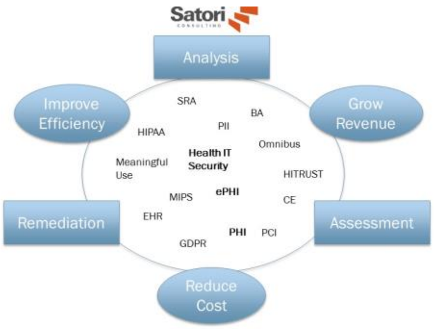
Satori Health IT Security Checkup



Objective

Provide insights into cybersecurity risks including prioritization of the remediation activities to allow deliberate action. Conducted by third party to reinforce internal transparency and organization commitment to a comprehensive risk management plan. Aligns with HIPAA SRA requirement.

About 14.7 million consumers had their private medical data breached, hacked or stolen in 2017, a year in which there were 477 healthcare data breaches, says the U.S. Department of Health and Human Services Office of Civil Rights.

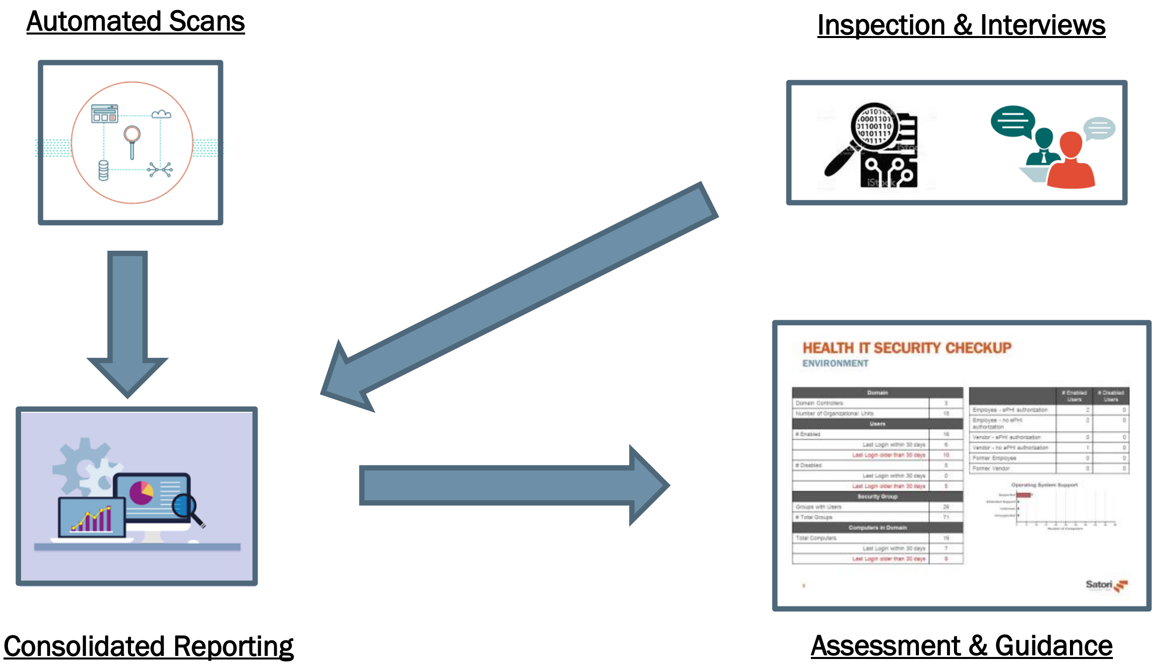
Satori Health IT Security Checkup – addressing Key Considerations

Health IT Security requires focus on risk management rather than simply compliance. Addressing the key considerations below will establish clarity and enable effective risk identification.

- Automated Scans – scans and identifies key risk areas; establishes a baseline that can be used to assess remediation progress
- Inspection & Interviews – scans are complimented by physical environment review and structured interviews of key technical and business stakeholders
- Consolidated Reporting – data is consolidated into reporting appropriate for all levels of management
- Assessment & Guidance – findings are presented against leading security practices providing insights into longer-term remediation plan(s)

Checkup scales to your requirements

Satori's Health IT Security Checkup scales to your organization's size and requirements.



Automated Scans

Inspection & Interviews

Consolidated Reporting

Assessment & Guidance

HEALTH IT SECURITY CHECKUP

ENVIRONMENT

Domain	
Domain Controllers	3
Number of Organizational Units	15
Users	
# Enabled	16
Last Login within 30 days	6
Last Login older than 30 days	10
# Disabled	5
Last Login within 30 days	0
Last Login older than 30 days	5
Security Group	
Groups with Users	26
# Total Groups	71
Computers in Domain	
Total Computers	16
Last Login within 30 days	7
Last Login older than 30 days	9

	# Enabled Users	# Disabled Users
Employee - ePHI authorization	2	0
Employee - no ePHI authorization	2	0
Vendor - ePHI authorization	0	0
Vendor - no ePHI authorization	1	0
Former Employee	0	0
Former Vendor	0	0

Operating System Support

Satori Health IT Security Checkup

Satori's Health IT Security Checkup scales to your organization's size and requirements.

Task	Value	Deliverable	Sliver	Gold	Platinum
Evaluate inbound firewall configuration and search for known external vulnerabilities	· Checks for vulnerabilities in the firewall · Validates requirement for a managed firewall service (if not in place) · Ensures firewall changes and exposure of outward- facing applications are minimized.	· External Vulnerability Management Plan · External Vulnerability Scan by Issue Report	✓	✓	✓
Evaluate out-bound firewall configuration	· Tests implementation of egress filtering to ensure blocking of unnecessary traffic (eliminating spread of viruses, etc.).	· Outbound Security Report	✓	✓	✓
Evaluate current patch management	· Validates patches have been applied	· Detailed Report	✓	✓	✓
Evaluate anti-virus and anti-spyware deployment	· Validate deployment of anti-virus and anti-spyware and up to date	· Detailed Report	✓	✓	✓
Administrator review	· Validates (interviews), list of users with administrative privileges	· Detailed Report	✓	✓	✓
Share permission review	· Validates which users have access to critical business data through interview with the business owner	· Share Permission Reports	✓	✓	✓
Physical security walk-through	· Provides an in-person walk-through of facility	· Response Report	✓	✓	✓
Internal vulnerability scan	· Scans for internal vulnerabilities to identify security flaws that could be exploited	· Internal Vulnerability Management Plan · Internal Vulnerability Detail Reports		✓	✓
Anomalous login detection	· Reviews security audit logs looking for suspicious logins	· Anomalous Login Report · Login History Reports		✓	✓
Security policy assessment	· Reviews default Group Policy and applicable Local Security Policies	· Security Policy Assessment		✓	✓
IT Administrator Review	· Reviews user, computers, and Layer 2/3 detail identify any rogue users and systems	· Layer 2/3 Reports · Detailed Report		✓	✓
Compliance-level auditing	· HIPAA compliance-level audit to identify security violations.	· HIPAA Evidence of Compliance Report			✓
		INVESTMENT**	$3,500	$5,000	$7,500+

** Based on estimated device counts

Customer Responsibility

- Completion of a Non-Disclosure Agreement (NDA)
- Provide Technical details of network and infrastructure; support pre-scan preparation
- Stakeholder questionnaire completion and interview
- Participation in risk vetting and prioritization

Satori Value

A Health IT Security Checkup service provides many benefits including:

- Cybersecurity & Compliance Risk Assessment – The Satori team brings current security knowledge based upon regulation interpretation and independence relative to findings and guidance.
- Security Leading Practices – Satori's industry leading expertise identifies existing risks and supports internal communication and prioritization for remediations.