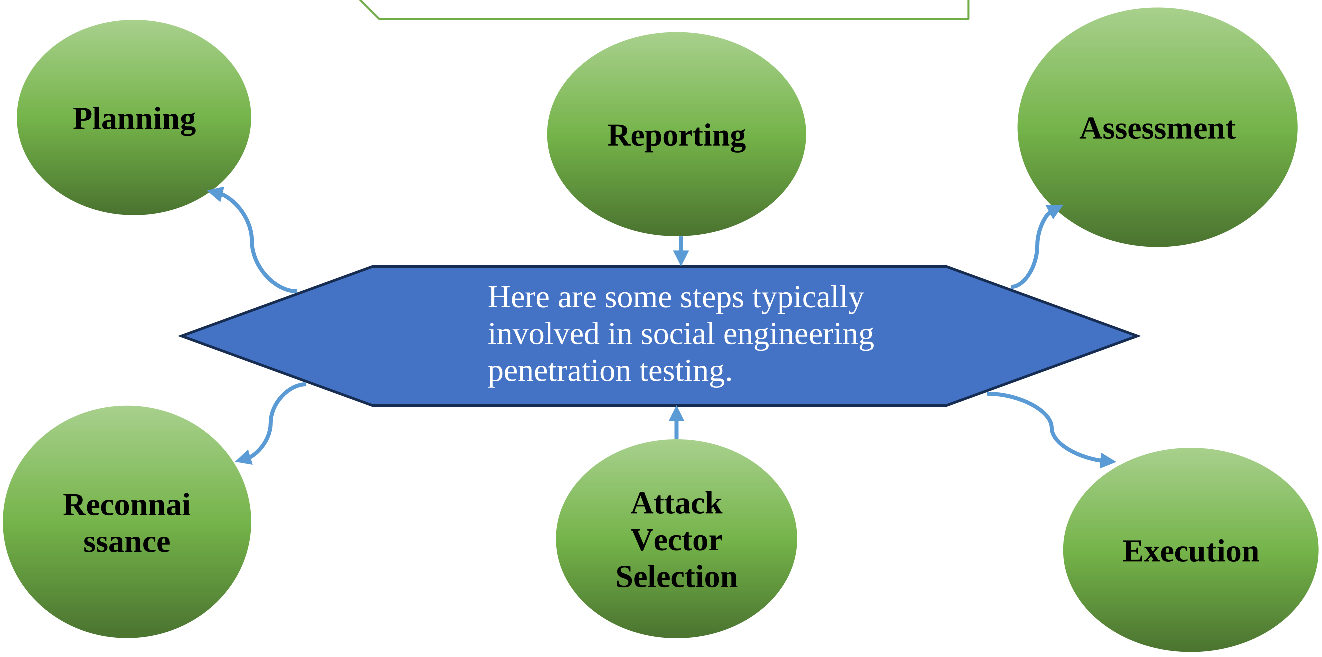
7. **Denial of Service (DoS) testing:** Test the resilience of the wireless network against DoS attacks. Attempt to flood the network with excessive traffic or deauthenticate legitimate clients to disrupt network operations.

8. **Eavesdropping and Man-in-the-Middle (MitM) attacks:** Test for vulnerabilities that could allow eavesdropping on wireless network traffic or conducting MitM attacks. Assess the security of protocols like WEP, WPA, or WPA2 to determine if they can be compromised.

9. **Reporting:** Document the findings, including vulnerabilities discovered, their impact, and recommended remediation steps. Provide a comprehensive report to the organization, outlining potential risks and suggestions for improving the security of the wireless network.

Wireless network penetration testing helps identify and address vulnerabilities in wireless networks, ensuring the security of network communications, preventing unauthorized access, and protecting against potential attacks. It's important to conduct wireless network penetration testing with proper authorization and adhere to ethical guidelines to ensure the security of the tested networks.

(Social Engineering)


Planning
Reporting
Assessment
Here are some steps typically involved in social engineering penetration testing.
Reconnaissance
Attack Vector Selection
Execution

Social engineering penetration testing is a process of assessing an organization's security by simulating real-world social engineering attacks. The goal of this testing is to identify vulnerabilities in human behavior, policies, and procedures that could be exploited by malicious actors. The objective is to evaluate the effectiveness of an organization's security controls and educate employees about potential risks associated with social engineering attacks.

Here are some steps typically involved in social engineering penetration testing:

1. **Planning:** The testing team defines the scope, objectives, and methodologies for the social engineering tests. This includes identifying target individuals or departments within the organization.

2. **Reconnaissance:** The testers gather information about the target organization, such as its employees, infrastructure, policies, and publicly available information. This helps in designing effective social engineering attacks.

3. **Attack Vector Selection:** The testers choose appropriate attack vectors based on the gathered information. These may include phishing emails, phone calls, physical impersonation, USB drops, or other tactics.

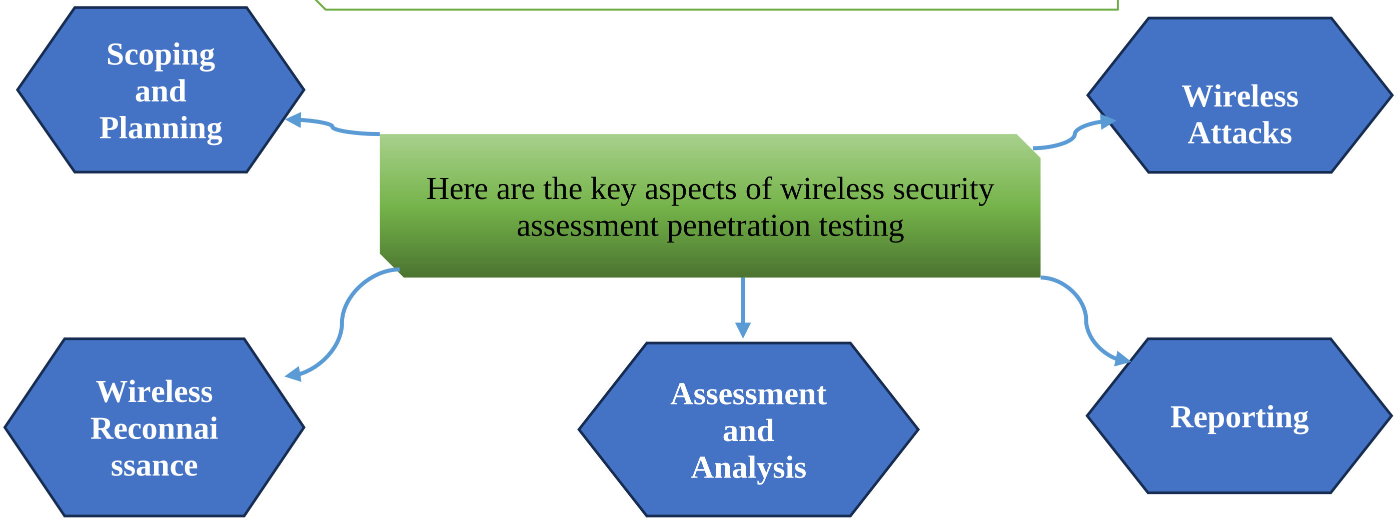
4. **Execution:** The testers execute the social engineering attacks, attempting to manipulate individuals into performing actions that could compromise security. This could involve tricking employees into revealing sensitive information, providing unauthorized access, or downloading malicious files.

5. **Assessment:** The testers document the success rate of the social engineering attacks and assess the organization's vulnerability to such tactics. They identify weaknesses in security awareness, policies, and procedures.

6. **Reporting:** A comprehensive report is prepared, detailing the findings, vulnerabilities, and recommendations for mitigating the identified risks. This helps organizations understand their security gaps and take appropriate measures to improve their defenses.

Social engineering penetration testing is an important part of a comprehensive security assessment, as it provides insights into the human element of security. By understanding vulnerabilities in employee behavior and awareness, organizations can strengthen their security posture, implement effective security training programs, and develop policies and procedures to mitigate social engineering risks.

(Wireless Security Assessment)



Here are the key aspects of wireless security assessment penetration testing

Scoping and Planning

Wireless Attacks

Wireless Reconnaissance

Assessment and Analysis

Reporting

Wireless security assessment, also known as wireless penetration testing or wireless vulnerability assessment, is the process of evaluating the security of wireless networks and devices. It involves simulating real-world attacks to identify vulnerabilities and weaknesses in wireless network configurations, encryption protocols, authentication mechanisms, and other related components.

Here are the key aspects of wireless security assessment penetration testing:

1. **Scoping and Planning:** The testing team collaborates with the organization to define the scope of the wireless security assessment. This includes identifying target wireless networks, devices, and objectives, as well as any specific compliance requirements or security concerns.

