

Red Team Engagement Prepared for: Sample Company

COMPLETE REPORT
January 1st, 2026

Red Sentry

This engagement was performed in accordance with the Statement of Work, and the procedures were limited to those described in that agreement. The findings and recommendations resulting from the assessment are provided in the attached report.

Given the time-boxed scope of this assessment and its focus on client-provided Objectives only, the findings in this report should not be taken as a comprehensive listing of all security issues.

Contact Information

+1 (888) 337-0467

hello@redsentry.com



TABLE OF CONTENTS

TABLE OF CONTENTS	2
SUMMARY	4
Project Overview	4
Goals	4
Dates	4
Result	4
Objectives	4
Blacklist Scope	5
Rules of Engagement & Assumptions	6
Detection Expectations	6
Allowed Persistence Methods	6
Expected Blue Team Awareness Level	6
Deconfliction Process	6
Executive Summary	7
Critical Attack Chain Demonstration	7
Risk Overview	8
Hybrid Attack Paths	8
Critical Attack Chain Walkthrough	12
Critical – Hybrid Physical and Network Compromise Leading to Administrative Control and Sensitive Data Exfiltration	12
Attack Path Overview	12
Storyboard	15
Reconnaissance	15
Engagement	17
Appendix (A) Objective Impact Description	21
Business Impact Descriptions	21

SUMMARY

Project Overview

{Sample Company} engaged Red Sentry to assess the effectiveness of their defensive security (Blue) team via an objective-based Red Team Engagement.

The following report details these objectives, the steps taken to accomplish them, and the observed proactive and reactive steps Blue Team members took to inhibit attackers' progress.

Goals

Evaluate the speed and effectiveness of security infrastructure against a widespread professional attack synchronized across multiple vectors.

Dates

January 1st, 2026

KickOff

January 1st – 5th, 2026

Testing Period

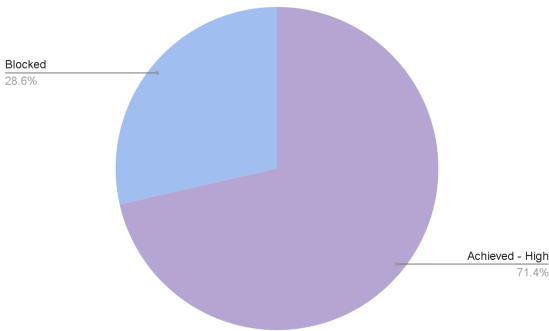
January 5th, 2026

Report Delivery

Result



GRADE



Objectives

Accomplish the following as determined in concert with the on-site contact:

- Establish persistence from a black-box perspective



- Insert the phrase “Sample Company is undergoing a security review” somewhere plainly visible on the main webpage
- Enact an illegitimate transaction.
- Exfiltrate client or end-user payment information
- Locate and exfiltrate the “Flag”: a file or physical object stored in a heavily secured area
- Acquire Administrator-level access

Blacklist Scope

The Assessment team was instructed not to interact with the following:

- external_api.samplecompany.com
- Top Secret Security Clearance room 5 at 1000 Building Lane, city, STATE, USA
- Radioactive Site B at 1000 building lane, city, STATE, USA

Rules of Engagement & Assumptions

Detection Expectations

The team has been instructed not to identify themselves as contracted Red Team members if detected. They are instructed to attempt to deconflict without breaking character or revealing the nature of their business unless doing so would risk injury, widespread panic, or any other general loss of situational control or safety risk.

The team will alert local law enforcement that testing is underway at the target facilities and provide contact information for client security for safety and smooth deconfliction purposes in the case authorities are contacted.

Allowed Persistence Methods

No restrictions have been placed on persistence methods allowed during this engagement, so long as the method is not destructive in nature and can be easily reversed.

Expected Blue Team Awareness Level

The team will proceed under the assumption that no blue team members, save the primary contact at Company, are aware of the testing underway. All strategies, goals, and result weighting are based on this assumption.

Deconfliction Process

In preparation for a scenario where de-escalation is required, the team will be provided with a card identifying them as contracted by the primary contact at Company.

Executive Summary

Red Sentry conducted a hybrid red team engagement combining physical intrusion, social engineering, and internal network compromise techniques to simulate a real-world adversary targeting enterprise infrastructure.

