QOMPLX:CYBER

Offensive security service

Tailored engagements, white glove service

> We need to get a pen test

> Should we have someone review our site for vulnerabilities?

If any of the above sounds familiar then you know how hard it can be to find the right team to assess your business critical systems. How do you know which service is right for your security program and who you can trust to give you the confidence and insights you need? Our Offensive Security Services are conducted by leading security experts in an innovative, approachable, and friendly way.

Why choose us?

We are recognized experts

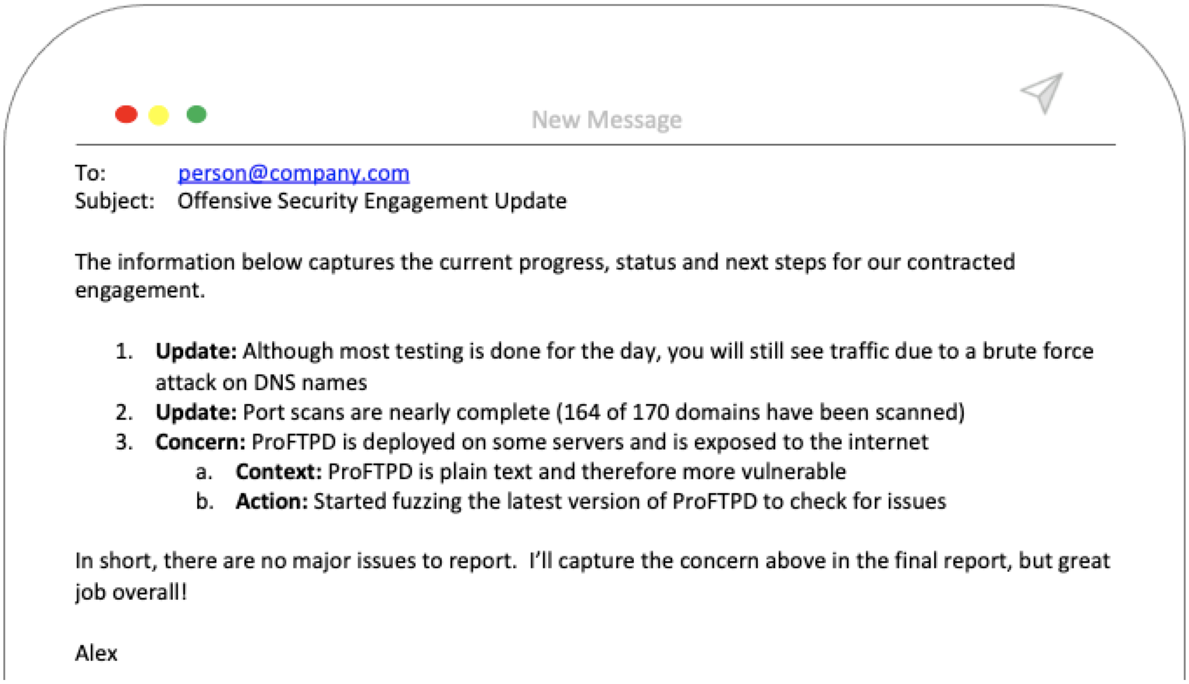
Our Offensive Security Service team is led by world-renowned offensive security researcher, Alejandro (@_hyp3ri0n) Caceres. He rose to prominence through the launch of PunkSPIDER, the world's first internet scale web vulnerability search engine. Since then he's gone on to lead a team of offensive security experts who have worked with DARPA and IARPA, among other entities. They've created the most comprehensive extant sensing and internet device scanning tool, compiled extensive breach data sets, developed and published 0-day exploits, built dark web scanners, and numerous OSINT tools. These tools enable faster and more complete reconnaissance, the capability to leverage known and unknown vulnerabilities and exploits, as well as the uncommon ability to crawl the dark web in search of sensitive information traffic pertaining to your enterprise.

We are an extension of your team

What if you could have a friendly hacker sitting next to your team ready to answer any questions and offer advice on securing systems? Our team is ready to answer your questions throughout the engagement in a friendly and approachable manner — we call this the *“hacker buddy”* approach.

We give continuous updates of findings

Most of our competitors leave you in the dark, leaving you wondering how the engagement is going and worrying what they might find. You only hear from them in the beginning of engagement and then again at the end when they deliver a report; our approach is different. Our experts will provide constant updates to inform you of not only what tests we’re performing but also any findings...



To: person@company.com
Subject: Offensive Security Engagement Update

The information below captures the current progress, status and next steps for our contracted engagement.

1. **Update:** Although most testing is done for the day, you will still see traffic due to a brute force attack on DNS names
2. **Update:** Port scans are nearly complete (164 of 170 domains have been scanned)
3. **Concern:** ProFTPD is deployed on some servers and is exposed to the internet
    a. **Context:** ProFTPD is plain text and therefore more vulnerable
    b. **Action:** Started fuzzing the latest version of ProFTPD to check for issues

In short, there are no major issues to report. I’ll capture the concern above in the final report, but great job overall!

Alex

Defenders love us!

With our consistent updates we make the Blue Team look good! For ***penetration tests*** our team will provide details of what we’re testing for the day and the methods we’re using. This allows the Blue Team to train on attack detections and response. It also allows defenders to get ahead and fix any findings before the final report is delivered. By the time the executive staff sees the final report your team can be well into remediation.

