Vollautomatisiertes Sicherheitsassessment für
Behörden-, Ämter- und Unternehmensumgebungen

Vulidity?

In Ihrem Netz wurde gerade der Anhang einer Mail geöffnet…

Stellen Sie sich eine Welt vor, in der IT Sicherheit mehr als nur eine Kostenstelle ist

Wir geben jeden Tag alles, um Ihnen diese Erfahrung zu ermöglichen

War Vulidity ein Gedankenblitz?

Nein!

Ausführliche Marktanalyse zusammen mit dem Forschungsbereich, Behörden und Unternehmen.

Das Ergebnis war, dass Administratoren keine neuen Firewallfeatures oder noch einen Schwachstellenscanner mit zusätzlichen Buzz-Words brauchen, sondern ein Werkzeug, das ihm unabhängig von seinen Fähigkeitslevel tatsächlich zeigt, ob seine Infrastruktur in realen Situationen standhält und Mitarbeiter genug Bewusstsein gegen Social Engineering besitzen.

Warum?

Die Vision von Vulidity ist es Behörden, Unternehmen und NGOs endlich ein Werkzeug an die Hand zu geben, damit diese ..

- .. ihre Infrastruktur in realen Szenarien testen können
- .. ihr Sicherheitskonzept auf Praxisfähigkeit analysieren und fehlende Prozesse und Strukturen erkennen können
- .. ein solides Sicherheitsniveau aufbauen können

Ein Komplettpaket

Vulidity bildet die drei wichtigsten Angriffsvektoren der heutigen Zeit ab. Es ist ein Softwarebundle, welches als HW oder virtualisierte Lösung nahtlos in Ihre Firmenumgebung integriert werden kann

-

Es funktioniert out-of-the-box und benötigt keine Schulung!

Vulidity Module

01

OSINT

Welche sensiblen Informationen bzw. Daten sind über Ihr Netz frei erhältlich?

02

Social Engineering

Trainieren Sie die größte Schwachstelle jedes Netzwerkes mit vorgefertigten Szenarien und Kampagnen - den Mensch!

03

Netzanalyse

Überprüfen Sie, ob die Aussagen Ihres Firewall- bzw. IDS-Herstellers der Wahrheit entsprechen!

Social Engineering

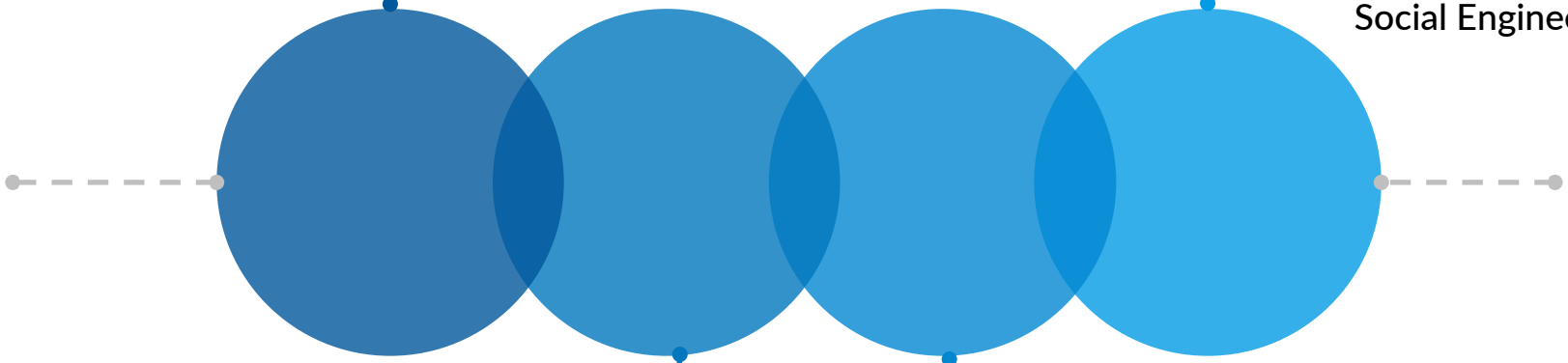
Echte Szenarien die ihre Mitarbeiter nachhaltig und effektiv schulen