The assessment began from a black-box perspective, assuming no prior credentials or trusted access.

During the engagement, the Red Team successfully demonstrated a complete attack chain resulting in full administrative control of the internal network, compromise of security monitoring systems, and physical and digital exfiltration of restricted assets.

Critical Attack Chain Demonstration

During this engagement, the Red Team demonstrated a complete adversary lifecycle beginning with unauthenticated physical access and culminating in full administrative control and sensitive data exfiltration.

Attack Path Summary:

1. Physical infiltration and rogue device deployment
2. Passive interception of unencrypted credentials
3. Internal SSH access
4. Administrative password enumeration
5. Domain-level control achieved
6. Security camera access and physical target identification
7. Physical and digital exfiltration of restricted assets

This chained progression illustrates how individually moderate weaknesses combined to create a full enterprise compromise.

These successes were not isolated achievements, but sequential phases of a single adversary lifecycle.

The Red Team first established persistence from a black-box perspective by physically infiltrating Location B and installing a rogue device on an exposed internal network port. From that foothold, the team captured unencrypted credentials belonging to a sales associate with access to sensitive customer payment information. Leveraging weaknesses in password policy enforcement and the absence of MFA on administrative SSH access, the team escalated privileges to full administrative control of the internal environment.

Each phase directly enabled the next. What began as unauthorized physical presence ultimately resulted in domain-level access, surveillance system compromise, and both digital and physical asset exfiltration.



While the Red Team was unsuccessful in initiating unauthorized financial transactions due to strong MFA enforcement within the accounting environment, this control represented an isolated defensive strength within an otherwise vulnerable attack surface.

The Blue Team did not detect the Red Team at any point. There were times during the engagement when members of the Blue Team interacted directly with the Red Team. When gaining physical access to the facility, the Red Team members should have been stopped and questioned immediately by the Blue Team. They should have been asked their purpose, for identification, and when unable to provide known, expected information, they should have been both denied entry flatly and reported to security personnel.

Risk Overview

Three of the achieved objectives were classified as Critical due to their potential impact on confidentiality, integrity, and availability of enterprise systems.

The demonstrated chain shows that:

- A motivated adversary could gain persistent internal access without phishing or malware deployment.
- Administrative accounts lacked sufficient protections such as multi-factor authentication.
- Surveillance systems were accessible post-compromise.
- Sensitive data and restricted physical assets could be exfiltrated without detection.
- In a real-world scenario, this level of access would enable ransomware deployment, large-scale data exfiltration, operational disruption, and significant regulatory exposure.

Hybrid Attack Paths

For this project, the team implemented several hybrid approaches to accomplish the chosen objectives, ignoring all else. The Team has provided a high-level summary of these approaches below.

	Objective	Technical Component	Non-Technical Component	Summation of Efforts
1	Establish Persistence	Mobile Rogue Device installation	Unauthorized physical access Lock tampering Social Engineering	The team was able to compromise a secured window during daylight hours and use it for re-entry at night to install a mini-PC in an unsecured network port.
2	Deface Main Webpage	Html injection Authentication bypass	Social Engineering	The Blue Team's policies and coding practices successfully prevented the Red Team from enacting meaningful changes on the main webpage.

3	Exfiltrate Customer Payment Information	- Rogue Device Installation (1) - Unencrypted communication capture - Directory Enumeration	- Social Engineering - Physical entry	Using the Rogue Device installed in Section 1, the Red Team was able to capture plaintext login credentials for a member of the sales team by listening to unencrypted communications broadcast over the network. Utilizing these credentials, the team gained access to customer payment information by accessing the messaging history where it had been shared.
4	Initiate Unauthorized Transfer	- Rogue Device Installation (1) - Login Bypass - MFA bypass	- Social Engineering - Physical entry	The Blue Team's coding practices, policies concerning MFA usage, and the diligence of the accounting team in resisting Social Engineering and securing their devices against unauthorized access prevented the Red Team from completing any transfers.

