Homeland Security

National Cybersecurity and Communications Integration Center

NATIONAL CYBERSECURITY ASSESSMENT AND TECHNICAL SERVICES TEAM

The NCCIC serves as the Department of Homeland Security's lead for cybersecurity and communication coordination, applying analytic perspectives, organizing shared cybersecurity and communications situational awareness, and orchestrating synchronized response, mitigation, and recovery efforts in the event of a cyber or communications incident. The NCATS team supports the NCCIC's mission by offering cybersecurity scanning and testing services to provide remediation and mitigation recommendations allowing the stakeholder to improve their cybersecurity posture on findings from the NCATS team.

WHAT WE DO

NCATS security services currently available include:

- Vulnerability Scanning and Testing
- Penetration Testing
- Social Engineering (Phishing)
- Web Application Scanning and Testing
- Operating System Scanning
- Database Scanning
- Wireless Discovery and Identification

NCATS leverages existing "best in breed" cybersecurity assessment methodologies, commercial best practices and threat intelligence integration that enables cybersecurity stakeholders to better develop decision making and risk management guidance. NCATS has branded this service opportunity as our **"Absolute State of the Hack"** mindset and methodology.

NCATS also provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks. Additionally, NCATS will promote enhanced situational awareness while assisting in improving the overall security posture of the stakeholder's critical cyber assets.

NCATS security services are available at no-cost to stakeholders and can range from one day to two weeks depending on the security services required.

WHO WE ARE

The NCCIC NCATS team consists of subject matter experts in penetration testing methodology and tactical delivery. Team members have extensive experience in current and emerging web applications, networks, databases, wireless, mobile computing, cloud security, social engineering, social media and intelligence gathering.

WHAT TO EXPECT

Prior to beginning any engagement, legal paperwork must be completed and signed. A dedicated Technical Team Lead will be assigned to assist in all pre-assessment, assessment and post assessment matters. A final report detailing findings and mitigations will be delivered upon completion of the engagement.

CONTACT

For additional information on NCATS security services, scheduling, timeline and expectations, please contact us at the email address listed below:

NCATS_Info@hq.dhs.gov

Homeland Security

National Cybersecurity and Communications Integration Center

Risk and Vulnerability Assessment Process

Complete Rules of Engagement

DHS Processes

Scoping Meeting

Select Testing Dates

DHS notifies appropriate parties

Testing

Deliver Report

Agency Action

DHS Action

QUESTIONS:
NCATS_INFO@HQ.DHS.GOV

Cyber Hygiene Process

Complete Letter of Authority

DHS Processes

Provide IP list to DHS

DHS schedules Scan

DHS notifies appropriate parties

Scans Start

Deliver Report