For ***Red Team engagements*** we insist on out-briefing the Blue Team first. The Red Team is only successful if the Blue Team gets better at detection and response. We want to work with your Blue Team until they can successfully defend your network against any of our attacks.

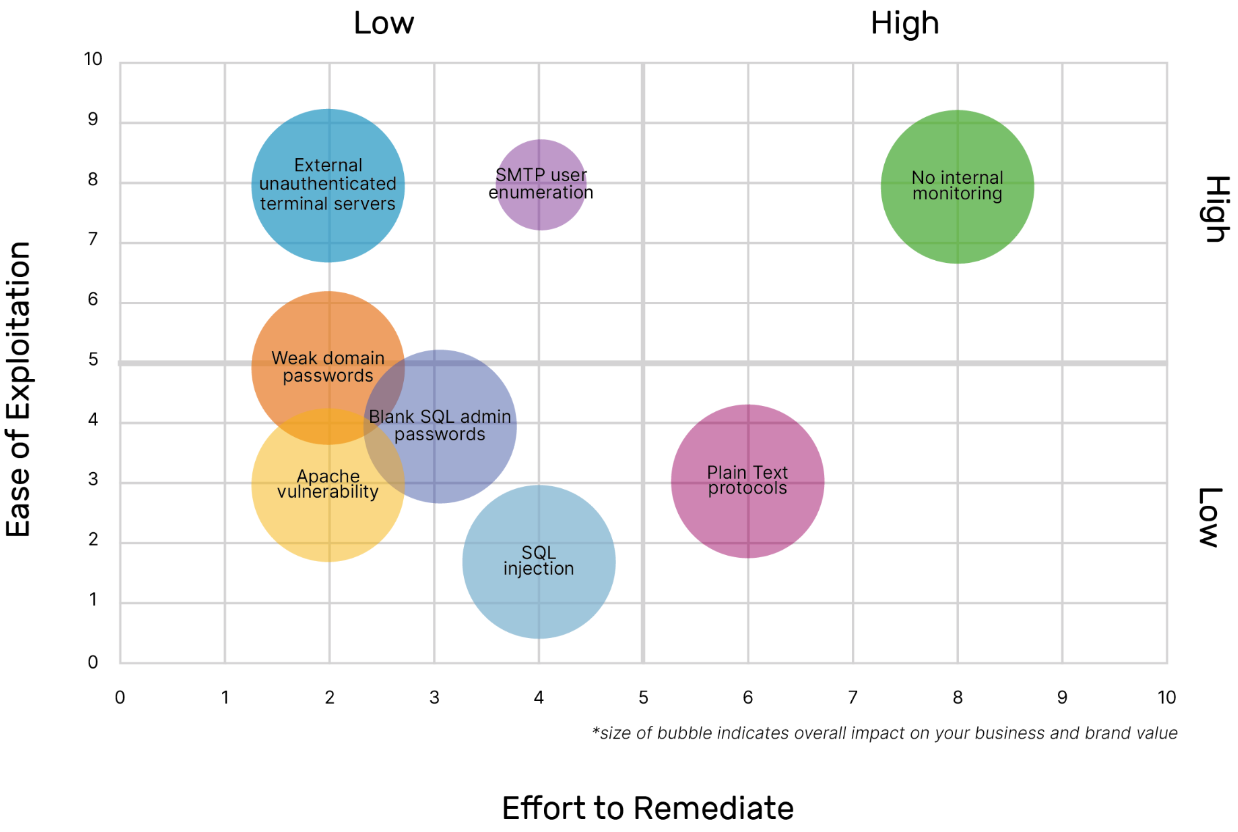
We are happy when your defenders look like "Rock Stars"

We highlight what's working

It is just as important to know what your team is doing right as well as any areas that need improvement, and that's why we include positive security findings and trends in our reports.

We prioritized findings by business impact

Our resource deployment strategic consulting focuses on getting the most out of your financial, infrastructural, and human resources. We use a simple Business Impact Matrix to provide you with reasonable paths forward, removing complexity for your team.



Our approach is comprehensive

Common	Above and Beyond	Specialized Needs	Action Output
Expert reconnaissance	0-day hunting	Internet of things	Priority remediation order
Attack vector ID	Fuzzing	Social engineering	Severity scoring
Targeted exploits	Reverse engineering	Phishing	Speed of remediation scoring
Prioritized remediation	Distributed denial of service	Compliance penetration testing	Cost to remediate scoring
Web app and network	Custom malware/AV testing	Physical penetration testing	Complexity of remediation scoring
	Deep prioritization	Mobile device	
	Constant communication		

Ready to learn more about *QOMPLX Offensive Security-as-a-Service*? Contact us today.

+1 (703) 995-4199 | info@QOMPLX.com | www.QOMPLX.com

Why QOMPLX®

QOMPLX is the cloud-native leader in risk analytics. We help organizations make intelligent business decisions and better manage risk through our advanced, proprietary analytics platform. We are the leaders at rapidly ingesting, transforming, and contextualizing large, complex, and disparate data sources through our data factory, in order to help organizations better quantify, model, and predict risk in areas like cyber security, insurance, and finance. QOMPLX is headquartered in Tysons, VA with offices in New York, Denver, London, Cambridge, Oxford, and Montevideo. More information about QOMPLX can be found at www.qomplx.com.