2. **Wireless Reconnaissance:** The testers conduct passive and active reconnaissance to gather information about the wireless networks, such as SSIDs (Service Set Identifiers), encryption protocols, signal strengths, and MAC (Media Access Control) addresses. They also identify potential vulnerabilities or misconfigurations in wireless access points and devices.

3. **Wireless Attacks:** The testers attempt various wireless attack techniques to exploit vulnerabilities and gain unauthorized access to the wireless network. This may include brute-forcing encryption keys, conducting rogue access point attacks, exploiting weak authentication mechanisms, or conducting wireless eavesdropping.

4. **Assessment and Analysis:** The testers analyze the results of the wireless security assessment, including successful attacks, vulnerabilities, and weaknesses identified. They assess the impact and severity of these findings to determine the level of risk and potential impact on the organization's wireless network security.

5. **Reporting:** A comprehensive report is prepared, documenting the findings, vulnerabilities, and recommendations for improving the security of the wireless networks. This report helps organizations understand their wireless security risks, prioritize remediation efforts, and implement effective security controls.

Wireless security assessment penetration testing is crucial for organizations that rely on wireless networks for their operations. By identifying and addressing vulnerabilities, organizations can mitigate the risk of unauthorized access, data breaches, or other wireless network-related security incidents.

It is important to note that wireless security assessment penetration testing should always be conducted ethically, with proper authorization and in compliance with legal and ethical guidelines. Organizations should engage experienced and qualified professionals to perform wireless security assessments to ensure accuracy, safety, and effectivenes.

(Red Team Testing)

Red team testing, also known as adversarial simulation or red teaming, is a type of penetration testing that simulates real-world cyberattacks to evaluate an organization's security posture and resilience. It involves a team of skilled professionals, referred to as the "red team," who actively try to breach the organization's defenses and identify vulnerabilities and weaknesses.

Here are the key aspects of red team testing penetration testing:

1. **Objective Setting:** The red team collaborates with the organization to define specific objectives for the engagement. These objectives could include gaining unauthorized access to sensitive data, compromising critical systems, or bypassing security controls. The objectives are tailored to the organization's unique security concerns and priorities.

2. **Reconnaissance:** The red team conducts extensive reconnaissance to gather information about the organization's infrastructure, systems, employees, and potential attack vectors. This may involve open-source intelligence gathering, social engineering techniques, or network scanning to identify potential entry points.

3. **Active Attacks:** The red team performs a variety of active attacks to exploit vulnerabilities and gain unauthorized access to the organization's systems. This may include network exploitation, web application attacks, phishing campaigns, physical intrusion attempts, or even insider threat simulations. The goal is to assess the organization's ability to detect and respond to real-world threats.

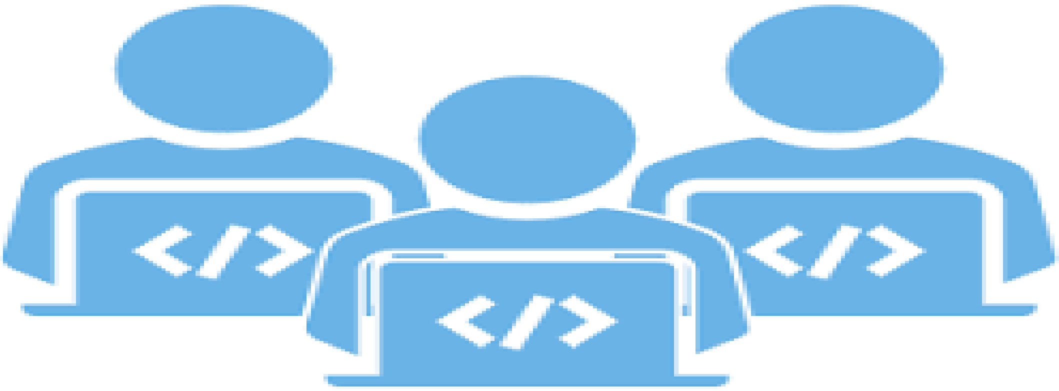
4. **Persistence and Lateral Movement:** Once the red team gains initial access, they may attempt to maintain persistence within the organization's network and move laterally to explore additional targets. This allows them to assess the effectiveness of segmentation, access controls, and detection mechanisms in place.

5. **Reporting:** After the engagement, the red team prepares a comprehensive report detailing the findings, including successful attack vectors, vulnerabilities, and recommendations for improving the organization's security posture. The report aims to provide actionable insights and help the organization enhance its defenses and incident response capabilities.

Red team testing goes beyond traditional vulnerability assessments and penetration tests by adopting a proactive and adversarial approach. It helps organizations identify gaps in their security controls, improve their incident response capabilities, and enhance overall resilience against real-world cyber threats.

It is essential to conduct red team testing in a controlled and authorized manner, with close collaboration between the organization and the red team. Proper legal and ethical considerations should be followed to ensure the safety and integrity of the testing process. Organizations should engage reputable and experienced red teaming professionals to conduct these assessments effectivel

(Blue Team Testing)



Blue team testing is a type of security testing that simulates a real-world attack on an organization's security infrastructure. The goal of blue team testing is to identify and remediate vulnerabilities in the organization's security posture, and to improve the organization's ability to respond to and recover from a cyberattack.

Blue team testing typically involves the following steps:

1. Attack planning: The blue team develops a plan for the attack, which includes the following:
    1. The target systems or applications
    2. The attack vectors that will be used
    3. The desired outcomes of the attack
2. Attack execution: The blue team executes the attack plan, using the attack vectors that were identified in the planning phase.
3. Post-mortem analysis: The blue team analyzes the results of the attack, identifies any vulnerabilities that were exploited, and makes recommendations for remediation.

Blue team testing can be conducted by internal or external security teams. Internal security teams typically have a better understanding of the organization's specific security needs, but they may lack the expertise and resources to conduct a comprehensive blue team test. External security teams can provide a more objective and comprehensive assessment of the organization's security posture, but they may lack the understanding of the organization's specific needs.

Blue team testing is an important part of any organization's security program. By simulating a real-world attack, blue team testing can help organizations identify and remediate vulnerabilities, and to improve their ability to respond to and recover from a cyberattack.

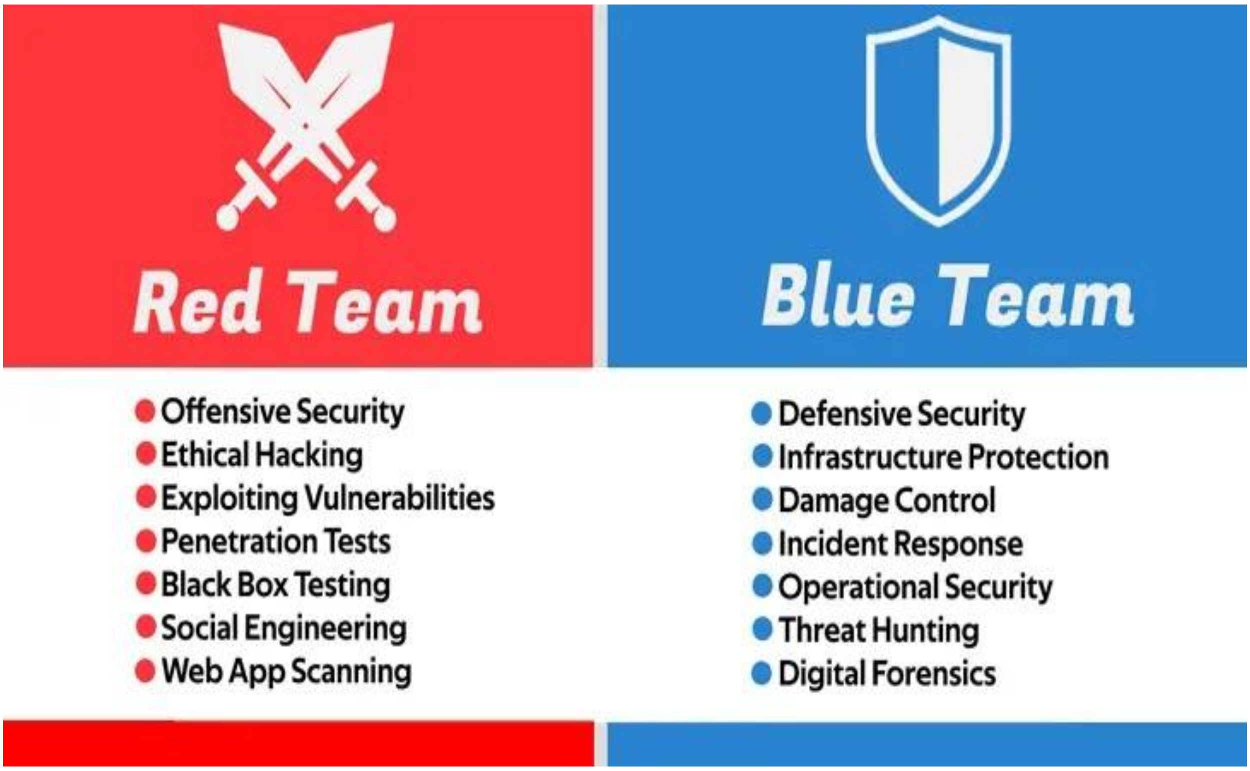
Here are some of the benefits of blue team testing:

1. Improved security posture: Blue team testing can help to improve an organization's security posture by identifying and remediating vulnerabilities. This can make it more difficult for attackers to exploit vulnerabilities and gain access to sensitive data.
2. Reduced risk of data breaches: Data breaches can be costly and damaging for organizations. Blue team testing can help to reduce the risk of data breaches by identifying and remediating vulnerabilities that could be exploited by attackers.

