CENTER FOR
SECURITY STUDIES
& CYBER DEFENSE

Curated Intelligence & Security Research

The Anderson University Center for Security Studies and Cyber Defense offers curated intelligence and security research for clients; including experienced review of documentation and security standards, suggestions for system security plans based on industry knowledge, and research for the best fitting security products.

AU CSSCD can review an organization's current policies and plans and advise them on what steps they can take to better protect themselves. AU CSSCD can also prepare reports on specific security products that organizations are curious about. These reports can contain information such as prices, names, reviews, benefits, and downsides of using the product, intended to inform an organization before a purchase..

Documentation and Security Standards Review

Systems Security Plans

Security Product Research

Benefits of Curated Intelligence and Security Research

A third-party review of currently implemented plans can help organizations identify and address potential vulnerabilities. Third-party reviews of documentation can help an organization reduce its attack surface by identifying and remediating any potential risks before a security incident occurs. Additionally, a third-party review of security products can identify unforeseen risks of purchasing a product or implementing it into an organization's current network infrastructure. This curated intelligence and research may prevent potential downtime due to unforeseen risks and prevent the likelihood of a successful cyberattack, saving an organization financial and reputational damages.

For more information, contact the Center for Security Studies and Cyber Defense at csscd.org or at csscd@anderson.edu.

CENTER FOR
SECURITY STUDIES
& CYBER DEFENSE

Penetration Testing

Penetration testing (pen-testing) is the process of executing a planned and sanctioned infiltration against a company's systems to find any weaknesses or misconfigurations. Penetration testing helps companies identify and remediate vulnerabilities and fulfill specific controls needed for compliance with identified frameworks such as PCI DSS and NIST.

The AU CSSCD offers penetration testing that includes planning, scoping, information gathering, vulnerability scanning, attacking and exploitation, as well as reports detailing the results of the penetration test. After action reports are designed to provide recommendations to clients about actionable methods to improve their security posture.

Planning and Scoping

Penetration Testing

Reporting and Remediation

The AU CSSCD utilizes cybersecurity tools such as Nmap, Metasploit, Tenable Nessus, Wireshark, and more to thoroughly perform reconnaissance, weaponization of vulnerabilities, and exploitation of threats to mimic real-world attacks; allowing companies to accurately assess their security risks.

Benefits of Penetration Testing

Regular penetration testing creates continual improvement of a company's security systems and will minimize any system downtime by identifying open vulnerabilities. Penetration testing can also help organization leaders in their risk management and budget planning.

For more information, contact the Center for Security Studies and Cyber Defense at csscd.org or at csscd@anderson.edu.

CENTER FOR
SECURITY STUDIES
& CYBER DEFENSE

Co-Managed SOC Operations

The Anderson University Center for Security Studies and Cyber Defense offers co-managed Security Operations Center (SOC) operations for clients, including Systems Information and Event Manager (SIEM) log analysis, suggestions for security improvement, incident response remediation, and provides incident reports after detecting and verifying anomalies. SOC operations provide clients with around-the-clock monitoring of security product logs and incident reporting.

AU CSSCD co-managed SOC operations can assist companies with monitoring events, deterring active threats, and remaining vigilant in protecting their security outlook.

Log Analysis

Improvement and Remediation Advising

Incident Reports

Benefits of a Co-Managed SOC

The CSSCD co-managed SOC assists companies in managing the functions of a SIEM or similar software with incident detection and prevention capabilities through log analysis. The CSSCD can help companies choose a SIEM that works for them, help monitor the chosen SIEMS from a central dashboard, and alert the company regarding potential threats; providing incident reports and actionable remediation suggestions.

Co-managed SOCs reduce the amount of work required to maintain security operations using a third party. Co-managed SOCs are designed to help companies find a balance requiring less resources to monitor their security on their own as well as less money than employing a managed SOC.

For more information, contact the Center for Security Studies and Cyber Defense at csscd.org or at csscd@anderson.edu.

CENTER FOR
SECURITY STUDIES
& CYBER DEFENSE

Security Awareness Training

The Anderson University Center for Security Studies and Cyber Defense offers security awareness training templates, advising, and tabletop exercises to improve clients' security awareness training practices.

