RED TEAM

OFFENSIVE SECURITY

Der Red Team-Service von IMQ Intuity betrachtet Unternehmen mit den Augen eines „Hackers “ und simuliert einen echten Angriff. Er hilft seinen Kunden zu überprüfen, ob ihre Sicherheitsstrategie wirksam ist, um einem Cyberangriff der neuesten Generation entgegenzuwirken.

Der Red Team-Service von IMQ Intuity verkörpert den Denkprozess echter Angreifer und verwendet ihre eigenen Techniken. Er untersucht alle Aspekte der **Security Posture des Unternehmens**: Netzwerkinfrastruktur, Anwendungssicherheit, menschliches Verhalten, physische Sicherheitskontrolle und Geschäftsprozess.

Für den Kunden stellt es eine Gelegenheit dar, seine Sicherheit zu erhöhen und seine Erkennungs- und Reaktionsfähigkeiten zu verfeinern, indem er ein größeres Bewusstsein für die von echten Angreifern verwendeten Techniken und Verfahren erwirbt.

DER RED TEAM-SERVICE SIMULIERT EINEN ECHTEN CYBERANGRIFF, INDEM ER DIE SICHERHEITSTECHNOLOGIEN UND -DIENSTE DES KUNDEN UMGEHT.

IMQ INTUITY SRL | info@intuity.it | intuity.it/de
Headquarters Via A. Ceron 2, 35129 | +39 049 817 0850 | **Registered Office** via M. F. Quintiliano, 45 - 20138 Milano

ANGRIFFSARTEN

OSINT
IMQ Intuity führt dank des Einsatzes besonderer Techniken wie Open Source Intelligence (OSINT) eine gründliche Suche nach Informationen über das Unternehmen durch, die zur Vorbereitung eines Angriffs genutzt werden können oder die selbst ein Risiko für das Unternehmen darstellen.

INFRASTRUCTURE ATTACK
Das Red Team versucht, die Unternehmenssicherheit zu durchbrechen, indem es Schwachstellen ausnutzt, die auf die Infrastruktur zurückzuführen sind oder, wie es zunehmend der Fall ist, in Webanwendungen vorhanden sind.

HUMAN ATTACK
Unternehmen mit den Augen des Hackers zu betrachten, bedeutet auch, den menschlichen Faktor als auszunutzende Sicherheitslücke zu betrachten. Daher umfasst der Red Team-Service Aktivitäten im Bereich Social Engineering, wie z. B. Phishing, Impersonation, und Baiting.

PHYSICAL ACCESS
Manchmal kann ein unbefugter Zugang auf Bereiche oder Räumlichkeiten das Unternehmen erheblichen Risiken aussetzen. Aus diesem Grund zielt der Red Team-Service darauf ab, die Wirksamkeit der vom Unternehmen eingeführten Kontrollen überprüfen. (Aktivität nicht im Service „Hack-In-A-Day" enthalten).

PROCESS EVALUATION
Die vom Red Team-Service erzielten Ergebnisse ermöglichen es, die Angemessenheit von Geschäftsprozessen aus IT-Sicht anhand objektiver Daten zu überprüfen und die kritischen Probleme hervorzuheben, die sich auf die Sicherheit auswirken.

WHITEBOARD ATTACK
Diese Aktivität wird in Form eines «Rollenspiels» durchgeführt, bei dem Angreifer (IMQ Intuity-Spezialisten) und Verteidiger (Kunde), um einen Tisch sitzend, sich gegenseitig herausfordern, ihre jeweiligen Ziele zu erreichen, wobei sie ihre eigenen Strategien anwenden. (Aktivität nicht im Service „Hack-In-A-Day" enthalten)

DAS VERFAHREN

Der Angriffsmodus der Red Team-Service ist vom Typ BlackBox, der keine anfängliche Weitergabe von Informationen über das Ziel und keine Art von Autorisierungs- oder Zugriffsinformationen vorsieht. Diese Art von Modus ermöglicht es IMQ Intuity, das Ziel so zu „sehen", **wie es ein externer Angreifer sehen würde.**

Der direkte Vergleich mit dem IMQ Intuity Red Team ermöglicht es dem Kunden, seine Aufmerksamkeit auf echte Sicherheitsvorfälle zu lenken, seine Fähigkeit zu testen, anomale Aktivitäten zu erkennen und zu blockieren.

Der Service **Hack-In-A-Day** simuliert einen eintägigen Cyberangriff und nutzt dabei die wichtigsten Vorgehensweisen des **Red Teams**.

Der Service ermöglicht zu beweisen und zu dokumentieren, welche Unternehmensschwachstellen ein „Hacker" an einem einzigen Tag ausnutzen könnte und welchen potenziellen Schaden er Ihrem Unternehmen, Ihrer Infrastruktur oder Ihren Mitarbeitern zufügen könnte.

Ziel des Service ist es, seinen Kunden einen ersten Überblick über das Schutzniveau des Unternehmens hinsichtlich der Informationssicherheit zu geben und zu verstehen, wo man eingreifen muss, um es zu verbessern.