3. Increased compliance: Many industries, such as financial services and healthcare, have regulations that require organizations to have a secure environment. Blue team testing can help organizations to demonstrate compliance with these regulations.
4. Enhanced employee awareness: Blue team testing can help to raise employee awareness of security risks. This can help employees to take steps to protect sensitive data and prevent attacks.
5. Improved decision-making: Blue team testing can provide valuable information that can help organizations make informed decisions about security investments. This information can help organizations to prioritize security risks and allocate resources effectively.

Overall, blue team testing is an important part of any organization's security program. By simulating a real-world attack, blue team testing can help organizations identify and remediate vulnerabilities, and to improve their ability to respond to and recover from a cyberattack.

The difference between **Red Team Testing** and **Blue Team Testing:**



(Mobile Penetration Testing)

Security probllems

Code vulnerabilities

API vulnerabilities

Configuration vulnerabilities

Data vulnerabilities

Mobile penetration testing is a security assessment method that involves simulating an attack on a mobile app in order to identify and exploit vulnerabilities. This type of testing can be performed on both native and web-based mobile apps, and can help to identify a wide range of security issues, including:

1. **Code vulnerabilities:** These vulnerabilities can be found in the app's code, and can allow an attacker to gain unauthorized access to the app, its data, or the device it is running on.

2. **Configuration vulnerabilities:** These vulnerabilities can be found in the app's configuration settings, and can allow an attacker to bypass security controls or gain unauthorized access to the app.

3. **API vulnerabilities:** These vulnerabilities can be found in the app's APIs, and can allow an attacker to interact with the app in ways that were not intended by the developer, such as making unauthorized requests or modifying data.

4. **Data vulnerabilities:** These vulnerabilities can be found in the app's data, and can allow an attacker to steal sensitive information, such as user credentials or financial data.

Mobile penetration testing is an important part of the overall security assessment process for mobile apps. By identifying and remediating vulnerabilities before they can be exploited by attackers, mobile penetration testing can help to protect mobile apps and the data they contain.

Here are some of the benefits of mobile penetration testing:

. Identify security vulnerabilities: Mobile penetration testing can help to identify security vulnerabilities in mobile apps that may not be visible to developers or testers. This can help to protect users from data breaches, financial loss, and other security threats.

1. **Improve security posture:** Mobile penetration testing can help to improve the security posture of mobile apps by identifying and remediating vulnerabilities. This can help to reduce the risk of data breaches and other security incidents.

2. **Meet compliance requirements:** Many industries, such as financial services and healthcare, have regulations that require mobile apps to be secure. Mobile penetration testing can help organizations to meet these requirements and demonstrate that they are taking steps to protect their users.

If you are developing or using mobile apps, it is important to consider mobile penetration testing as part of your overall security strategy. By identifying and remediating vulnerabilities before they can be exploited, mobile penetration testing can help to protect your users and your business.

Here are some of the most common tools used for mobile penetration testing:

1. **OWASP Zed Attack Proxy (ZAP):** ZAP is a free and open-source security testing tool that can be used to scan web applications for vulnerabilities. ZAP can also be used to scan mobile apps, but it is not as comprehensive as some other tools.

2. **Burp Suite:** Burp Suite is a commercial security testing tool that is more comprehensive than ZAP. Burp Suite can be used to scan web applications and mobile apps for vulnerabilities.

3. **MobSF:** MobSF is a free and open-source security testing framework for mobile apps. MobSF can be used to scan Android and iOS apps for vulnerabilities.

4. **ImmuniWeb Mobile Security Scanner:** ImmuniWeb Mobile Security Scanner is a commercial security testing tool that can be used to scan Android and iOS apps for vulnerabilities.

When choosing a tool for mobile penetration testing, it is important to consider the following factors:

1. **The type of mobile apps you are developing or using:** Some tools are better suited for Android apps, while others are better suited for iOS apps.

2. **The features you need:** Some tools have more features than others. Make sure the tool you choose has the features you need to scan your apps for vulnerabilities.

3. **The cost:** Some tools are free, while others are commercial. Choose a tool that fits your budget.

Mobile penetration testing is an important part of the overall security assessment process for mobile apps. By identifying and remediating vulnerabilities before they can be exploited, mobile penetration testing can help to protect users from data breaches, financial loss, and other security threats.

(Clintent side Penetration Testing)

Client-side penetration testing (CS-PT) is a type of security assessment that focuses on identifying and exploiting vulnerabilities in client-side applications, such as web browsers, email clients, and office suites. CS-PT is often used in conjunction with network penetration testing (NPT) and web application penetration testing (WAPT) to provide a comprehensive assessment of an organization's security posture.
Client-side applications are often the weakest link in an organization's security chain. This is because they are typically developed by different teams than the organization's network and web applications, and they are often not updated as frequently. As a result, client-side applications can contain a wide range of vulnerabilities that can be exploited by attackers.

CS-PT can be conducted in a variety of ways, but it typically involves the following steps:

1. Information gathering: The penetration tester gathers information about the client-side applications that are in use within the organization, such as their versions, configurations, and known vulnerabilities.

2. Vulnerability scanning: The penetration tester uses automated tools to scan the client-side applications for known vulnerabilities.

3. Manual testing: The penetration tester manually tests the client-side applications to identify additional vulnerabilities that may not have been found by automated tools.

4. Exploitation: The penetration tester attempts to exploit any vulnerabilities that have been identified in order to gain access to the organization's network or systems.

5. Reporting: The penetration tester reports their findings to the organization, including the vulnerabilities that were identified, how they were exploited, and any recommendations for remediation.

CS-PT can be a valuable tool for organizations that want to improve their security posture. By identifying and remediating vulnerabilities in their client-side applications, organizations can reduce their risk of being attacked and can protect their sensitive data.
Here are some of the benefits of client-side penetration testing:

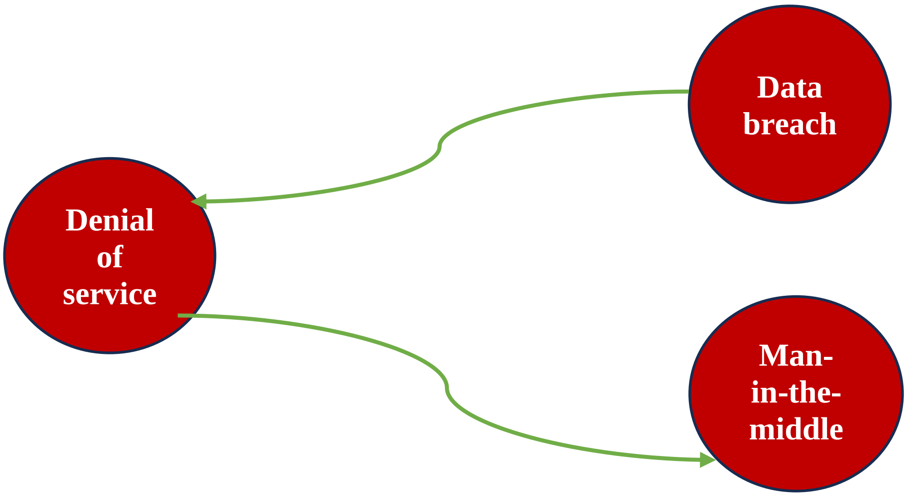
1. Identify security vulnerabilities: CS-PT can help to identify security vulnerabilities in client-side applications that may not be visible to developers or testers. This can help to protect users from data breaches, financial loss, and other security threats.

2. Improve security posture: CS-PT can help to improve the security posture of client-side applications by identifying and remediating vulnerabilities. This can help to reduce the risk of data breaches and other security incidents.

3. Meet compliance requirements: Many industries, such as financial services and healthcare, have regulations that require client-side applications to be secure. CS-PT can help organizations to meet these requirements and demonstrate that they are taking steps to protect their users.

