Synack

SOLUTION BRIEF

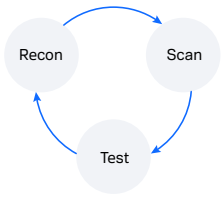
Reducing Risk of Third-Party Partners and M&A Targets

For organizations with extensive digital portfolios or supply chains, securing the organization's digital assets and attack surface begins with due diligence. Whether it's a partner currently interfacing with your attack surface or an M&A target who could be soon, there's potential risk, and it's reflected in the numbers.

There's often a mismatch between your acceptable risk levels and that of a partner and target acquisition. When a third party has an undiscovered vulnerability in their ecosystem, that vulnerability can later become a threat to the larger ecosystem.

Bottom line: A third party can be a ransomware onramp to your environment.

Their attack surface is your attack surface. Protect your third-party digital ecosystem with a data-driven approach.



Step 1: Reconnaissance

Step 2: Scanning

Step 3: Testing

Third-Party Risk by the Numbers

- **82%** of CIOs believe their software supply chains are vulnerable[1]
- Supply chain attacks impacted **62%** of organizations[2]
- High-risk vulnerabilities are present on the network perimeters of **84%** of companies[3]
- **75%** of attacks in 2020 used vulnerabilities that were at least two years old[4]
- **75%** are concerned about the ransomware risks posed by third parties, but only **36%** of organizations evaluate their third parties' security and privacy practices[5]

Reconnaissance

Synack Digital Reconnaissance assesses brand and organizational risk by combining automated and human analysis that provide visibility into potential threat vectors, and describing how the information can be used by attackers. The process enables you to:

- Discover unknown risks to your organization
- Enumerate potential weaknesses and identify current strengths
- Share information about your digital risk
- Expand your attack surface coverage by investigating untested assets
- Augment internal teams with unique skills brought by the Synack Red Team (SRT)

1. Source: Venafi, 2022
2. Source: Anchore, 2022
3. Source: Positive Technologies
4. Source: Check Point, 2021
5. Source: Ponemon, 2020

The intelligence gathering leverages OSINT methods, focusing on key attack surface areas: network, website, cloud, and human information.

Network

- Open ports
- SSL misconfiguration
- Milicious IPs
- Unmaintained hosts

Web/Cloud

- API keys
- Open storage buckets
- Cloud misconfiguration
- Darknet mentions
- Similar domains

Human

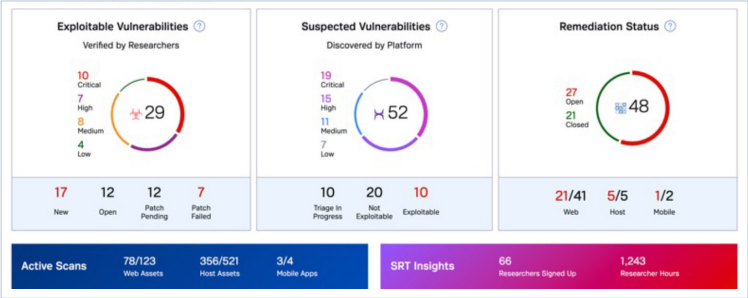
- Compromised email addresses
- Hashed or plaintext passwords
- Job posting information

The results can convey valuable information to internal stakeholders and help target both automated vulnerability scanning and future human-led security testing priorities.

Automated Vulnerability Scanning

While there is no substitute for the human creativity of penetration testing, scanners are an indispensable tool for locating and identifying known vulnerability types. Synack's SmartScan scales security testing by identifying known vulnerabilities and accelerating human-led testing and remediation.

SmartScan® uses a combination of scanning tools to continuously scan web and host assets for changes in your environment. Once a Suspected Vulnerability is confirmed as exploitable, human testers (the SRT) generate a detailed vulnerability report, with steps to reproduce and fix the vulnerability.



62% of Common Weakness Enumerations (CWEs) found through a manual penetration test cannot be found through automation[1]

Penetration Testing

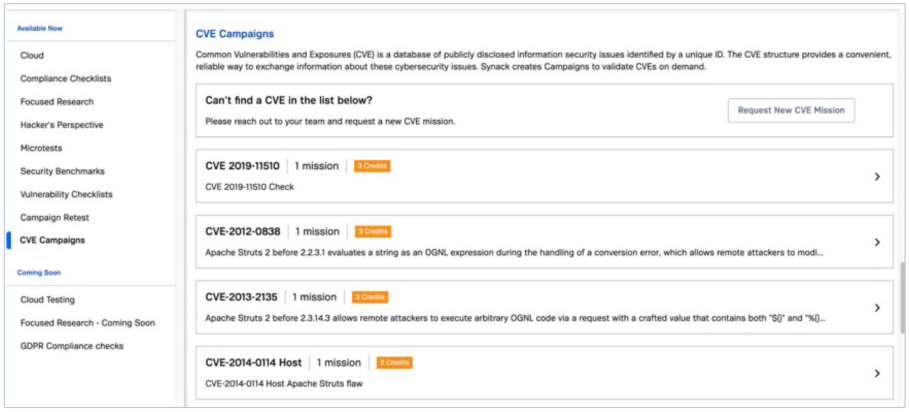
The rate of modern software development and infrastructure change strains everyone's security testing and operations capacity. Your organization, partners and acquisition targets have gone remote and digital, increasing the risk of introducing new vulnerabilities and creating a continuous stream of new risks.

TESTING CATEGORY	PASS	FAIL	N/A	SUCCESS RATE
Authentication	7	2	1	78%
Authorization	3	1	0	75%
Business Logic	2	6	1	25%
Client Side	10	2	0	83%
Configuration and Deploy Management	5	1	0	83%
Cryptography	2	1	0	67%
Data Validation	14	1	0	93%
Error Handling	2	0	0	100%
Identity Management	2	2	0	50%
Information Gathering	8	0	0	100%
Session Management	5	2	1	71%
information Gathering	1	0	0	100%

1. Source: Veracode, 2022

Synack's continuous pentesting solutions combine an advanced testing platform, integrated vulnerability operations, and the SRT's adversarial analysis to deliver a better pentesting experience. An experience that:

- Starts in days, not months
- Can be run on-demand for web, host, API and mobile
- Offers technical analysis that typically involves 50+ experts from a diverse community of 1,500+ vetted security researchers, not just one or two pentesters
- Blends automatic and adversarial human analysis with the platform's vulnerability management to maximize efficacy
- Produces real-time insight and control of current testing scope and activities with a standard set of reports that make the results actionable
- Can also leverage the Synack Platform and SRT for testing unexpected vulnerabilities like Log4j



By following the recon-scan-test data-driven methodology, organizations will gain actionable visibility into a partner's risk posture. For more information on Synack's digital reconnaissance, automated vulnerability scanning, and penetration testing capabilities, see www.synack.com.

© 2022 Synack Inc. All rights reserved.