5	Acquire Administrator-level network access	- Rogue Device Installation (1) - internal SSH - Brute Forcing utilizing Python	- Physical Access - Shoulder Surfing	The Red Team gained daylight entry to the building and witnessed IT personnel using SSH to run administrator commands. Since the administrator was accessible remotely, they utilized the physical device installed in (1) and a Python script to run a modified password list and attempt to log into a machine as Administrator. After some time, the password list succeeded, and the team had access to the administrator password, which was not MFA-protected when utilized to log in to any machine.
---	--	---	---	--

6	Locate and exfiltrate the “Flag”	- Rogue Device installation (1) - Network Enumeration - IOT (Camera) access	- Physical Entry - Lock Manipulation	The team gained access to security camera footage after gaining administrator-level network access. They used this footage to locate the physical location of the “Flag” file. The team successfully exfiltrated the physical file by manipulating the exterior lock to this restricted area. They exfiltrated the digital file after discovering it via directory enumeration using administrator credentials.
---	----------------------------------	---	---	--

Table 1: Hybrid approaches

Critical Attack Chain Walkthrough

Critical – Hybrid Physical and Network Compromise Leading to Administrative Control and Sensitive Data Exfiltration

Executive Overview

During this engagement, the Red Team demonstrated a complete adversary lifecycle beginning from a black-box perspective and culminating in full administrative control of the internal network, access to sensitive customer data, surveillance system compromise, and physical exfiltration of a restricted asset (“the Flag”).

Individually, several weaknesses may have appeared moderate in isolation. However, when chained together, they enabled a full enterprise compromise without detection. The Blue Team did not identify or interrupt any phase of the attack.

Attack Path Overview

1. Unauthorized physical access to the facility
2. Rogue device installation on internal network
3. Interception of unencrypted credentials
4. Internal SSH access without MFA
5. Administrative password enumeration
6. Domain-level administrative control
7. Security camera system access
8. Physical and digital exfiltration of restricted assets

This progression demonstrates how layered control failures across physical, network, identity, and monitoring domains can be combined to achieve critical business impact.

Phase 1 – Initial Access (Physical Infiltration and Rogue Device Deployment)

The Red Team obtained physical access to the facility during business hours using light social engineering and a benign pretext. No identity verification or escort controls were enforced.

Once inside, the team identified exposed, unsecured Ethernet ports. A preconfigured miniature computing device with encrypted outbound command-and-control capability and cellular failover was connected to the internal network.

No Network Access Control (NAC), port authentication, or device validation mechanisms prevented this connection.

Impact: Persistent internal network foothold established without valid credentials.



Phase 2 – Credential Acquisition (Unencrypted Communications)

After establishing an internal presence, the team deployed a passive network monitoring tool from the rogue device.

Internal messaging traffic was observed transmitting credentials in plaintext. The Red Team captured valid login credentials belonging to a user with access to sensitive customer data.

No encryption or network segmentation controls prevented credential interception.

Impact: Valid internal credentials obtained without phishing, brute force, or malware deployment.

Phase 3 – Privilege Escalation (Administrative Access Without MFA)

Using the captured credentials, the team performed internal enumeration and identified administrative systems accessible via SSH.

It was observed that administrative SSH access did not enforce multi-factor authentication. The team conducted controlled, time-spaced password enumeration using a customized wordlist derived from organizational naming conventions and OSINT findings.

After several hours of low-noise attempts, the administrator credential was successfully compromised..

Impact: Full administrative control of the internal network environment.

Phase 4 – Internal Reconnaissance and Surveillance System Compromise

With administrative access, the Red Team accessed internal file shares, user desktops, and the organization's security camera storage.

The surveillance system was accessible without additional segmentation or privileged isolation. Recorded footage was reviewed to identify the physical location of the restricted "Flag" asset.

No alerting or logging controls flagged the access to security infrastructure.

Impact: Compromise of security monitoring systems and loss of confidentiality of surveillance data.

Phase 5 – Objective Fulfillment (Physical and Digital Exfiltration)

Armed with knowledge of the restricted area's location, the on-site asset re-entered the facility and accessed the secured space containing the "Flag."

The exterior lock mechanism was manipulated without triggering alarms or a response. The physical asset was removed.

Separately, the digital copy of the "Flag" was located via directory enumeration and exfiltrated using administrative credentials.

Impact: Successful physical and digital exfiltration of restricted assets.

Business Impact

This chained attack demonstrates the following critical risk conditions:

- An external actor can gain persistent internal access without credentials.
- Internal communications were vulnerable to interception.
- Administrative accounts lacked MFA protection.
- Password policies were susceptible to controlled enumeration.
- Security monitoring systems were accessible post-compromise.
- Physical security controls did not prevent restricted-area access.
- No detection mechanisms interrupted any phase of the attack lifecycle.
- No alerting, logging, or behavioral anomaly detection interrupted this chain at any stage.