If you are responsible for the security of a client-side application, it is important to consider CS-PT as part of your overall security strategy. By identifying and remediating vulnerabilities before they can be exploited, CS-PT can help to protect your users and your business.

risks Penetration Testing:



Penetration testing is a valuable security assessment tool that can help organizations identify and remediate vulnerabilities in their systems and networks. However, there are some potential risks associated with penetration testing, such as:

1. **Data breach:** If a penetration tester is able to exploit a vulnerability in a system or network, they may be able to gain access to sensitive data, such as financial information, customer data, or intellectual property.
2. **Denial of service:** A penetration tester may be able to use a vulnerability in a system or network to disrupt or disable the system or network, which could prevent employees from working or customers from accessing services.
3. **Man-in-the-middle attack:** A penetration tester may be able to use a vulnerability in a system or network to eavesdrop on communications or to inject malicious code into traffic.

It is important to note that these are just some of the potential risks associated with penetration testing. The specific risks will vary depending on the specific organization and the specific system or network being tested.

If you are considering penetration testing, it is important to weigh the potential risks against the potential benefits. It is also important to work with a qualified and experienced penetration testing firm to minimize the risks and maximize the benefits of the testing.

Here are some tips for reducing the risks of penetration testing:

1. **Choose a qualified and experienced penetration testing firm:** A qualified and experienced penetration testing firm will have the knowledge and expertise to identify and exploit vulnerabilities in your systems and networks without causing undue harm.
2. **Get approval from management:** Before conducting a penetration test, it is important to get approval from management. This will help to ensure that the testing is conducted in a responsible and professional manner.
3. Have a plan: Before conducting a penetration test, it is important to have a plan in place. This plan should include the following:
    1. The specific goals of the testing
    2. The methods that will be used during the testing
    3. The steps that will be taken to mitigate any risks that are identified during the testing
4. Monitor the testing: During the testing, it is important to monitor the testing to ensure that it is conducted in a responsible and professional manner.
5. Report the findings: After the testing is complete, it is important to report the findings to management. This report should include the following:
    1. The vulnerabilities that were identified
    2. The steps that need to be taken to remediate the vulnerabilities

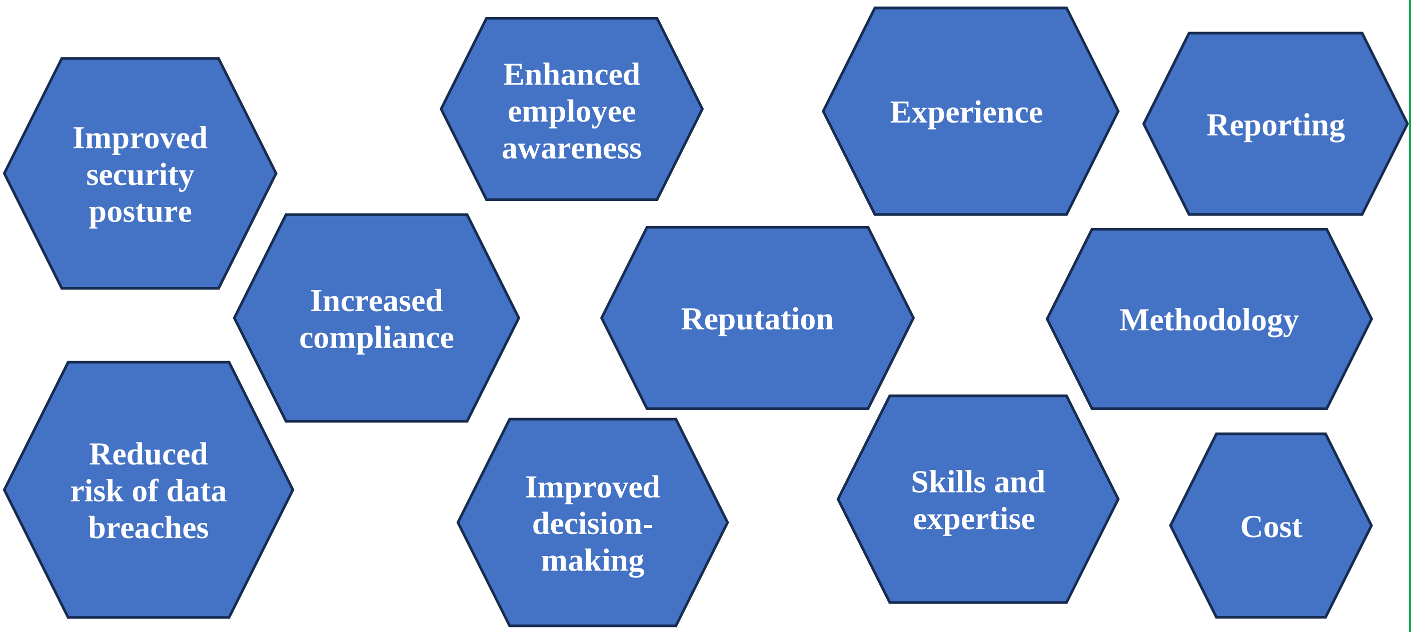
By following these tips, you can help to reduce the risks of penetration testing and maximize the benefits of the testing.

Here are some additional things to consider when planning a penetration test:

1. **The scope of the test:** What systems and networks will be tested?
2. **The level of engagement:** Will the penetration testers be able to interact with employees and customers?
3. **The reporting format:** How will the results of the test be reported?
4. **The cost of the test:** Penetration testing can be expensive, so it is important to get quotes from multiple firms before making a decision.

By carefully planning and executing a penetration test, organizations can identify and remediate vulnerabilities in their systems and networks, which can help to improve their overall security posture.

benefits Penetration Testing:



Penetration testing is a valuable security assessment tool that can help organizations identify and remediate vulnerabilities in their systems and networks. Here are some of the benefits of penetration testing:

1. **Improved security posture:** By identifying and remediating vulnerabilities, penetration testing can help to improve an organization's security posture. This can make it more difficult for attackers to exploit vulnerabilities and gain access to sensitive data.
2. **Reduced risk of data breaches:** Data breaches can be costly and damaging for organizations. Penetration testing can help to reduce the risk of data breaches by identifying and remediating vulnerabilities that could be exploited by attackers.

3. **Increased compliance:** Many industries, such as financial services and healthcare, have regulations that require organizations to have a secure environment. Penetration testing can help organizations to demonstrate compliance with these regulations.
4. **Enhanced employee awareness:** Penetration testing can help to raise employee awareness of security risks. This can help employees to take steps to protect sensitive data and prevent attacks.
5. **Improved decision-making:** Penetration testing can provide valuable information that can help organizations make informed decisions about security investments. This information can help organizations to prioritize security risks and allocate resources effectively.

Overall, penetration testing is a valuable security assessment tool that can help organizations improve their security posture and reduce the risk of data breaches.

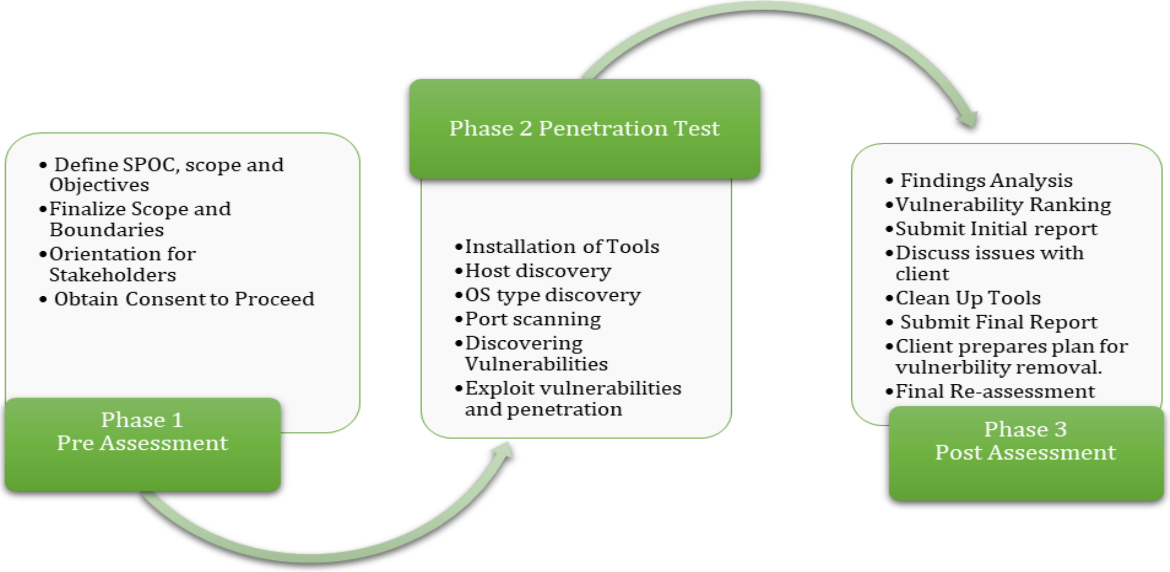
Here are some of the factors to consider when choosing a penetration testing firm:

1. **Experience:** The firm should have experience conducting penetration tests for organizations in your industry.
2. **Reputation:** The firm should have a good reputation in the industry.