USB Szenarien

Erstellen Sie automatisiert präparierte USB Sticks für Szenarien wie z.B. USB Dropping

Automatisierung

Überlassen Sie Vulidity die Verwaltung von regelmässigen Aufgaben und die Erstellung von Social Engineering Kampagnen



Mail Szenarien

Erzeugen Sie durch vordefinierte und gefälschte E-Mail Nachrichten, ein realistisches Social Engineering Szenario

QR Szenarien

Benutzen Sie QR Codes um Social Engineering Angriffe durchzuführen

Open Source Intelligence (OSINT)

File Extraction
Analysieren Sie, welche Dateien aus Ihrer Domain öffentlich verfügbar sind

Geleakte Informationen
Überprüfen Sie, ob Informationen aus Ihrem Netz bereits geleakt wurden bzw. öffentlich verfügbar sind

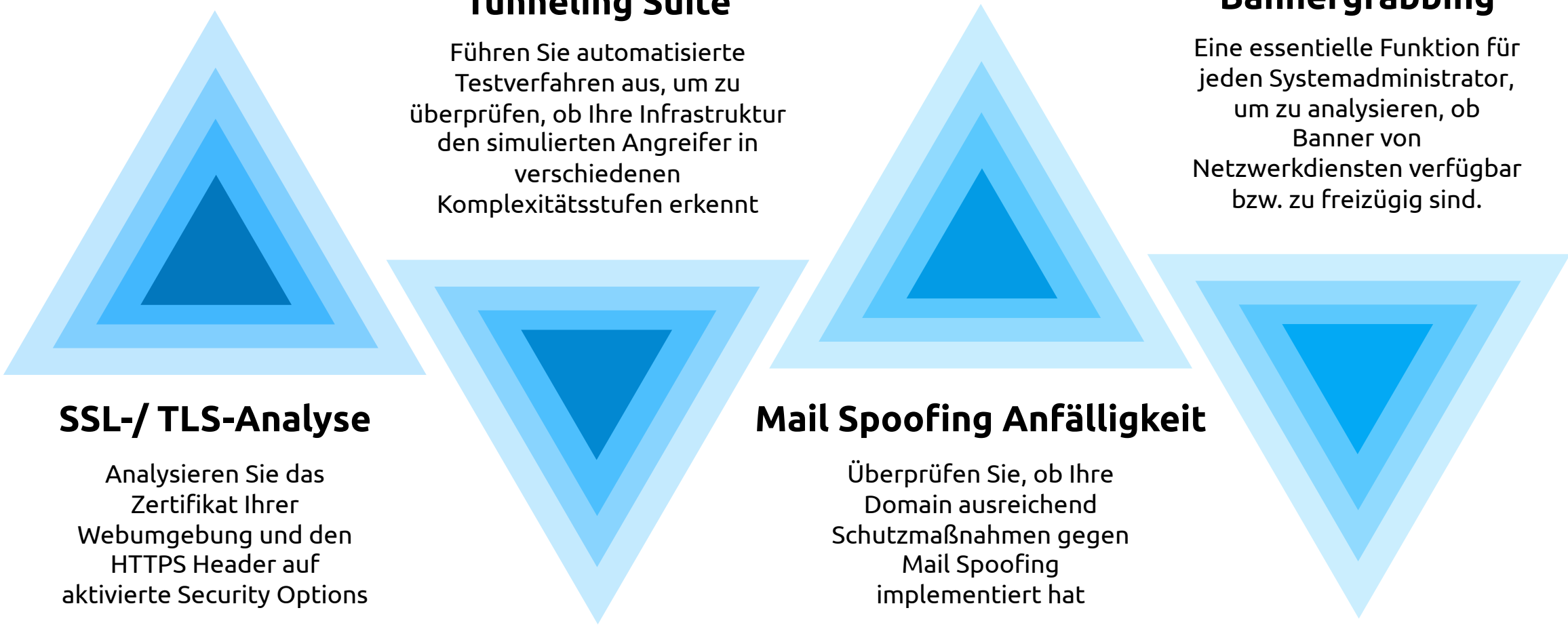
E-Mail Verwendungsanalyse
Testen Sie, wo eine bestimmte oder alle E-Mail Adressen Ihres Unternehmens auf domainfremden Seiten verwendet werden

