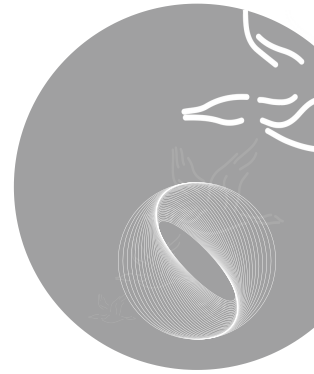


MERIMETSO

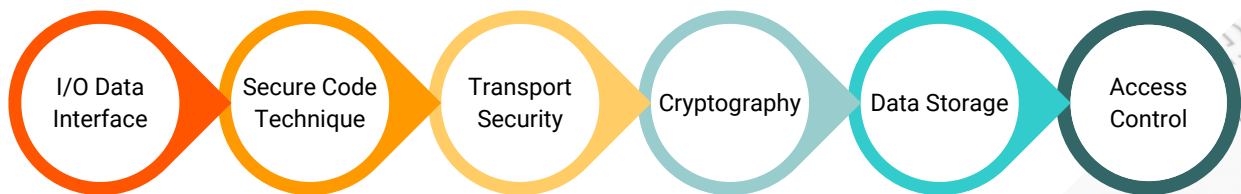
Product Code Review



Service Description Introduction

A code review will be conducted on any product source code. This will involve detailed analysis of the code and will output a list of vulnerabilities and areas where best secure code design practice can be improved. Specific and general mitigation and remediation options and ongoing consultancy to resolve these issues. Providing a secure product to your customers requires a good understanding the types of threats that are prevalent in the industry today, how your product can be attacked and a full understanding of all the software used to build the product. With the shortage of cyber security skills in the industry and the increased time to market pressures, building and maintaining this knowledge and the expertise is critical

Our Approach



Engagement Structure

From an electronic copy of the source code, a senior security consultant with in depth programming and secure development experience will review the code.

Methodology

Input/output Data Interfaces

Manual code tracing and automated testing to locate application interfaces and review sanitisation of input or output data. This testing is designed to locate potential injection vulnerabilities that may allow an attacker to send malicious input that affects the application execution flow.

Secure Coding Techniques

Further analysis will be performed to identify sections of code vulnerable to issues such as format string errors, race conditions, memory leaks, buffer overflows, integer overflows or command injection points.

Transport Security

Manual examination will be performed on the protection mechanisms for the network traffic. Improper use of PKI and SSL/TLS validation vulnerabilities will be investigated.

Cryptography

Code will be verified for cryptographic implementation errors that could affect the confidentiality and integrity of data: weak password generation systems, weak random number generators and incorrect use of high level cryptographic primitives.

Data Storage

A review will be conducted to test the protection measures for sensitive data storage. Including compliance with data protection regulations, suitable use of operating system or platform storage mechanisms. Storage of personally identifiable information and appropriate storage of application sensitive security tokens or keys.

Access Control

A review will be carried out to ensure that proper permissions are in place for interfaces, including IPC interfaces, network interfaces requiring authorisation / authentication, and filesystems.

Deliverables

In-depth report, broken down into 3 main parts:

1. Management Summary
2. Technical Overview
3. Detailed Technical Findings

Highlighting the vulnerabilities:

1. Type of RISK
2. The EFFECT of that RISK
3. Recommendations on how to address and mitigate vulnerabilities
4. Estimate of effort required to remediate any vulnerabilities identified

Project Management

Project Management resource will be assigned throughout the engagement but will not be allocated full time.

Key roles and responsibilities:

- Run engagement kick off workshop.
- Run engagement closure.
- Maintain and communicate engagement risks and issues log.
- Weekly status meetings and engagement tracker.

Prerequisites

The following pre-requisites are required from the client:

- Physical access to the device or exported configuration files
- Make and Model of the Firewalls
- Written permission from the client to test
- Login credentials and digital certificates (if applicable)
- Point of Contact details

Deliverable Acceptance Criteria

Merimetso may present interim deliverables to the customer for review throughout the engagement. Should Merimetso present an interim deliverable, the customer will review, and either accept, or document specific corrective items in writing within three (3) business days. In the absence of any comments, deliverables produced by Merimetso will be deemed accepted after three (3) business days.