3. **Skills and expertise:** The firm should have the skills and expertise to conduct a comprehensive penetration test.
4. **Methodology:** The firm should have a well-defined methodology for conducting penetration tests.
5. **Reporting:** The firm should provide a detailed report of the findings of the penetration test.
6. **Cost:** The cost of the penetration test should be reasonable.

It is important to note that penetration testing is not a silver bullet. It is just one tool that can be used to improve an organization's security posture. However, when conducted properly, penetration testing can be a valuable asset in protecting an organization from cyberattacks.

Vulnerability Assessment and Penetration Testing Service:



Phase 1
Pre Assessment

- Define SPOC, scope and Objectives
- Finalize Scope and Boundaries
- Orientation for Stakeholders
- Obtain Consent to Proceed

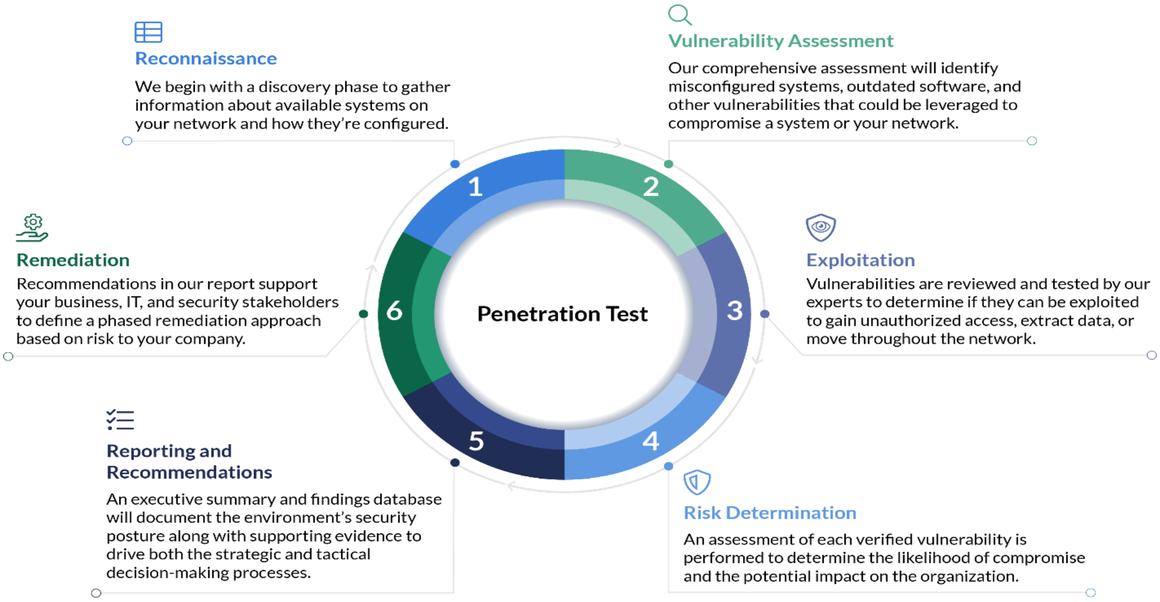
Phase 2 Penetration Test

- Installation of Tools
- Host discovery
- OS type discovery
- Port scanning
- Discovering Vulnerabilities
- Exploit vulnerabilities and penetration

Phase 3
Post Assessment

- Findings Analysis
- Vulnerability Ranking
- Submit Initial report
- Discuss issues with client
- Clean Up Tools
- Submit Final Report
- Client prepares plan for vulnerbility removal.
- Final Re-assessment

Our **Penetration Testing** services model is illustrated below comprising the full cycle Vulnerability Assessment, Penetration Testing, and post assessment activities.



Reconnaissance

We begin with a discovery phase to gather information about available systems on your network and how they're configured.

Vulnerability Assessment

Our comprehensive assessment will identify misconfigured systems, outdated software, and other vulnerabilities that could be leveraged to compromise a system or your network.

Exploitation

Vulnerabilities are reviewed and tested by our experts to determine if they can be exploited to gain unauthorized access, extract data, or move throughout the network.

Risk Determination

An assessment of each verified vulnerability is performed to determine the likelihood of compromise and the potential impact on the organization.

Reporting and Recommendations

An executive summary and findings database will document the environment's security posture along with supporting evidence to drive both the strategic and tactical decision-making processes.

Remediation

Recommendations in our report support your business, IT, and security stakeholders to define a phased remediation approach based on risk to your company.

Reporting and Deliverables:

1. The final report will start with an Executive Summary and an overview of the assessment process that has been taken, and then followed by the statement of
2. Methodology and the statement of scope. Also, it will contain The Documentation of Identified Vulnerabilities which contain all the details of the steps, test Vectors, and exploited vulnerabilities that lead to Positive and/or false positive penetration during testing for which remediation and retesting are required.

In addition, it will include analysis of the findings and finally concluded by the list of recommendations to fix the gaps/ vulnerabilities discovered

Tools to be Used Penetration Testing:

Tools Name	Usage Purpose
Oracle VM VirtualBox	A virtualization product
Parrot OS	a Linux distribution based on Debian with a focus on security, privacy, and development. Designed for ethical hackers and penetration testers
Qualys	Qualys is a proprietary vulnerability scanner
NMAP	Network Assessment
Sslmscan	Scan an HTTPS service to enumerate what protocols (SSLv2, SSLv3 and TLS1) and what ciphers the HTTPS service supports.
Metasploit	To do in depth analysis, correlation and cross verify the automation tool results and to check the scripting and coding vulnerabilities, Injection attack possibilities, brute-forcing…
Smbclient	ftp-like client to access SMB/CIFS resources on servers
Burp Suite	Helps you identify vulnerabilities and verify attack vectors that are affecting web applications
Manual Reviews	
XSS Proxy	Cross-Site scripting toolkit
SQLMap	Sql Injection toolkit
FOCA	Review Webserver Metafiles for Information Leakage
Webhosting.info	Enumerate Applications on Webserver
Wappalyzer	shows you what websites are built with.
Hydra	Brute-Forcing tools
Hashcat	Password cracking
Dirbuster	brute force directories and files names on web/application servers
Impacket	Focused on providing low-level programmatic access to the packets and for some protocols (e.g. SMB1-3 and MSRPC) the protocol implementation itself
Responder	Poison LLMNR, DNS and SMB
Purple Knight	Active Directory security assessment tool
Ping Castle	Active Directory security assessment tool
Nmap wafw00f Burp-Suite	WAF Fingerprinting

(Test EDR)

To test your EDR, you can use a variety of methods, including:

1. Using a third-party testing service: There are a number of third-party companies that offer EDR testing services. These services typically use a variety of methods to test your EDR, including simulated attacks, vulnerability scanning, and behavioral analysis.
2. Using a red team: A red team is a group of security professionals who simulate a cyberattack on your organization. This can be a great way to test your EDR's ability to detect and respond to real-world threats.
3. Using a self-assessment tool: There are a number of self-assessment tools available that can help you test your EDR. These tools typically ask you questions about your EDR configuration, policies, and procedures.

No matter which method you choose, it's important to test your EDR regularly to ensure that it's up to date and effective. Regular testing can help you identify any gaps in your security posture and take steps to improve it.

Here are some specific steps you can take to test your EDR:

1. Install the EDR software on your endpoints.
2. Configure the EDR software according to the vendor's instructions.
3. Enable all of the EDR features.
4. Monitor the EDR logs for any suspicious activity.
5. Run simulated attacks against your endpoints.
6. Review the EDR alerts to see if they detect the simulated attacks.
7. Repeat steps 4-6 on a regular basis.

By following these steps, you can help ensure that your EDR is effective in detecting and responding to cyberattacks.

Here are some additional tips for testing your EDR:

1. Use a variety of methods to test your EDR. This will help you get a more comprehensive view of its effectiveness.
2. Test your EDR in a production environment. This will help you identify any potential issues that could impact your business.
3. Get feedback from your security team. This will help you identify any areas where your EDR could be improved.
4. Keep your EDR up to date. The vendor will release new updates and patches on a regular basis. These updates can improve the EDR's effectiveness and fix any known vulnerabilities.

By following these tips, you can help ensure that your EDR is effective in protecting your organization from cyberattacks.

(ByPass EDR)

Endpoint Detection and Response (EDR) solutions are designed to detect and respond to malicious activity on endpoints. However, there are a number of ways that attackers can bypass EDR protection.