Subdomain Enumeration
Sehen Sie was ein Angreifer über Ihre Domain sieht

Webauditing
Auditieren Sie Ihr CMS auf unvollständige Konfigurationen oder Freigaben

Und noch viele weitere Information Gathering Funktionen, sowie Google Hacks

Netzanalyse



Tunneling Suite

Führen Sie automatisierte Testverfahren aus, um zu überprüfen, ob Ihre Infrastruktur den simulierten Angreifer in verschiedenen Komplexitätsstufen erkennt

Bannergrabbing

Eine essentielle Funktion für jeden Systemadministrator, um zu analysieren, ob Banner von Netzwerkdiensten verfügbar bzw. zu freizügig sind.

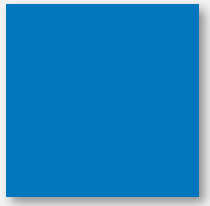
SSL-/ TLS-Analyse

Analysieren Sie das Zertifikat Ihrer Webumgebung und den HTTPS Header auf aktivierte Security Options

Mail Spoofing Anfälligkeit

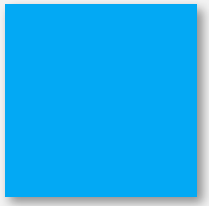
Überprüfen Sie, ob Ihre Domain ausreichend Schutzmaßnahmen gegen Mail Spoofing implementiert hat

Auszug aus den bisherigen Ergebnissen



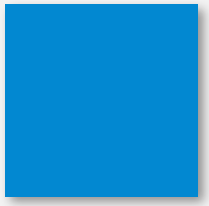
Falsche Freigaben

Firma A hatte eine falsche Freigabe auf Konstruktionspläne im Unternehmensnetz, welche von außen zugreifbar war



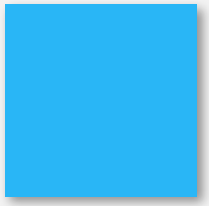
Beobachtung: USB Dropping

90% der USB Sticks mit Label wie “Nacktbilder” werden in Firmencomputer eingesteckt

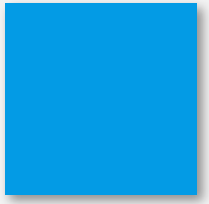


File Extraction Ergebnisse

Gehaltslisten, Passwortlisten, Arbeitsverträge, Mitarbeiterbewertungen, ...

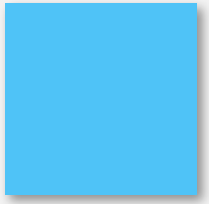


Bei den ersten Einsätzen von Vulidity werden auf ca. **85%** der Anhänge von fremden Adressen mit Rechtschreibfehler geklickt... Der regelmäßige Einsatz von Vulidity senkt diese Zahl drastisch!



E-Mail Adressen

Mitarbeiter A hat seine Unternehmensadresse auf verschiedenen pornographischen Webseiten benutzt



“Erwischt werden”

Durch den psychologischen Aspekt, direkt betroffen zu sein, ist ein nachhaltiges und effektives Bewusstsein geschaffen

Continious Delivery Policy

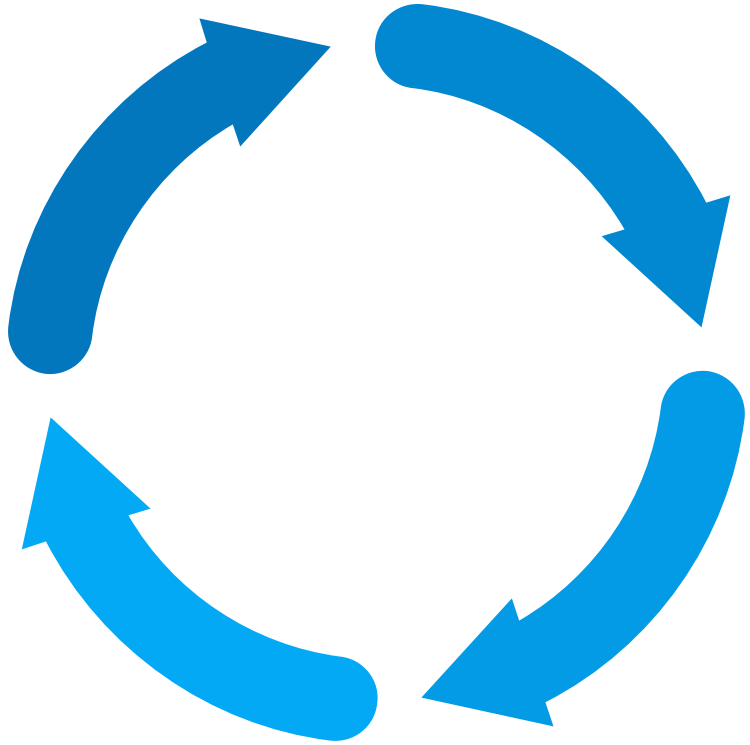
In der kompletten Lizenzlaufzeit bekommen Sie kostenlos:

