Cyber Security Health Checks
Vendor Service Offerings
September 2021

This document describes the services and deliverables provided by the participating Cyber Security Health Check vendors. Please review this document to make sure you fully understand the scope of services and deliverables that will be provided to you when selecting an assessment

HubTech

In Scope:
HUB Tech is offering a portfolio of cursory IT security-centric engagements at no cost to the municipalities and school districts. Communities that elect to participate could select one of the fiveoptions included in the portfolio. Each offering, described below, is designed to quickly provide customers with valuable insights related to current security posture.

A. **IT Security Posture Profiling:** Discuss municipality or school district's current IT security program to obtain insights on how they measure up against Center for Internet Security BestPractices and Controls and gain practical advice for next best steps.

B. **Cyber Security Sounding Board:** Discuss strategies to rationalize and prioritize investments offinancial and human capital to improve cyber security.

C. **Backup & Recovery Strategy Assessment:** Discuss the state of the current backup and recoverystrategy to ensure their perceived safeguards will perform as intended when needed.

Deliverables:

1. **IT Security Posture Profiling:**
   a. 60-90 minute discussion to gain an understanding of the business environment, policies, technical controls, etc.
   b. document summarizing identified security gaps relative to CIS best practices.
   c. topical action plan to consider in improving IT security posture.
   d. findings review call.

2. **Cyber Security Sounding Board:**
   a. discussion of a community identified cyber-security-related challenge for up to two hours.

3. **Backup & Recovery Strategy Assessment:**
   a. discussion of customer environment and backup/restore considerations for up to one hour.
   b. written report including the size of backups, retention strategy, cloud hosting requirements and time objectives.
   c. findings review call.

INNO4

In Scope:

INNO4 is offering a portfolio of cursory IT security-centric engagements at no cost to the municipalities and school districts. Communities that elect to participate could select one of the five options included in the portfolio. Each offering, described below, is designed to quickly provide customers with valuable insights related to current security posture.

A. **IT Security Posture Profiling:** Discuss municipality or school district's current IT security program to obtain insights on how they measure up against Center for Internet Security Best Practices and Controls and gain practical advice for next best steps.

B. **Cyber Security Sounding Board:** Discuss strategies to rationalize and prioritize investments of financial and human capital to improve cyber security.

C. **G Suite Security Assessment of Administrator Accounts**: Identify G Suite security features and application settings for administrator accounts that deviate from security best practices, as defined by Google, INNO4, or both.

D. **External Vulnerability Scan**: Perform an external network scan for up to 100 hosts to help the municipality or school district understand what vulnerabilities and exploits on endpoints and network devices could be leveraged for malware, ransomware, remote control, etc.

Deliverables:

A. **IT Security Posture Profiling:**
   a. 60-90 minute discussion to gain an understanding of the business environment, policies, technical controls, etc.
   b. document summarizing identified security gaps relative to CIS best practices.
   c. topical action plan to consider in improving IT security posture.
   d. findings review call.

B. **Cyber Security Sounding Board:**
   a. discussion of a community identified cyber-security-related challenge for up to two hours.

C. **G Suite Security Assessment of Administrator Accounts**
   a. INNO4 will require administrator access to the organization's G Suite tenant, or access via a screen share.
   b. Report with actionable remediation recommendations with risk analysis for each recommendation

D. **External Vulnerability Scan**

a. Discovery discussion to gain an understanding of the business environment, policies, technical controls, etc.

b. Conduct external scan to identify vulnerabilities.

c. Document summarizing recommendations.

d. Report walkthrough with key personnel.

IntraSystems

In Scope:

INTRASYSTEMS, INC. is offering a portfolio of cursory IT security-centric engagements at no cost to the municipalities and school districts. Communities that elect to participate could select one of the five options included in the portfolio. Each offering, described below, is designed to quickly provide customers with valuableinsights related to current security posture.

A. **Endpoint Security Assessment** – Today's sophisticated attackers are going "beyond malware" to breach organizations, increasingly relying on exploits, zero days, and hard-to-detect methods such as credential theft and tools that are already part of the victim's environment or operating system. Endpoint security products respond to those challenges with a solution that unifies next-generation antivirus (NGAV), endpoint detection and response (EDR), managed threat hunting capabilities and security hygiene that is cloud-managed and delivered.

B. **Public Cloud Readiness Assessment -** IntraSystems provides a Cloud business review of your infrastructure. IntraSystems will discuss the readiness of your infrastructure to move to the cloud; identify gaps in current infrastructure to deliver on your cloudvision; and make you aware of changes that will happen from a business perspective.

C. **Email Ransom and Phishing Attack Scan -** Spear phishing is rapidly becoming the most significant security threat today. Countless individuals and organizations have unwittingly wired money, sent tax information, and emailed credentials to criminalswho were impersonating their boss, colleague, or a trusted customer. These attacks are compelling and cannot be stopped with existing email security solutions—creating devastating results for individuals, businesses, and brands.

D. **IT Security Posture -** Proven security guidelines will enable you to safeguard operating systems, software, and networks thatare most vulnerable to cyber attacks.

E. **Backup & Disaster Recovery -** Ensure customer's Backup and Disaster Recovery strategy is functioning properly and meetingthe needs of the customer.

F. **AD Hardening Review/Assessment –** Assessment is designed to discover and analyze privilege account exposure and providetransition assistance for deviations from Microsoft's privileged administration recommendations.

G. **Wireless Security Assessment –** Wireless networks are particularly vulnerable to attacks because it is extremely difficult to prevent physical access to them. The deployment of a wireless network within your organization can introduce additional risks thatneed to be properly managed. IntraSystems assessment ensures that the customer's wireless environment complies with the latest security controls.