Here are some of the most common EDR bypass techniques:

1. AMSI bypass: AMSI is a Microsoft framework that allows EDR solutions to scan files, memory, and streams for malicious payloads. Attackers can bypass AMSI by using techniques such as obfuscation, code signing, and memory patching.
2. Unhooking: EDR solutions often use hooks to monitor and control the behavior of processes. Attackers can bypass these hooks by unhooking them, which allows them to execute malicious code without being detected.
3. Reflective DLL loading: Reflective DLL loading is a technique that allows attackers to load malicious DLLs into processes without using the operating system's normal loading mechanisms. This can bypass EDR solutions that monitor DLL loading.
4. Using native Windows binaries: Attackers can use native Windows binaries, or "Living off the Land" (LoLBin) binaries, to bypass EDR protection. LoLBins are legitimate Windows binaries that can be used for malicious purposes. EDR solutions often do not detect LoLBins because they are not considered to be malicious.
5. Using sandbox escape techniques: Sandboxes are used to isolate malicious code and prevent it from affecting the rest of the system. However, there are a number of sandbox escape techniques that allow attackers to escape from sandboxes and execute malicious code on the host system.

It is important to note that these are just a few of the many ways that attackers can bypass EDR protection. As EDR solutions become more sophisticated, attackers will continue to develop new techniques to bypass them.

The best way to protect against EDR bypass attacks is to use a layered security approach that includes EDR, firewalls, intrusion detection systems, and other security solutions. You should also keep your security software up to date and implement security best practices.

Here are some additional tips for protecting against EDR bypass attacks:

1. Use a layered security approach: A layered security approach is the best way to protect against EDR bypass attacks. This means using a combination of security solutions, such as EDR, firewalls, intrusion detection systems, and others.
2. Keep your security software up to date: Attackers are constantly developing new techniques to bypass security software. It is important to keep your security software up to date with the latest patches and updates to protect against these new threats.
3. Implement security best practices: There are a number of security best practices that can help protect against EDR bypass attacks. These include using strong passwords, implementing multi-factor authentication, and keeping your operating systems and applications up to date.

By following these tips, you can help protect your organization from EDR bypass attacks.

(Test data Leakage)

Sure, here are some ways to test for data leakage:

1. Use a data leakage prevention (DLP) tool: DLP tools can help you identify and prevent data leakage by monitoring your network and systems for sensitive data.
2. Perform regular audits: Regular audits can help you identify any potential data leakage issues.
3. Train your employees: Employees should be trained on how to identify and prevent data leakage.
4. Implement security controls: Security controls, such as strong passwords and access controls, can help prevent data leakage.

Here are some specific steps you can take to test for data leakage:

1. Identify your sensitive data: The first step is to identify the sensitive data that you need to protect. This could include customer data, financial data, or intellectual property.
2. Monitor your network and systems: Once you know what data you need to protect, you can start monitoring your network and systems for any signs of data leakage. This could include monitoring for unauthorized access, data exfiltration, or data breaches.
3. Perform regular audits: Regular audits can help you identify any potential data leakage issues. This could involve reviewing your security logs, interviewing employees, and conducting vulnerability assessments.
4. Train your employees: Employees should be trained on how to identify and prevent data leakage. This training should cover topics such as data classification, password security, and social engineering.
5. Implement security controls: Security controls, such as strong passwords and access controls, can help prevent data leakage. These controls should be implemented across all of your systems and applications.

By following these steps, you can help ensure that your organization is protected from data leakage.

Here are some additional tips for preventing data leakage:

1. Use strong passwords: Strong passwords should be used for all accounts, including email, social media, and corporate accounts.
2. Be careful what you click on: Phishing emails are a common way for attackers to steal sensitive data. Be careful what links you click on and what attachments you open.
3. Keep your software up to date: Software updates often include security patches that can help protect your systems from vulnerabilities.
4. Use a VPN: A VPN can help protect your data when you are using public Wi-Fi.
5. Encrypt your data: Encrypting your data can help protect it from unauthorized access.

By following these tips, you can help protect your data from leakage.

(Test domain controller)

Testing your domain controller is an important part of keeping your Active Directory environment healthy and secure. There are a few different ways to test your domain controller, but some of the most common methods include:

1. Using the DCDiag tool: DCDiag is a Microsoft-provided tool that can be used to test the health of your domain controllers. DCDiag can check for a variety of issues, including connectivity, DNS, replication, and security.
2. Using a third-party tool: There are a number of third-party tools that can be used to test your domain controller. These tools often offer more features than DCDiag, such as the ability to test for specific vulnerabilities.
3. Manually testing: You can also manually test your domain controller by performing a variety of tasks, such as logging in, creating users, and creating objects. Manual testing can be time-consuming, but it can be a good way to ensure that your domain controller is functioning properly.

It is important to test your domain controller on a regular basis. The frequency of testing will depend on the size and complexity of your environment. However, it is a good idea to test your domain controller at least once a month.

Here are some of the things you can test for when testing your domain controller:

1. Connectivity: Make sure that your domain controller is properly connected to the network.
2. DNS: Make sure that your domain controller is configured with the correct DNS settings.
3. Replication: Make sure that your domain controller is replicating properly with other domain controllers in your forest.
4. Security: Make sure that your domain controller is properly secured. This includes setting strong passwords, enabling security features, and keeping your software up to date.

By following these tips, you can help ensure that your domain controllers are healthy and secure.

Here are some additional tips for testing your domain controller:

1. Test from multiple locations: If possible, test your domain controller from multiple locations. This will help you identify any issues that may be specific to a particular network or location.
2. Test during off-peak hours: If possible, test your domain controller during off-peak hours. This will help minimize the impact of any testing-related disruptions.
3. Document your findings: After you have completed testing, document your findings. This will help you track any issues that you have identified and make sure that they are addressed.

By following these tips, you can help ensure that your domain controller testing is effective and efficient.

(Test office 365)

Here are some ways to test Office 365:

1. Use the Office 365 Test Environment: Microsoft provides a free test environment for Office 365. This environment can be used to test Office 365 features and applications without impacting your production environment.
2. Use a third-party tool: There are a number of third-party tools that can be used to test Office 365. These tools often offer more features than the Office 365 Test Environment, such as the ability to test for specific vulnerabilities.
3. Manually test: You can also manually test Office 365 by using the applications and features in your production environment. Manual testing can be time-consuming, but it can be a good way to ensure that Office 365 is functioning properly.

Here are some of the things you can test for when testing Office 365:

1. Connectivity: Make sure that you can connect to Office 365.
2. Applications: Make sure that you can access and use all of the Office 365 applications.
3. Features: Make sure that all of the Office 365 features are working properly.
4. Security: Make sure that your Office 365 environment is secure.

By following these tips, you can help ensure that your Office 365 environment is healthy and secure.

Here are some additional tips for testing Office 365:

1. Test from multiple locations: If possible, test Office 365 from multiple locations. This will help you identify any issues that may be specific to a particular network or location.
2. Test during off-peak hours: If possible, test Office 365 during off-peak hours. This will help minimize the impact of any testing-related disruptions.
3. Document your findings: After you have completed testing, document your findings. This will help track any issues that you have identified and make sure that they are addressed.

By following these tips, you can help ensure that your Office 365 testing is effective and efficient.

Here are some specific tests you can run:

1. Connectivity: You can test connectivity to Office 365 by trying to access an Office 365 application, such as Outlook or Word. If you are unable to access the application, then there may be an issue with your network connection.
2. Applications: You can test the applications in Office 365 by trying to create a new document, send an email, or collaborate on a project. If you are unable to perform any of these tasks, then there may be an issue with the application.
3. Features: You can test the features in Office 365 by trying to use a specific feature, such as the spell checker or thesaurus. If you are unable to use the feature, then there may be an issue with the feature.
4. Security: You can test the security of your Office 365 environment by trying to log in with a non-administrator account. If you are able to log in with a non-administrator account, then there may be a security issue.

By running these tests, you can help ensure that your Office 365 environment is healthy and secure.

(Test and bypass google)

There are a number of ways to test and bypass Google. Some of the most common methods include:

1. Using a VPN: A VPN can help you bypass Google by routing your traffic through a server in another location. This can be useful if you are trying to access a website that is blocked in your region.
2. Using a proxy server: A proxy server can also help you bypass Google by acting as an intermediary between your computer and the website you are trying to access. This can be useful if you are trying to hide your IP address or if you are trying to access a website that is blocked in your region.
3. Using a Tor browser: The Tor browser is a special browser that encrypts your traffic and routes it through a series of servers, making it difficult for anyone to track your online activity. This can be useful if you are trying to bypass Google or if you are trying to browse the internet anonymously.
4. Using a custom DNS server: You can also bypass Google by using a custom DNS server. A DNS server is responsible for translating domain names into IP addresses. By using a custom DNS server, you can point your DNS requests to a server that is not controlled by Google. This can be useful if you are trying to bypass Google's filtering or if you are trying to access a website that is blocked in your region.

It is important to note that bypassing Google can have some risks. For example, if you are using a VPN or a proxy server, your internet traffic may be slower than if you were not using a VPN or a proxy server. Additionally, if you are using a Tor browser, you may have difficulty accessing some websites.

