SECURE NETWORK
TECHNOLOGIES

833-974-0015
SECURENETWORKINC.COM

SECURITY ASSESSMENT & PENETRATION TEST SERVICES

RISK BASED PENETRATION TEST

Our assessment focuses on identifying and prioritizing vulnerabilities by targeting areas with the highest potential impact, enhancing overall security based on specific risks.

PURPLE TEAM EXERCISE

SNT offers a collaborative engagement that combines red team (offensive) and blue team (defensive) activities in a real time to understand the strength of an organization's network.

ASSUMED BREACH

Our highly skilled engineers put your AV/EDR solutions to the test on how a threat actor can bypass various tools and move laterally throughout your network.

WEB APPLICATION SECURITY ASSESSMENT

Our Application Security Assessments identify vulnerabilities before they can be exploited, ensuring your critical business applications remain secure and reliable.

FORENSIC SERVICES

Our Digital Forensic Team focuses on available evidence and data sources to try to ascertain how the security event occurred, potential data exposure or potential threat actor persistence within the network.

PHISHING & SOCIAL ENGINEERING ASSESSMENTS

SNT emulates methods commonly used in phishing and social engineering attacks to leverage a security compromise, and provides a detailed report of the findings.

PHYSICAL SECURITY ASSESSMENTS

SNT Engineers will assess the effectiveness of physical barriers, access controls and test the "human element" to prevent unauthorized access to IT infrastructure.

RED TEAM EXERCISE

Experience a simulated cyberattack where our red team will attempt to remain anonymous and assess organization's security defenses, response capabilities and resilience.

INCIDENT RESPONSE

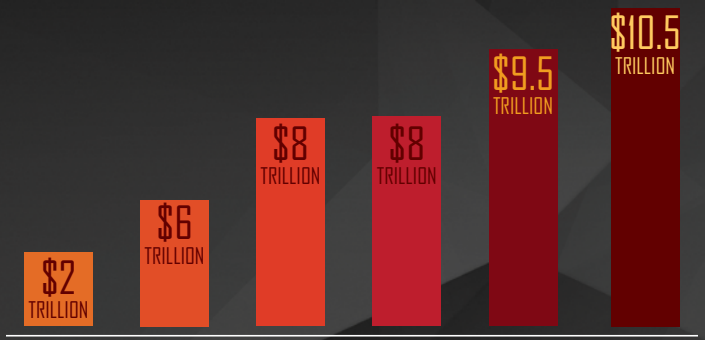
Our expert support helps organizations quickly detect, contain and recover from cybersecurity incidents.

BUG SWEEPING

Our engagement attempts to identify any intelligence-gathering devices which could be exploited for corporate, legal or political espionage and provide remedial recommendations.

NEED IMMEDIATE THREAT RESPONSE?
CALL 833-974-0015

BECAUSE THERE'S NO SHORTAGE OF BAD PEOPLE.



TOTAL ESTIMATED GLOBAL FINANCIAL LOSSES DUE TO CYBERCRIME BETWEEN 2020-2025

HTTPS://WWW.STATISTA.COM/FORECASTS/1280009/COST-CYBERCRIME-WORLDWIDE
HTTPS://WWW.IC3.GOV/ANNUALREPORT/REPORTS/2023_IC3REPORT.PDF

WITH THIS YEAR'S SECURITY STATS, DIGITAL HEISTS HAVE GONE UP ALMOST 500%*. HAS YOUR **SECURITY BUDGET**?

There is **no shortage of malicious actors** scanning the digital business landscape for unlocked doors. The implications of experiencing a network intrusion are huge - sometimes in the millions of dollars - for companies just like yours. Hackers can lock and steal your financial information, hold important data hostage for payouts and stop your company's progress in its tracks.

*500% INCREASE IN CYBER CRIME FROM 2020-2025
(FBI + IC3 + OTHER SOURCES AND OBSERVED TRENDS)

EVERY 11
SECONDS A BUSINESS BECOMES A VICTIM

$233-521 BILLION
2024 TOTAL FINANCIAL LOSS IN THE U.S. ALONE DUE TO DIGITAL FRAUD

3,320,000+
TOTAL COMPLAINTS 2020-2023

TOP 3 VICTIMS
OF RANSOMWARE BY VERTICAL:

- HEALTHCARE / PUBLIC HEALTH
- CRITICAL MANUFACTURING
- GOVERNMENT FACILITIES

2023 FBI + IC3 INTERNET CRIME REPORT + VARIOUS OTHERS
HTTPS://WWW.IC3.GOV/ANNUALREPORT/REPORTS/2023_IC3REPORT.PDF

THERE ARE TWO TYPES OF CORPORATIONS: ONES THAT HAVE BEEN HACKED, AND ONES THAT HAVEN'T BEEN HACKED **YET**.

It is now the norm to be the victim of a cyber attack. Corporations are open targets for attackers because of their constant engagement in commerce and public visibility. Dependence on web communications for everyday data and financial transactions means that others can leverage vulnerabilities in those same technologies for malicious means.

WE ARE
CYBER SECURITY EXPERTS
SKILLED IN THE ART OF YOUR ATTACKERS

SECURE NETWORK TECHNOLOGIES, INC.

CALL TODAY
833-974-0015
SECURENETWORKINC.COM