H. **External Vulnerability Scan –** Provide an external scan of customer's network to look for vulnerabilities or weaknesses that could lead to someone gaining access to customer's environment and data. Scanning and fixing the vulnerabilities protect againstpotential breaches.

Deliverables:

1. **Endpoint Security Assessment –**
    a. Review customer’s existing endpoint security strategy
    b. Deploy a limited number of sensors on customer identified endpoints
    c. Document vulnerabilities and threats found in the customer’s environment
    d. Meet with key personnel to review findings and provide recommendations

2. **Public Cloud Readiness Assessment -**
    a. Business discussion with IntraSystems Cloud professional and key customer personnel
    b. Data collection of existing IT environment and preferred cloud initiatives
    c. Review of security requirements for public cloud migrations
    d. Recommended action plan based on business discussion and initiatives
    e. Call review with key personnel, propose strategic public cloud plan

3. **Email Ransom and Phishing Attack Scan -**
    a. Review the difference between phishing and spear phishing and why it matters
    b. Review the techniques used in impersonation and spoofing attacks and how to recognize each
    c. Discuss the economics of ransomware and spear phishing and what that means for you
    d. Provide initial review of GAP analysis for email security threats
    e. Provide a recommended action plan for remediation
    f. Document all findings, provide review call/meeting with key personnel

4. **IT Security Posture -**
    a. Meet with key personnel to review current IT Security posture, policies and controls in place
    b. Document findings
    c. Identify security gaps relative to SANS20 best practices
    d. Provide strategic plan to improve IT security environment
    e. Provide review call/meeting with key personnel

5. **Backup & Disaster Recovery -**
    a. Review current Backup/Disaster Recovery strategy for both on-premise and cloud-based
    b. Document current Backup/Disaster Recovery plan and determine limitations of environment
    c. Discuss enhancements in current Backup/Disaster Recovery market solutions
    d. Meet with key personnel to review findings and provide recommendations

6. **AD Hardening Review/Assessment –**
    a. Discuss current security threats initiated by non-secure Active Directory configuration
    b. Review current Active Directory policies
    c. Discuss deficiencies present in current configuration
    d. Document findings and provide recommendations to harden and secure

7. **Wireless Security Assessment –**
    a. Discuss customer’s existing wireless environment and wireless requirements

b. Gather information on existing wireless equipment
c. Review customer’s existing wireless AP coverage map
d. Review authentication process for proper wireless access controls
e. Test security of Guest network, if applicable
f. Meet with key personnel to review findings and provide recommendations

8. **External Vulnerability Scan –**
    a. Review customer’s network and firewall policies to gain an understanding of their environment
    b. Conduct external scan to identify vulnerabilities and possible threats
    c. Document vulnerabilities and threats found in the customer’s network
    d. Meet with key personnel to review findings and provide recommendations

RetroFit

In Scope:

RETROFIT TECHNOLOGIES, INC. is offering a complimentary and comprehensive suite of IT security-centric engagements at no cost to the municipalities and school districts. RetroFit's Complete

Ransomware/Cyberdefense and IT Security package is designed specifically to help municipalities understand their current level of protection and arm them with the information they need to protect their data, infrastructure and employees. IT Security is not looking at one element or another - true Security can only be achieved by taking a wholistic approach, to that end all cities, towns and municipalities will receive all of the following services included (at no cost):

1. **External Vulnerability Scan** An external vulnerability scan looks for vulnerabilities at your network perimeter or website from the outside looking in. It specifically examines an organization's security profile from the perspective of someone who does not have access to systems and networkssecurity perimeter – "Hacker View".

2. **Internal Active Directory Scan:** You will receive a report that provides an Executive Summary of your Windows Active Directory environment, along with a Risk Score outline all potential security risks and analysis of each Microsoft issue that we uncover. We will review this document with you and discuss thefindings.

3. **Data Recovery and Protection:** Assessment of current method of data protection and recovery, backup and disaster recovery policy & business continuity safeguards.

4. **Cyberdefense Consultation:** Discuss Intrusion Detection with our Security Services team to strategize on how to minimize the current risk and educate your team on what firewalls, spam filters, and anti- virus can miss.

The number of engagements is not limited and will depend on RetroFit staffing availability. RetroFitagrees to a minimum of 25 municipality and/or school district engagements by December 31, 2022.

Deliverables:

1. External Vulnerability Scan

- External scan to identify vulnerabilities within external environment including:
- Find security vulnerabilities in services on an Internet facing system.
- Detect known web application vulnerabilities on Web Servers.
- Understand security issues through detailed reporting so that risk assessment and re-mediationcan be undertaken.
- Scan options include Full Scan, web server scan, WordPress and Joomla scan types. For up to 5 IP address.
- Scan for firewall changes.
- Document summarizing findings & recommendations.
- 60–90-minute review call to discuss findings and recommendations.

2. Internal Windows Active Directory Scan

- Internal Windows Active scan to identify vulnerabilities within internal environment including:
- Hardware – Active Directory Server
- Software – Missing patches, service packs, security updates, password policy, anti-virus, anti-spyware & firewall configurations

- Configuration -Security policy across network, servers, computers, outbound system access &content filtering
- Accessibility – configuration of end user access to network share and AD security group membership
    - Document summarizing findings & recommendations.
    - 60–90-minute review call to discuss findings and recommendations.

3. Backup & Recovery Strategy Assessment

- Discussion to understanding of current back up environment, processes & recovery point objectiveand recovery time objective requirements written report including current state & a summary of gaps from objectives and recommendations findings review call.

4. Cyberdefense Consultation:

- Meet with our security analyst to review the programs overall findings, summarize areas of vulnerability and potential recommended steps to mitigate security risks.