A successful security awareness training program will inform employees of cybersecurity risks, threat identification, and best practices for "cyber hygiene". Proper training can reduce the success of an attack against a company and prevent downtime due to a security incident; potentially reducing the financial and reputational costs of a company due to a security breach.

Table-top exercises are a security exercise used by professionals in a variety of fields to test both personnel and active security protocols. These table-top exercise scenarios often include major, common threats to an organization's cybersecurity; allowing security teams to identify and remediate issues before an actual emergency incident arises.

Security Awareness Training Template and Advising

Controlled Simulations

Workshopping Security Policy

AU CSSCD can provide organizations with training policy templates. These templates, once filled out, can be used to show compliance with certain security frameworks, such as NIST. The AU CSSCD may also provide recommendations regarding security awareness training best practices and a sample program for each client. These scenarios are created to test the limits of personnel and current security policy plans alike. Tabletop exercises provide clients with valuable critical incident response experience. This experience occurs in a simulated environment; while testing real-world scenarios, controls, and relevant security protocols.

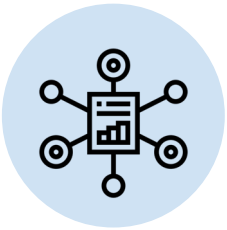
For more information, contact the Center for Security Studies and Cyber Defense at csscd.org or at csscd@anderson.edu.

CENTER FOR
SECURITY STUDIES
& CYBER DEFENSE

Cyber Audit Assistance

The Anderson University Center for Security Studies and Cyber Defense provides cyber audit assistance for clients to pre-assess a client's compliance with security standards such as NIST, ISO, and FedRAMP.

Audits are evaluations of the security posture within a company, ensuring that organizations meet necessary standards and compliances. There are several different types of audits within cybersecurity that organizations will need to pass to qualify for certifications. Third party vendors often conduct audits and can cost large amounts of money and time. The AU CSSCD offers audit assistance to ensure that organizations comply with the guidelines set by audits before the actual auditing process begins to ensure that any organization does not lose time or money to a poor audit check.



Relevant Framework and Security Standards Review

Framework and Compliance Audit Assistance

Remediation Advising

Benefits of Cyber Audit Assistance

Cyber Audit Assistance can benefit companies because it provides a low-cost way for companies to reduce the likelihood of failing a cybersecurity audit by validating their controls beforehand. Even if a company does not seek a certification, the AU CSSCD can review and validate a company's security controls; strengthening their cybersecurity practices, preventing the risk of a successful cyberattack, and reducing the likelihood of losses due to fines, reputational loss, or other financial damages.

For more information, contact the Center for Security Studies and Cyber Defense at csscd.org or at csscd@anderson.edu.

CENTER FOR
SECURITY STUDIES
& CYBER DEFENSE

Table-Top Exercises

The Anderson University Center for Security Studies and Cyber Defense offers table-top exercises for clients to assist with security awareness training. A table-top exercise is a role-playing activity where participants, assigned critical function roles, respond to scenarios presented and managed by facilitators.

Table-top exercises are a security readiness tool utilized by professionals in a variety of fields to test both personnel and active security protocols. Scenarios often include both major and minor threats to an organization's security posture, allowing exercise security teams to remediate identified issues before an actual critical incident.

Controlled Simulations

Workshopping Security Policy

In addition to assisting clients in developing security awareness training and policy, the AU CSSCD develops table-top scenarios to exercise an organization's security strategy. They are beneficial because they evaluate a client's administrative controls and measure the effectiveness of identified protocols such as incident response and business continuity.

Table-top Exercises are designed to test the limits of personnel, security protocols, and incident response plans alike. Exercised personnel often gain valuable experience and insight through participation in a simulated event relevant to their area of expertise. Table-top exercises incorporate a learning-centric focus, where participants can have open conversations, take notes, and generally have space to learn more about security solutions.

For more information, contact the Center for Security Studies and Cyber Defense at csscd.org or at csscd@anderson.edu.