Not remediating the constant stream of new vulnerabilities in your computing operations and applications is a great way to ensure you will suffer expensive cyber-attacks.

Intensive vulnerability scanning and analysis, therefore, is an essential part of preventing these attacks. But far too often vulnerability reports are difficult and time-consuming to use.

Practical Cyber's service solves that problem. We provide custom, easy-to-use reports that deliver outstanding value.

INTRODUCTION

Practical Cyber provides high-quality, intensive vulnerability scanning and analysis for your overall computing operations and/or for your web and mobile applications. Our intensive engagements combine the best available scanning tools with decades of experience to provide easy to use, custom vulnerability reports that make it much simpler for you to remediate your vulnerabilities.

OUR METHODOLOGY

One of the biggest problems with vulnerability scanning reports is that they are hard to read and even more difficult to use to efficiently remediate your vulnerabilities. We, therefore, created a better approach that produces easy-to-use custom reports that provide outstanding value.

We begin by thoroughly understanding the following:

1. Your computer operations and/or applications;

2. Your goals for the scanning and analysis; and

3. How you want to leverage the results.

This information enables us to provide a custom report that will allow you to achieve your results most easily.

Our second step is properly configuring and using the best available tools to scan your computer operations and/or applications. This produces the raw, overall data we need for step 3.

In step 3 we diligently use our decades of expertise to review the overall results from the scanning tools to create a custom, easy to understand and use vulnerability report.

HOW WE APPLY OUR EXPERTISE:

Properly configuring and using the best scanning tools is essential. But these tools produce an overall set of raw results that can include many false positives and be difficult to understand and use to remediate your vulnerabilities. We, therefore, apply decades of experience to diligently analyze the results and produce the best possible custom report that:

1. Reduces false positives.

2. Uses clear language to make it easy to understand how to remediate vulnerabilities and prioritize your remediation.

3. Saves you a lot of time and headaches when using the report to remediate your vulnerabilities.

PRACTICAL CYBER'S MULTIDISCIPLINARY TEAM

Cybersecurity & Computing Continuity Expert – Dr. Marc Rogers.

Internationally known cybersecurity expert and founder of MKR Forensics.

Tenured Cybersecurity Professor and Executive Director of the graduate and undergraduate cybersecurity programs at one of the top university cybersecurity departments in the world.

25+ years practical cybersecurity experience enhanced by academic career & access to talented graduate students and alumni with excellent practical experience.

Device, Cyber & Privacy Law + Cyber Risk Expert – Elliot Turrini, JD.

Former federal cybercrime prosecutor, cyberlaw/privacy attorney in private practice, & tech company General Counsel.

Cyber risk mitigation & transfer expert – both insurance and contract.

Co-Editor & Author of Cybercrimes: A Multidisciplinary Analysis.

Cybersecurity Researcher, Practitioner, & Pragmatist – Alissa Gilbert Ph.D. Candidate.

Nationally ranked ethical hacker. Highly skilled vulnerability tester.

One of the top cybersecurity researchers in the United States. Many years of practical experience protecting organizations from cyber-attack

COO of CircleCityCon, an elite cybersecurity conference.

Ph.D. candidate and instructor at Purdue University.

To learn more, email Elliot Turrini at Elliot@PracticalCyber.com.