Had this been a malicious adversary rather than a controlled engagement, the following outcomes would have been possible:

- Deployment of ransomware across the enterprise environment
- Destruction or encryption of business-critical systems
- Large-scale exfiltration of customer payment information
- Manipulation or deletion of surveillance footage
- Prolonged undetected persistence within the network
- Significant regulatory, financial, and reputational impact

Because the attack progressed from unauthenticated external presence to full administrative control and physical compromise without detection, this chain represents a Critical-level enterprise risk scenario.

Storyboard

Reconnaissance

During the Recon phase, the Red Team takes as indirect an approach as possible to gather information about their target. They already have their goals in mind, and the information gathered and utilized here is tailored to meet those goals. After spending a long time gathering information generally about the target(s), the team will begin to organize the information into viable attack paths and gather deeper info where necessary, branching out sometimes several steps away from the organization itself in terms of direct relevancy.

Details

The Red Team began the reconnaissance phase by looking up the history of Sample Company. They researched the owners, the vision, mission statement, and searched for records referring to holdings, acquisitions, transfers of leadership, or any legal action in public records. They also expanded searches to gather as many names of employees as possible, along with their positions in the company. They attempted to discover these individuals on various social media platforms and form a generalized profile on each that could be fleshed out further if needed, including names of close friends, acquaintances, and friends of friends that could be used to help establish credibility during Social Engineering. The basic version of this information can be found in Table 2 below.

Targeted	Name	Position	Phone		Email	Socials
No	John Doe	Manager	[not discovered]		Jdoe@samplecompany.com	[facebook] [instagram] [linkedin]
Yes	Mary Jane	CFO	234-567-8901		mjane@samplecompany.com	[tiktok] [reddit] [linkedin] [facebook]
(etc)	(etc)	(etc)	(etc)		(etc)	(etc)

Table 2: Employee Information Gathering

While gathering information on employees, the Red Team also performed physical reconnaissance via Google Maps to identify potential entry points, identify parking areas with ideal access to restricted areas, and those with poor visibility. This also allowed the team to have a general idea of what kind of security to expect upon arrival. The team followed up on

this investigation upon physically arriving at the site. They noted the positions of security cameras, where employees entered and exited the building, how often, and whether there seemed to be any authentication apparatus. At this point, the team noted that there seemed to be only physical locks on the second-story windows with no alarms in place, as shown in Figure 2 below.



Figure 2: Simple Window Lock

At the same time as the OSINT and physical inspections, the Red Team also began examining the target environment from a digital perspective. This included identifying the technical stack from a black-box perspective. They took note of Sample Company's technology stack, utilizing a series of non-invasive scans run against IPs found to be owned by the company. They followed up by enumerating subdomains and exploring endpoints in both an automated and manual fashion. In many cases, the team could discover or infer the version of the technologies in place and, using that information, make a list of potential vulnerabilities that could be utilized to accomplish the objectives listed in the Objectives section

Engagement

After gathering information, the team took time to put together an attack plan for each objective and act upon each in an organized and synchronized timeline. Below is a description of these efforts at meeting each objective.

Details

Establish Persistence - Successful

After discussing the objectives, the team decided that attempting to establish persistence should be the first step. Reviewing the profile they had built, the most promising avenue to this was installing a rogue device into Sample Company's Network. This device would have a mobile network, Wi-Fi, and Ethernet connectivity.

Utilizing social engineering and a loose disguise (a custom-ordered Sample Company shirt and a clipboard), our on-site asset gained physical access early on in the engagement. The asset was able to locate several open network ports and installed a number of rogue devices throughout the facility. These devices were installed in various places, such as under a desk, as shown below in Figure 3.

