DATA SHEET

OWL Cyber Defense

Security Architecture Assessment

Owl provides a comprehensive security assessment of system architecture and configuration for a multitude of clients including: U.S. Defense, Intelligence, Civilian Government, and Critical Infrastructure platforms and networks. Since its inception in 1999, Owl has established itself as a leader in advancing fundamental platform security technology and applying security technology to solve real-world problems. Our experience in all aspects of operating system and platform security, including fundamental technology research and development, tool development, policy development and analysis, solution design, implementation, and testing provides an edge when it comes analyzing your solution security needs.

Benefits

An insecure design can't be made secure by applying security as an afterthought. By engaging with Owl early in the development lifecycle, we can help you start with a secure architecture, and provide guidance on how to implement that architecture in a secure manner. This "built-in security" approach provides assurance that your solution meets the security objectives, and will ultimately reduce the cost of developing, testing, and certifying your product.

Having Owl perform an assessment demonstrates genuine concern for building secure solutions that meet unique requirements, and provides your customers with reassurance that the solution meets their security needs. Where appropriate, the assessment report can form the foundation for the system certification and accreditation activities.

Quick Turnaround

Owl's agile approach and reporting allows you to quickly address any gaps in your architecture and system design. The turnaround time for a security architecture assessment engagement is four weeks in most cases.

Reliable Performance

Owl's CASCADE, our enterprise quality management program, is based on the Carnegie Mellon Capability Maturity Model Integrated (CMMI), the IBM Rational Unified Process (RUP), the Eclipse Foundation Eclipse Process Framework (EPF) Open Unified Process (OpenUP), and other best of breed industry standards (e.g., ISO 9000, Project Management Body of Knowledge). CASCADE allows us to align resources and schedules to meet your requests and effectively manage the cost and schedule for each engagement.

COMMERCIAL

Strong security is not only for traditionally risky environments – risk is everywhere. Your customers want to know that they can trust your product or application. Having Owl perform a security architecture assessment of your design gives you the confidence that your solution won't become their problem.

CRITICAL INFRASTRUCTURE

In addition to enterprise and mobile application ecosystems, Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS) are part of the unique risk profile for Critical Infrastructure. Owl can help you understand how your systems help satisfy Government and Industry security guidance requirements.

GOVERNMENT

The Government has stringent security requirements, often driven by specific guidance. Owl has worked with US Government security standards as a developer and an evaluator for more than ten years. Among others, our expertise includes the DCID 6/3, and the NIST Risk Management Framework (RMF), including NIST SP 800-53. Owl can help ensure your design satisfies those requirements, and can give you a foundation for entering the RMF process.

OUR APPROACH

Everyone interested in security understands the benefits of evaluating system architecture early in the development lifecycle. As developers ourselves, Owl is uniquely qualified to collaborate with customer product teams at every stage of the lifecycle to produce secure system architectures and develop trustworthy solutions.

INITIAL SECURITY ARCHITECTURE REVIEW

Our experienced security engineers will review your planned or existing security requirements, system architecture, usage configuration, and concept of operations (CONOPS) to derive security relevant information, identify solution specific characteristics, and gather background information to facilitate an onsite assessment.

ONSITE ASSESSMENT

To validate our understanding of the system from our initial security architecture review, we will engage with your team for an in-depth discussion of the security requirements and your planned solution.

INITIAL REPORT

Using the information obtained during the security architecture review and onsite assessment, we will map your security objectives against the existing system architecture. This report will identify gaps in achieving the goals and recommend solutions to address any gaps.

TELECONFERENCE FOLLOW-UP

After submitting our initial report, we will hold a teleconference with your team to discuss any comments or questions you may have about the initial report. Our goal is to make sure the conclusions we document are accurate and relevant, and that you understand what they mean for your way forward.

FINAL REPORT

After the teleconference discussion, we will update the initial report to address your comments and questions. Want to learn more about our Security Architecture Assessment offerings and how they can help you?

SECURED BY OWL

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com