Neue Features

Alle neuen Features sind in Ihrer Lizenz inklusive

Verbesserungen

Grafische Verbesserungen, neue Designs, Fehlerbehebungen und Anpassungen



Ihr Feedback

Ihr Feedback ist uns wichtig und fließt in unseren Entwicklungsprozess mit ein (Anpassungen, neue Features, …)

Updates

Vulidity und das darunterliegende System wird ständig aktualisiert

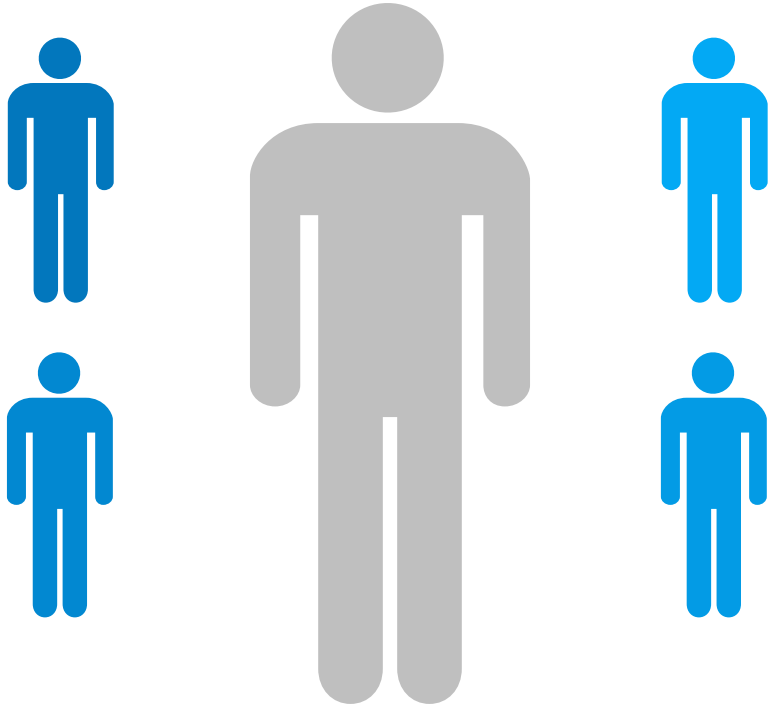
Konkurrenz

Firewall und Netzwerkinfrastruktur

Sind nur das Fundament einer Sicherheitsinfrastruktur und haben außerdem keine Social Engineering und Open Source Intelligence Funktionalitäten.

OpenSource Werkzeuge

Es gibt unzählige Tools mit überschneidenen Funktionalitäten und oft keinen Support für Enterprise-Umgebungen.



Schulungen und Belehrungen

Schulungseffekt oft nicht gegeben, weil Teilnehmer am Smartphone sind, E-Mails schreiben oder mit den Gedanken ganz weit weg sind.

Penetrationstester / Auditoren

Kosten/Nutzen für den KMU nicht tragbar, da oft ein einziger Audit das Budget aufbraucht. Gleichzeitig sind nach Veränderungen der Infrastruktur neue Audits notwendig.

Ein Dokument kann keine Vorführung ersetzen.

Schreiben oder rufen Sie uns an, um einen Termin für eine Live-Demo zu vereinbaren!

Vulidity GmbH

08633 505694

info@vulidity.de