

Zero-touch Cyber Resiliency Services For Managed Service Providers



Accedian's Cyber Resiliency Services enable MSPs and MSSPs to resell or white-label a comprehensive offering of services and solutions for today's ever-present cyber threats.

- Eliminate the overhead of building a technical cybersecurity practice with experts to monetize the red-hot cybersecurity market
- Easily address the mid-market consumers of services, closing their staff and skills gap
- Select service bundles or à la carte options to suit your needs, and choose flexible partner-branded or referral options
- Take advantage of an award-winning delivery team recognized by **Gartner** (Top 10 Security Consulting Vendor) & **Clutch** (Top Cyber Security Company in 2020)

Become a strategic partner to your client with next-generation Cyber Resiliency Services

- For MSPs, Agents, Consultants and SIs: easily incubate a cybersecurity services business
- For MSSPs: conveniently fill gaps in your current cybersecurity services portfolio

Market Opportunity

Global spending on security-related hardware, software and services will grow at a compound annual growth rate (CAGR) of **9.2%** between 2018 and 2022 to total of **\$133.8B** in 2022.

Source: IDC

Cyber resiliency consulting and vCISO

- Harden security postures and set up policy and programs with a vCISO Service. Advisory and supervisory services for all identified security measures necessary to effectively protect a client's assets with a Cyber Resiliency Consulting Service. Deliver knowledge and expertise to assess, prevent, mitigate, and respond to possible security threats and breaches.

Pentesting, ethical hacking and vulnerability assessments

- Vulnerability Assessments assess perimeters, organizations, and applications for potential vulnerabilities that could expose critical organizational systems, data and financial assets.
- Pentesting combines the tools and techniques used by malicious "hackers" with disciplined scientific procedures to provide unique insight into the state of security for customer Information Systems environments and network vulnerabilities from an external hacker's perspective. Network devices, including firewalls, routers, switches, servers, printers, and remote-access devices, connected to the Internet (DMZ and LAN) will all be assessed.
- Ethical Hacking takes you to the next level! As certified Ethical Hackers, we go beyond risk assessment and carry out the exploits using a wide range of techniques and attack vectors.

Managed detection & response (MDR)

MDR is a 24x7 Security Monitoring Service (as a subscription) that delivers the proper people, processes, and top SIEM technology for an effective security program. Security analysts will continuously monitor and notify customers of potential security incidents.

Incident response

Conduct incident forensics and response, ransomware recovery, and assess and improve overall security posture to mitigate any other potential entry points for attackers (Security Hardening Service). Work with the customer IT/Security team on-site to ensure the network, infrastructure and data is safe, to implement all required cybersecurity best practices, and to confirm that security remediation has reduced the probability of further breaches.

For more information, contact your Accedian Account Manager or reach out to us at accedian.com/contact.