If you are considering bypassing Google, it is important to weigh the risks and benefits before making a decision.

Here are some additional tips for bypassing Google:

1. Be aware of the risks: As mentioned above, there are some risks associated with bypassing Google. Be sure to weigh the risks and benefits before making a decision.
2. Use a reputable VPN or proxy server: There are many VPNs and proxy servers available. Be sure to choose one that is reputable and that has a good reputation for security.
3. Use a secure browser: When bypassing Google, it is important to use a secure browser. The Tor browser is a good option, but you can also use other browsers that have good security features.
4. Be careful what you do online: When bypassing Google, you should be careful what you do online. If you are doing anything that is illegal or that could get you in trouble, you should not bypass Google.

By following these tips, you can help protect yourself when bypassing Google.

(Test and bypass Amazon)

There are a number of ways to test and bypass Amazon. Some of the most common methods include:

1. Using a VPN: A VPN can help you bypass Amazon by routing your traffic through a server in another location. This can be useful if you are trying to access a website that is blocked in your region.
2. Using a proxy server: A proxy server can also help you bypass Amazon by acting as an intermediary between your computer and the website you are trying to access. This can be useful if you are trying to hide your IP address or if you are trying to access a website that is blocked in your region.
3. Using a Tor browser: The Tor browser is a special browser that encrypts your traffic and routes it through a series of servers, making it difficult for anyone to track your online activity. This can be useful if you are trying to bypass Amazon or if you are trying to browse the internet anonymously.
4. Using a custom DNS server: You can also bypass Amazon by using a custom DNS server. A DNS server is responsible for translating domain names into IP addresses. By using a custom DNS server, you can point your DNS requests to a server that is not controlled by Amazon. This can be useful if you are trying to bypass Amazon's filtering or if you are trying to access a website that is blocked in your region.

It is important to note that bypassing Amazon can have some risks. For example, if you are using a VPN or a proxy server, your internet traffic may be slower than if you were not using a VPN or a proxy server. Additionally, if you are using a Tor browser, you may have difficulty accessing some websites.

If you are considering bypassing Amazon, it is important to weigh the risks and benefits before making a decision.

Here are some additional tips for bypassing Amazon:

1. Be aware of the risks: As mentioned above, there are some risks associated with bypassing Amazon. Be sure to weigh the risks and benefits before making a decision.
2. Use a reputable VPN or proxy server: There are many VPNs and proxy servers available. Be sure to choose one that is reputable and that has a good reputation for security.
3. Use a secure browser: When bypassing Amazon, it is important to use a secure browser. The Tor browser is a good option, but you can also use other browsers that have good security features.
4. Be careful what you do online: When bypassing Amazon, you should be careful what you do online. If you are doing anything that is illegal or that could get you in trouble, you should not bypass Amazon.

By following these tips, you can help protect yourself when bypassing Amazon.

(Test oracle)

To test Oracle, you can use a variety of tools, including:

1. SQL Developer: SQL Developer is a free, integrated development environment (IDE) for Oracle Database. It can be used to connect to an Oracle database, run queries, and create and edit PL/SQL programs.
2. Oracle Data Integrator: Oracle Data Integrator is a data integration tool that can be used to extract, transform, and load data from various sources. It can be used to test Oracle databases by loading test data into the database and then running queries against the data.
3. Oracle Application Express: Oracle Application Express (APEX) is a development platform that can be used to create web applications. It can be used to test Oracle databases by creating test cases that interact with the database.

When testing Oracle, it is important to test a variety of features, including:

1. Connectivity: Can you connect to the database?
2. Data integrity: Is the data in the database accurate and consistent?
3. Performance: How fast is the database?
4. Security: Is the database secure?

By testing Oracle regularly, you can help ensure that your database is healthy and secure.

Here are some specific tests you can run:

1. Connectivity: To test connectivity, you can try to connect to the database using SQL Developer or another tool. If you are unable to connect to the database, then there may be an issue with your network connection or with the database itself.
2. Data integrity: To test data integrity, you can run queries to check for duplicate records, missing data, or incorrect data. If you find any problems, then you will need to fix them.
3. Performance: To test performance, you can run queries and measure the time it takes for the database to return the results. If the performance is not acceptable, then you may need to upgrade the hardware or software that the database is running on.
4. Security: To test security, you can try to access the database using unauthorized credentials. If you are able to access the database, then there may be a security issue. You will need to fix the security issue to protect the database from unauthorized access.

By running these tests, you can help ensure that your Oracle database is healthy and secure.

(Testing SAP)

SAP testing is the process of ensuring that SAP applications meet the requirements of users and stakeholders. It is a critical part of the SAP implementation process and helps to ensure that SAP systems are reliable, efficient, and secure.

There are a variety of different SAP testing methods, including:

1. Functional testing: Functional testing is the most common type of SAP testing. It involves testing the functionality of SAP applications to ensure that they meet the requirements of users and stakeholders.
2. Performance testing: Performance testing is used to assess the performance of SAP applications under load. It helps to ensure that SAP systems can handle the expected volume of transactions and users.
3. Security testing: Security testing is used to identify and mitigate security vulnerabilities in SAP applications. It helps to protect SAP systems from unauthorized access, data breaches, and other security threats.
4. Regression testing: Regression testing is used to verify that changes to SAP applications do not break existing functionality. It is typically performed after changes to SAP code, data, or configuration.

SAP testing can be performed manually or using automated tools. Automated testing can be more efficient and effective than manual testing, but it can also be more expensive to implement.

The frequency of SAP testing depends on the criticality of the SAP applications and the environment in which they are used. For example, SAP applications that are used in mission-critical environments may need to be tested more frequently than SAP applications that are used in less critical environments.

SAP testing is an important part of the SAP implementation process. By following the best practices for SAP testing, you can help to ensure that SAP systems are reliable, efficient, and secure.

Here are some tips for testing SAP:

1. Start early: The earlier you start testing, the more time you will have to identify and fix problems.
2. Involve users: Users are the experts on how SAP applications should work. Get their input early in the testing process to ensure that your tests are comprehensive and accurate.
3. Use a variety of testing methods: Don't rely on just one type of testing. Use a variety of methods to get a comprehensive view of the quality of your SAP applications.
4. Automate your tests: Automated testing can save you time and money. However, it's important to choose the right tools and to develop your tests carefully.
5. Document your tests: Documenting your tests will help you to reproduce problems and to track your progress.
6. Continuously monitor your SAP applications: Once your SAP applications are in production, you should continuously monitor them to ensure that they are performing as expected.

By following these tips, you can help to ensure that your SAP applic

OUR SERVICES:

Green Circle Cyber Security Solutions:

1 Integrated Security Solutions

2 Managed Services

3 Compliances & Consulting

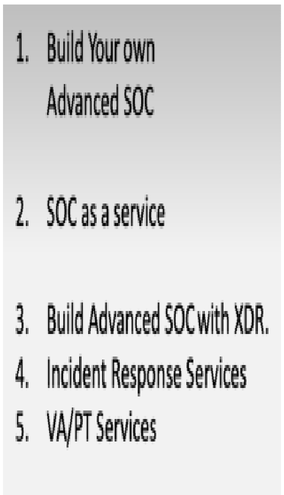
4 Security Education

Green Circle – Cyber security Solutions

(1)
Integrated Security

1. SIEM
2. WAF
3. Application security
4. Data base security
5. Email security
6. UTM
7. End point protection

(2)
SoC as a Service



1. Build Your own Advanced SOC
2. SOC as a service
3. Build Advanced SOC with XDR.
4. Incident Response Services
5. VA/PT Services

(3)
Compliances & Consulting

1. ISO 27001/2
1. PCI-DSS
2. HIPPA
3. SOC 2
4. Code Review
5. Building Security Maturity Model.
6. Cyber Security Consulting

(4)
Security Education Services

1. Policy & Awareness
1. Beginner / Advance Training
2. Educational cyber security Academy

Integrated Security

Our portfolio of ASOC solutions includes:

.1 Enterprise Governance and Cyber Security Support) Full Incident Lifecycle

.2 Securing networks and critical systems with real-time countermeasures

.3 SOC / Monitoring / Log / Operational / Security / Privacy Architecture Development

.4 Full Incident Response Lifecycle and Forensics Support to include fly-away team

.5. 24X7X356 Enterprise Managed Security Services Provider) MSSP (delivering Vulnerability Assessment Service ,Incident response , centralized management of antivirus measures and Security Log Management Service

Compliances and Consultation

1. Provide firms with compliance expertise required to meet tough regulatory demands.

2. Regulatory compliance oversight

3. Government advisory

4. Risk assessment and remediation

5. Business process and control improvements Internal and performance audits

6. ISO – 27001 HIPPA – SOC 2 – PCI DSS, Aramco SACS, SAMA, CBJ Cyber Framework.

Security Education

1. Embedding a culture of security within anorganization

2. provide a great way to educate personnel and keep the company's IT security policy fresh in their minds

3. Develop essential competencies ,new techniques and methods that are so essential in facing possible security issues.

4. Provide some level of maturity in incident response and help protect corporate resources ;by adopting an Security Familiarity Program ,a company greatly increases its security -related risk posture.