Limitations & Exclusions

- This engagement covers only the activities detailed in this document. Additional Merimetso offerings may be purchased as add-ons, otherwise additional consulting work not contained in this engagement is deemed out of scope.
- Working time is defined as Monday to Friday (excluding local bank/statutory holidays), 9am-5pm, with a 60-minute break for lunch.
- Merimetso is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities.
- Only third-party software and infrastructure identified during the pre-sales phase will be in scope for the engagement. There will be no change of scope where third-party software or infrastructure has been changed by the customer during the course of the engagement, or this will incur additional cost.

Customer Responsibilities

1. The customer must provide appropriate resources during the engagement from commencement date.
2. The customer must provide Merimetso representatives with information and resources to ensure Merimetso is able to successfully execute the engagement. This can include, without limitation, providing access and credentials to systems, completing installation prerequisites, providing resources, and attendance in planning, execution, or training meetings.
3. Customer will ensure resources are available in a timely manner to undertake tasks such as change control and documentation review.
4. Customer must ensure it has the necessary escalation and communication channels to resolve any blockers in a timely manner, including dependencies on third parties customer vendors, suppliers, and consultants.
5. If the consultant should travel to a customer location for the delivery of this engagement, there will be additional travel and expense costs. These travel and expense costs can be paid for prior to the engagement, or at actuals, at engagement completion.
6. The customer shall provide at least seventy-two (72) hours' notice for the cancellation or postponement of any work already scheduled as part of the engagement. In such scenario of a cancellation or postponement Merimetso reserves the right at its sole discretion to charge the customer for additional resources at Merimetso's then current daily rate for the delay period.
7. Customer must have a right to use the software and licenses. This requires that the customer must have purchased, or have converted, the appropriate license rights to the target environment.
8. Hardware requirements are the responsibility of the customer, and it is the customer's responsibility to ensure the hardware requirements are met prior to the engagement.

Merimetso may subcontract all or a portion of the services and/or have the services performed by one of its affiliates.

Note: The services described in this Service Description are subject to the terms and conditions by Merimetso Terms

Our Senior Testing Team

Dr Andrew Blyth - Founder and Director of R&D



Dr Blyth received his PhD in Computer Science in 1995 from Newcastle University, UK. Dr Blyth held the position of Professor of Computer Forensics at the University of South Wales, UK, throughout his illustrious career. Co-authored a textbook on Information Assurance, supervised 15 successful PhD candidates, created several BSc and MSc Computer Forensics and Cybersecurity Programmes. He was instrumental in the University of South Wales being the first University in the UK to have an MSc in Computer Forensics accredited by the UK Government's National Technical Authority (GCHQ/NCSC).

He was the Cybersecurity Technical Lead at the UK Ministry of Defence's (MOD), Defence Science and Technology Laboratory (DSTL). During that time, he created and ran the Computer Network Defence Technical Demonstrator programme and defined various other research programmes within DSTL. He has over 50 peer-review publications and managed millions of dollars of research funding.

Campbell Murray - Founder and COO



Campbell is an established global leader in the field of information security. With over 25 years of experience ranging from offensive security assessments and security engineering in a vast range of environments providing Campbell with rare detail and insight into the field of cybersecurity. Campbell established himself as a penetration testing consultant in 2000. A firm believer in knowledge transfer, Campbell was a founding director of the TigerScheme in 2007 and the Cyber Scheme in 2013.

The Cyber Scheme is the recognised course used by NCSC to affirm CHECK status on any penetration tester who wishes to work on Government infrastructure in the UK. Campbell is now the chair of the technical panel for the Cyber Scheme and is one of only a handful of GCHQ appointed CHECK Team Leader assessors.

David Mound - Founder and CTO



David is a highly experienced Cyber Security Researcher with a demonstrated history of working in the Computer & Network Security industry and threat intelligence. Skilled in Penetration Testing, Reverse Engineering, Computer Forensics, Red Teaming and Threat Intelligence, he has worked with numerous global agencies within the 5 Eyes community, including GCHQ and the NSA delivering, advising on Red Team methods and engagements to assess Blue Team capabilities.

David's current speciality and focus are cloud-based technologies, and he holds multiple cloud certifications such as AWS Certified Security Specialist. David is an ex-Naval officer and is currently a member of the Army Reserves, where he coordinates threat hunting and assists network defence within the UK MOD and Gov estates. David brings his extensive technical capability to design the innovation to the Merimetso Cyber Technical Training platform.