Secureworks®

Custom Adversarial Engagements

Secureworks® Adversary Group brings deep, technical skillsets and experience to test anything.

Overview and Benefits

The Secureworks® Adversary Group is a dedicated team of elite testers. We offer a suite of standard adversarial security testing services and custom testing of unique devices, systems, and threat models.

Custom adversarial testing engagements leverage the deep bench strength and specialized expertise of our team, providing vulnerability data to remediate security weaknesses and support ongoing business and operations.

Tests include:

IoT / SCADA / OT / Embedded systems testing
Hardware device reverse-engineering and adversarial testing
Vehicle systems testing (Automotive, CANBUS, autonomous, vessels, aircrafts)
SAP-specific adversarial testing
Medical device teardown, reverse-engineering, and adversarial testing
High-speed password cracking and analysis
Custom wireless applications (non-standard, non-802.11)
Blockchain-integrated applications
Supply chain attacks
Insider threat emulation

A Note From Us

Our team loves helping our customers with their unique challenges. No matter what devices, systems, software, or threat models you are working with, our team is staffed with Subject Matter Experts specific to your needs. Contact your security specialist if you have something non-standard that you would like to discuss with the team.

Secureworks®

Below are example goals and outcomes from engagements performed by the Adversary Group.

Target	Goal	Outcome
Cruise Ship	Test the ship's protections around navigation and control networks.	Testers worked from the guest Wi-Fi and compromised internal, sensitive networks. From there, testers moved laterally and compromised control networks – allowing testers to take control of the ship's navigation.
OBDII Automotive Dongle (CANBUS)	Compromise a vendor-supplied device that plugs into a vehicle's ODBII port.	The device was compromised via hardware-level attacks. Testers were able to spoof messages on the CANBUS network.
Active Directory Password Hash	Attack password hashes stored in Active Directory. Provide statistics on weak or predictable passwords.	Using a large, 24-GPU password cracking cluster, Secureworks recovered more than 90% of plaintext passwords in 24-hours. Statistics found that users are choosing predictable passwords, and several Domain Admin members share passwords with their regular user accounts.
Medical Device	Compromise the device via hardware, wireless, or software attacks. Recover patient data, and infect other medical devices.	Consultants were able to compromise the medical device via local access. Once on the operating system, AWS configuration keys were found, which allowed the consultants to compromise upstream package repositories, resulting in the compromise of ALL medical devices from this vendor.
Production SAP	Determine if a skilled attacker could compromise production SAP infrastructure.	Consultants found that a highly privileged account in the development system did not have a changed password. With this level of access in the development environment, Secureworks consultants accessed sensitive transactions and exfiltrated client usernames and password hashes. Numerous plaintext passwords were recovered, including those for accounts having the SAP_ALL profile. Further testing revealed that some of the recovered accounts were also reusing passwords within the production SAP system, ultimately leading to complete takeover of the entire landscape.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com

About Secureworks
Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.