Managed Services

Advanced SOC can be provided as per below models:

1. Managed SOC
    1. Fixed cost
    2. Independently managed SOC

2. SOC as a Service (Cloud)
    1. With MDR/XDR.
    2. Incident Response Services.

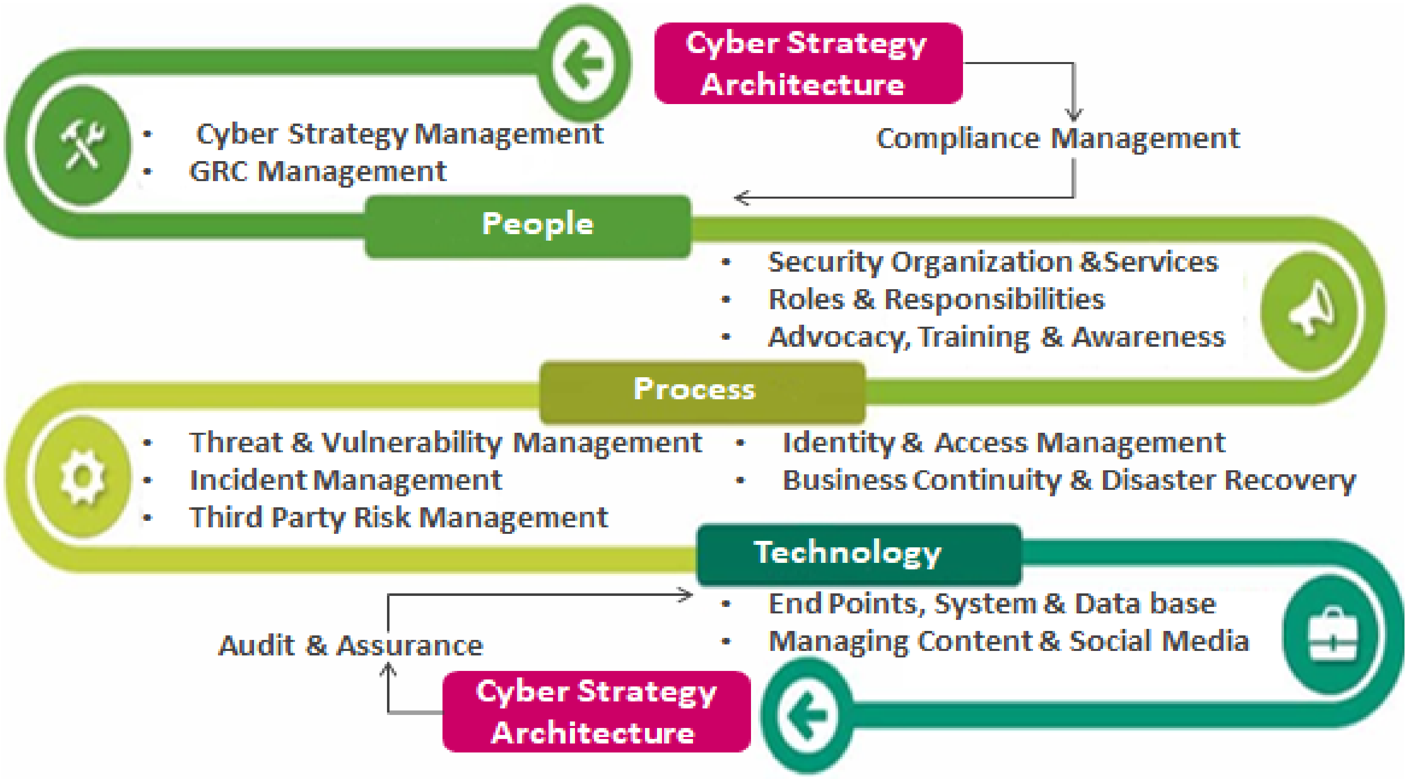
Consulting Services

Green Circle – Building Security Operation Center (SOC)

A SOC gives an organization the ability to anticipate and respond more quickly to threats, work more collaboratively and share knowledge more effectively. The SOC act as a *security-monitoring, detection and response* hub for the entire enterprise.
Here are 10 considerations for success:

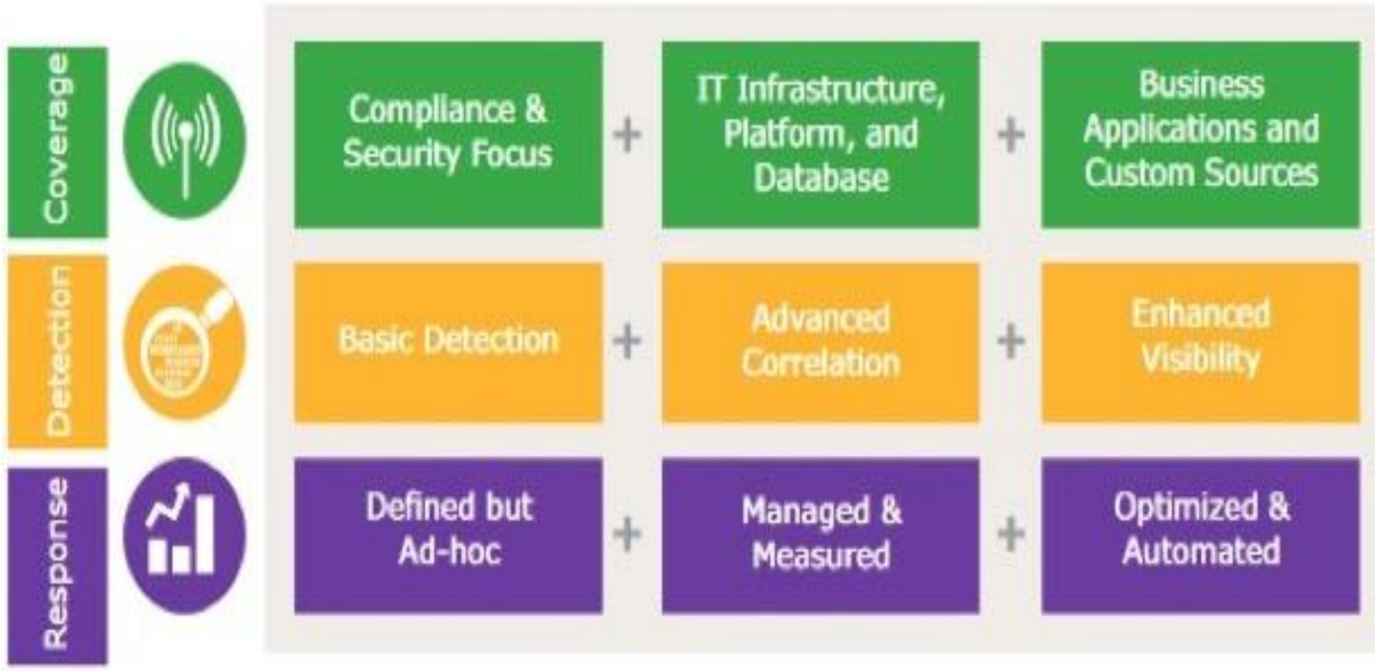
1-	Executives and board support
2-	Investment
3-	Strategy
4-	People
5-	Process
6-	Technology
7-	Environment
8-	Analytics and Report
9-	Physical space
10-	Continuous Improvement

Integrated Security change People, Process and Technology
You need to address all three areas – People, Process and Technology- to success.
Change it by addressing attitudes, procedures and tools.


Cyber Strategy Architecture
Compliance Management
Cyber Strategy Management
GRC Management
People
Security Organization &Services
Roles & Responsibilities
Advocacy, Training & Awareness
Process
Threat & Vulnerability Management
Incident Management
Third Party Risk Management
Identity & Access Management
Business Continuity & Disaster Recovery
Technology
End Points, System & Data base
Managing Content & Social Media
Audit & Assurance
Cyber Strategy Architecture

Green Circle – Building Security Maturity Model

To deliver modern use cases in a next-generation SOC,
the platform should support Big Data analytics and workflow- based response capabilities.
Analysis of information from various sources will eventually
improve endpoint and network visibility and enable enterprises to
facilitate advanced malware solutions.



Coverage	Compliance & Security Focus	+	IT Infrastructure, Platform, and Database	+	Business Applications and Custom Sources
Detection	Basic Detection	+	Advanced Correlation	+	Enhanced Visibility
Response	Defined but Ad-hoc	+	Managed & Measured	+	Optimized & Automated

SOC Maturity Model

GREEN CIRCLE

be aware..be secure

Thank You

www.grcico.com

00447898881982

00962792532833/00962770436404