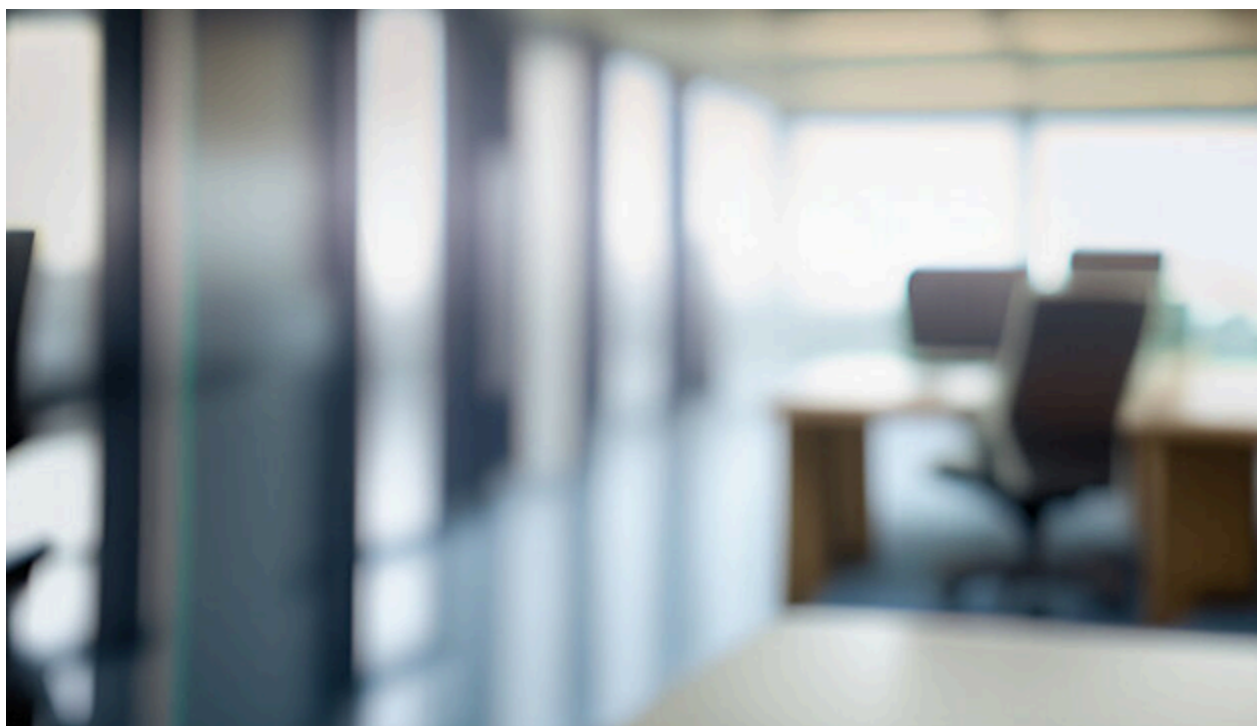


Figure 3: Mini PC Concealed Under Desk

Our on-site asset was not stopped or approached at any time during his invasion of Sample Company's physical space, even when he entered restricted areas.

Deface the Main Webpage - Unsuccessful

In order to deface the website, the team decided to target Sample Company's marketing team and design team. After gathering the OSINT information during Reconnaissance, the team deduced that both Marketing and Design teams were located offshore and likely fully remote. When physically infiltrating the office, this was confirmed. No access to Design personnel could be gained. The team built a social engineering campaign around approaching notable members of the teams and messaging them on various social media platforms, but none of the Web Development team members provided meaningful access or information.

Exfiltrate Customer Payment Information - Successful

The plan to exfiltrate customer payment information involved the crafting and delivery of a payload via a file upload vulnerability and a social engineering effort to lure employees in the sales department to interact with the file. The team found that filetypes uploaded using the technical support portal seemed to have no filters against potentially malicious filetypes, such as .exe files that can easily run code. Posing as a customer, they planned to ask for support with a malicious file, asking the sales staff to open and run it. This plan eventually became unnecessary.

After installing the device and running listening software on the network, the team was able to capture several sets of cleartext credentials sent over SampleCompanyMessage. One of these belonged to the head of sales, who was suspected of having access to sensitive customer information. These credentials were used to log into the company portal from inside the network using a rogue device and an SSH session to access a company device. The team was able to access sensitive customer data and exfiltrate it to a remote location via this method.

