Tech Data | Security Solutions

PROFESSIONAL SERVICES

Tech Data has a team of security professionals who are ready to help you deliver comprehensive security services to protect your customers.

Assessments

Tech Data's Assessment services can either evaluate the technical controls of a customer's environment via our Security Maturity Assessments or can deliver a deeper technical security test of their network with Vulnerability Assessments and Penetration Tests. The outcome of these services identifies security weaknesses and exploitable vulnerabilities with objective results and clear recommendations. This not only provides Tech Data's resellers a roadmap to recommend and deliver appropriate security products, but also services that best fit the customer's needs.

Vulnerability Assessments	Security Maturity Assessments	Physical Security Assessments
Penetration Testing	Cisco dCloud (POV)	Physical Penetration Testing

Compliance

Let Tech Data help you deliver compliance readiness services to your customers. We offer governance, as well as risk and compliance services across many of the industry-wide regulations, including HIPAA, HITRUST, PCI-DSS, NIST 800-171, ISO 270001, NERC-CIP, SOC 1&2, GDPR and more. Our services provide partners peace-of-mind and allow us to serve as their compliance advocate. We understand their driving needs, whether that means working with designated third-party auditors or helping certify additional staff as needed during the process.

CCPA	California Consumer Privacy Act	The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California.
CMMC	Cybersecurity Maturity Model Certification	The Cybersecurity Maturity Model Certification is intended to serve as a verification mechanism to ensure that Defense Industrial Base (DIB) companies implement appropriate cybersecurity practices and processes to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks.
DFARS	Defense Federal Acquisition Regulations Supplement	Defense Federal Acquisition Regulation Supplement is a set of restrictions for the origination of raw materials intended to protect the US Defense industry from the vulnerabilities of being overly dependent on foreign sources of supply.
FedRamp	Federal Risk and Authorization Management Program	The Federal Risk and Authorization Management Program is a US government-wide program that provides a set of security and privacy controls to protect federal information systems and organizations handling federal operations, assets, or individuals in the cloud.

GDPR	General Data Protection Regulation	The General Data Protection Regulation has brought a unifying set of information security regulations to protect the personal information of all citizens of the European Union (EU) and the United Kingdom (UK), regardless of where they currently reside.
GLBA	Gramm-Leach -Bliley Act	The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
GRC	Governance, Risk Management and Compliance	Governance, Risk Management and Compliance helps to avoid the ill effects of silos in the governance, assurance and management of business attributes.
HIPAA	Health Insurance Portability and Accountability Act	The Health Insurance Portability and Accountability Act of 1996 establishes policies and procedures that protect the security and privacy of Protected Health Information (PHI).
HITRUST	Health Information Trust Alliance	Health Information Trust certification by the HITRUST Alliance enables vendors and covered entities to demonstrate compliance to HIPAA requirements based on a standardized framework.
ISO 27001	Information Security Management System	ISO 27001 is an information security management framework designed to help your organization continuously secure assets such as financials, intellectual property, employee details, or information entrusted to third parties.
NIST	National Institute of Standards Technology	NIST guidance provides the set of standards for recommended security controls for information systems at federal agencies. In many cases, complying with NIST guidelines and recommendations will help federal agencies ensure compliance with other regulations, such as HIPAA, FISMA, or SOX.
NYDFS/ NYCRR	New York Department of Financial Services	The NYDFS Cybersecurity Regulation (23 NYCRR 500) is a new set of regulations from the NY Department of Financial Services (NYDFS) that places cybersecurity requirements on all covered financial institutions.
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection	The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards that preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the Critical Infrastructure Protection (CIP) standards is to protect the critical infrastructure elements necessary for the reliable operation of this system.
PCI-DSS	Payment Card Industry Data Security Standard	The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.
SOC 1	System and Organization Controls 1 Report	A SOC 1 Report (System and Organization Controls Report) is a report on Controls at a Service Organization which are relevant to user entities' internal control over financial reporting.
SOC 2	System and Organization Controls 2 Report	A SOC 2 Report evaluates the information security, confidentiality, availability, integrity, and privacy related to information systems in an organization and is a common requirement by clients for online services organizations.

Implementation

Tech Data offers implementation services including new installations, integration, patch services, health check services, configuration and staff augmentation services across many of our security products and solutions. Tech Data also helps with implementation of many security products such as Splunk, Palo Alto, and LogRhythm. These services are intended to help partners expand or enhance their current technical capabilities or further support their customer's security posture.

CARBONITE
Check Point SOFTWARE TECHNOLOGIES LTD.
CISCO
CYBERARK
CROWDSTRIKE
f5
FIREEYE
FORESCOUT
FORTINET
gemalto
IBM
imperva
Infoblox
LogRhythm
McAfee
okta
PING
paloalto NETWORKS
REDSEAL
RSA
SailPoint
SAVIYNT
SONICWALL
SOPHOS
splunk>
Symantec
TREND MICRO
VARONIS
WatchGuard
zscaler

Incident Response Services

Executing a swift and effective response to increasingly frequent and complex cyberattacks requires a large investment in technology, people and processes that many organizations struggle to achieve. Without a well-defined plan to contain, mitigate and recover from a security breach, businesses are left vulnerable to attacks. Tech Data Incident Response (IR) services helps ensure that your customers have the right capabilities in place to effectively respond to cyber threats.

CONTACT US

For more information, email securityservices@techdata.com
or call 1-800-237-8931 ext. 5540508