Aplura, LLC
5653 Blithaire Garth
Columbia, MD 21045
301-523-2110 (w)
410-864-8386 (f)

Focused Information Security
www.aplura.com

Aplura Security Assessment

Service Overview

About Aplura

Aplura, LLC is an information security consultancy offering comprehensive services in information security architecture, research, vulnerability assessment, penetration testing, computer incident response, security policy and procedure development, and security intelligence. Aplura's consultants perform information security engineering and analysis on three continents and for a variety of industries, including:

- Federal and state governments
- Education and research
- Service providers
- Military and commercial entities

Aplura's engineers have developed procedures for measuring the risk and effectiveness of IT infrastructure and security controls. This methodology results in a thorough understanding of the security posture of each of our clients, highlighting deficiencies in technical controls.

Aplura distinguishes itself as a leader in the industry above other security companies by providing excellent security analysis and not simply standardized reporting techniques. Our reports include actionable steps that our customers can perform immediately to reduce risk to their organizations. Aplura's consultants are credentialed security professionals who practice proven industry techniques to remediate real information security threats. Additionally, we make our customer's job easy by providing a series of *prix-fixe* menus featuring a breakdown of services and price. Our clients know exactly what to expect and what it will cost them after our very first meeting .

Organizational Goals

Aplura customizes its approach for each project, basing our security review specifically on our customer's unique organizational goals. These goals are considered with every piece of data we collect, interview we hold, and report we write.

Here are some examples of possible organizational goals and applicable validations we can monitor.

Organizational Goal	Example	Technical Validation
Maintain a positive public image	Stay out of press due to embarrassing security incident	Validate publicly available systems and ensure an effective incident handling procedure
Reliability of public IT systems	Internet-accessible Web applications should minimize unplanned downtime	Assess DMZ architecture, audit Web application for vulnerabilities, evaluate use/effectiveness of production environment, ensure effective Business Continuity Plan in practice.
Efficient use of network resources	Inefficient configurations and violations of acceptable computer use policies that cause unnecessary network load	Use a custom packet-capture system to "tap" into the network and collect traffic samples to determine usage. Evaluate network configurations to ensure accuracy.
Curtail corporate espionage or foul play	Ensure data integrity and reduce information leakage	Validate strict egress filtering and use of proxies for all interaction with users. Evaluate user's digital workspace, including: standard desktop image, strong desktop technical controls, and appropriate VPN policy and configurations.
Confidentiality of private data	Protect against unauthorized disclosure of corporate data	Validate strong network access control policies. Perform rogue (wired and wireless) detection. Implement ongoing rogue-detection program. Scrutinize data egress. Evaluate extrusion detection.

Engagement Objective

The overall objective of the engagement is to provide the customer with a thorough analysis of its existing architecture and evaluate its technical controls. Specific focus is made to technical controls supporting the customer's organizational goals.

Site Review

Aplura's engineers analyze the security of the customer's network architecture, use of standard networked services, and effectiveness of security controls.

Aplura analyzes the technical architecture by reviewing documentation and configuration, and conducting interviews with key staff. This provides Aplura with insight into the client's operational environment, thus allowing our recommendations to address specific IT Security needs.

During portions of the review, Aplura engineers require access to perform live work on the customer's network. This work involves passively monitoring network activity using packet-capture software, or actively scanning using vulnerability assessment software. Aplura consultants work closely with the customer's IT staff to minimize the likelihood of a negative impact on systems and applications. These reviews help to identify significant gaps in the security posture of an organization, along with specific recommendations for addressing the most high-risk concerns.

Incident Response

In the event that the security assessment uncovers an active network attack, Aplura engineers will notify the primary contact immediately. With the approval of the customer, Aplura can provide support in detecting the source vector of the attack, collecting evidence for later prosecution, repelling the attack, and recovering the affected system when possible. These services, while outside the scope of the security assessment, provide a more comprehensive coverage of our customer's needs.

Final Report

The final report includes specifics about the customer’s organizational goals and business model as well as standard criteria reporting.

The customized report is tailored to the client’s environment with practical recommendations that, when implemented, will improve IT security posture. Aplura engineers help organize and prioritize the identified risks. This allows the customer to reduce the exposure of critical assets as quickly as possible. Aplura consultants can help the customer to address the specific remediation as part of a separate contract. In the case of high-risk exposures, Aplura makes every effort to close the gap as swiftly and safely as possible through a separate agreement.