Initiate Unauthorized Transfer - Unsuccessful

In order to initiate unauthorized transactions, the team was aware that it would need access to some processes related to accounting. The Reconnaissance phase revealed that accounting services were likely not being outsourced, so the team planned to target accounting department members in a spearphishing campaign to grab their credentials using an iFramed imitation of their company portal. Secondly, as a last and noisy resort, they planned to attack accountingapi.samplecompany.com utilizing a common injection vulnerability to prompt the attached accounting software to initiate a transaction. The team was successful in Social Engineering when one of the accounting employees interacted with the fake accounting portal and captured the username and password of this employee. However, when attempting to access the accounting software, the team was met by MFA and stopped. The team decided not to attempt the injection vulnerability because they could not guarantee that

no damage would be done to Sample Company's infrastructure should the payload not act as intended.

Acquire Administrative Access - Successful

The Team decided to utilize the physical machine installed on-premises during the persistence phase to enumerate the network. OSINT and a careful review of social media activity among company members revealed an internal messaging system called SampleCompanyMessageSystem. The team planned to use a vulnerability in this system to trigger a privilege upgrade. Simultaneously, the team planned to search for unattended desktops or opportunities to shoulder surf or discover password notes once physical access to the facility was acquired.

After physical access was acquired and the rogue device was installed, the team discovered it was possible to SSH into the administrative machine from any internal device after observing a member of the IT team do so without MFA. They utilized some customized scripting to create an attack plan for enumerating the administrator password via a specialized hacking tool that operates over SSH, and utilized a customized wordlist.

After about 4 hours of carefully spaced attempts, the team successfully gained access to Sample Company's administrative environment with the password "SampleCo2015MountainLion". This password may seem strong because of its length, but it was easily guessable and enumerable given the knowledge of the local college football team's mascot, The Mountain Lion. The team achieved administrative network control.

Locate and Exfiltrate "The Flag" - Successful

During Recon, the team discovered several physical attack vectors, including simple door locks, reverse-exit vulnerable locks, and window locks with no visible alarm on the upper levels of the facility. After gaining access to the network via the rogue devices planted throughout the facility, they could freely move across file structures to search for the "Flag" file. The team eventually found files where security footage was being stored. These were access-controlled at first.

After gaining administrative access, the team found they could access security footage. They utilized this footage to discover the physical location of the "Flag."

The team re-entered the facility using a benign pretext and proceeded directly to the second-floor secure area without being challenged. He was not stopped or challenged and moved directly to the second-floor secure area, where he expected to find the "Flag." The on-site asset encountered a staff member while manipulating the lock mechanism. When questioned, the asset provided a benign pretext and was not further challenged or reported. No escalation occurred, and no verification of authorization was requested.



The lock was successfully bypassed, and the restricted room containing the “Flag” was accessed without triggering alarms or initiating a security response.

Separately, the team gained administrative network access and was able to locate the digital folder containing the flag at SampleCompanyMachine1/Admin/Desktop/FlagFolder by remotely accessing the desktop machine of John Doe using the admin credentials.

Appendix (A) Objective Impact Description

The assessment team ascribes success or failure in objective completion to a scale of business impact relevant to the client's known environment. Below is a description of each of these outcomes which can be found.

Business Impact Descriptions

Objective Achieved - High Business Impact

SUCCESS - HIGH

The team successfully completed the assigned objective. The objective itself or the way in which it was accomplished has a clear, demonstrable, serious impact on business and operations in the target environment. This represents a scenario in which a malicious actor could inflict serious damage.

Objective Achieved - Moderate Business Impact

SUCCESS - MODERATE

The team successfully completed the assigned objective. The objective itself or the way in which it was accomplished demonstrates some impact on business and operations in the target environment. This represents a scenario in which a malicious actor could inflict damage that may be mitigated by other controls or have a limited sphere of impact.

Objective Partially Achieved

PARTIAL SUCCESS

The team either completed some portion of the objective or fully completed it, but was detected or had its impact foiled while doing so. There is some business impact, but technical or personnel controls clearly mitigated some or all of the damage that could have demonstrably been inflicted in this scenario.

Objective Blocked by Controls

BLOCKED

The team made clear, concerted attempts to achieve the objective, but was summarily prevented from any meaningful impact by the controls put in place in the target environment. No demonstrable business impact was achieved.

Objective Not Attempted

NOT ATTEMPTED

The team, after researching the target environment and potential attack vectors, deemed that the odds of success with any approach allowed by the Rules of Engagement or Law did not merit an attempt. The team focused its efforts on other objectives with a higher likelihood of meaningful impact.