Security consulting services

Comprehensive, 360-degree cybersecurity solutions from architecture planning to verification testing

perspecta LABS

Introduction

Today's communications environments are highly interconnected, interdependent systems with a growing variety of remote access capabilities and employ an increasing number of security controls. Your network, applications, data, processes and people are always changing. So are your physical and cybersecurity vulnerabilities as the threat landscape rapidly evolves and attack surfaces expand. Cyberattacks now affect organizations of all types and sizes in dramatically increasing numbers. A substantial disruption to your networks would have a profound impact on the confidentiality, integrity and availability of mission-critical services on which your business rely.

Perspecta Labs end-to-end cybersecurity consulting services help you determine your cybersecurity posture and risks to your business, in addition to fortifying your organization from threats. With decades of cybersecurity experience in public and commercial sectors—spanning defense, communications, energy, transportation, healthcare, finance and entertainment—Perspecta Labs has been providing customers with state-of-the-art security services from comprehensive security programs and risk assessments to innovating new methods, techniques and tools to address their dramatic environmental changes. Perspecta Labs' ground-breaking applied research and solution development experience has been performed for government agencies to advance the science of cybersecurity protection for complex networks, data and critical infrastructure.

Cybersecurity services to fortify your security posture

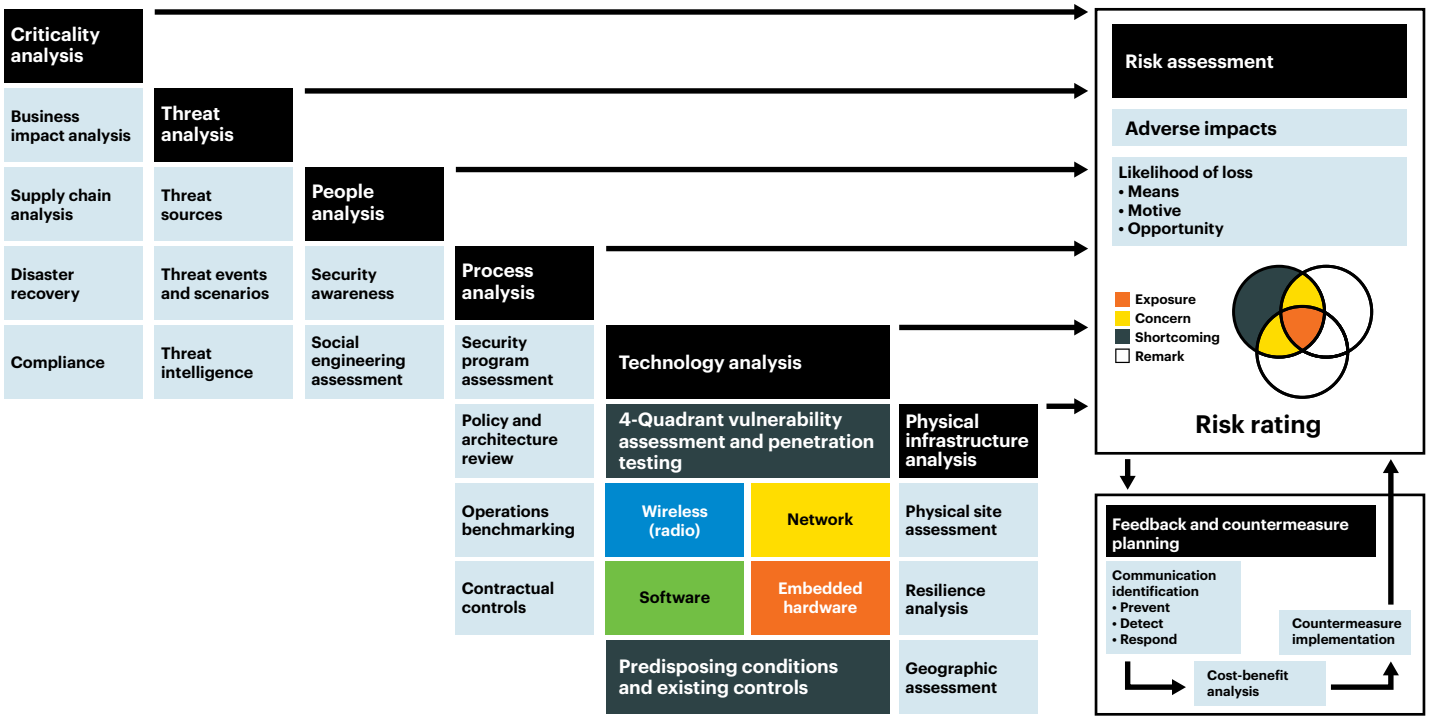
Perspecta Labs offers a comprehensive, 360-degree suite of cybersecurity services to help you develop, assess and maintain an effective end-to-end security management program to meet your changing needs in today's threat-laden business environments.

Criticality analysis

We provide services to help you identify and assess the criticality of your business assets and processes and their proper prioritization to ensure their availability under conditions of stress.

Business impact analysis: Perspecta Labs helps you focus attention and resources on business processes and their supporting applications, networks, personnel resources, critical relationships to internal and external organizations, as well as interdependencies that are critical to business operations. If these resources or business process attributes are corrupted or disabled, it would likely lead to mission failure or degradation. Perspecta Labs helps you identify and group mission threads, decompose these interdependences into their functions and assign them criticality levels. We map the mission-critical functions to the system architecture and identify the components that implement those functions. We then work with you to assign criticality levels to those components in proportion to the consequence of their failure on the system's ability to perform its mission. Furthermore, we apply DOD Trusted Systems and Network techniques along with other applicable commercial standards. Perspecta Labs works with managers and executives of all organizations in a structured approach to ensure proper balance and to drill down to the components that support the top three to five critical business processes to identify recovery time and recovery point objectives, risk impacts, tolerances, constraints and trade-offs via a collaborative approach across organizations.

Supply chain analysis: As product supply chains become increasingly global and complex, the threats they pose to your network and services become more serious and often, harder to track—especially as they extend to off-shore developed and maintained system components and software, each with their own supply chain. We provide a holistic approach to supply chain integrity, with risk mitigation elements that include procedural, contractual, physical, and technical approaches. We surpass the basic product and life cycle testing done by most organizations to provide a comprehensive analysis of the vulnerabilities in your critical vendors' products and even in their supporting supply chains. We help you reduce the risks and make sure you are implementing the appropriate controls on an end-to-end basis.



Disaster recovery: Perspecta Labs helps customers fortify their emergency management program to organize and manage their resources and responsibilities for dealing with all aspects of emergencies such as preparedness, response, continuity of operations, incident mitigation and recovery. The aim is to reduce the harmful effects of all hazards, including physical and cyber disasters. We help customers focus on preparing technology, people and processes for use when a negative event occurs. Our assessment and recommended plans seek to reduce our customer's vulnerability to disaster, mitigate the impacts of a disaster, or respond more efficiently in an emergency. Our services can include continuity of operations planning to ensure that organizations are able to continue performance of essential functions under a broad range of circumstances. They can also include disaster recovery planning for specific organizations, processes or functionality.

Compliance: Regulatory compliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with laws and regulations relevant to their business sector. Perspecta Labs services seek to determine and interpret the growing number of relevant requirements your business faces to subsequently develop cost-effective response plans and estimate the cost for non-compliance fines, penalties and litigation. We also consider the negative business impacts of non-compliance such as loss of customers, investor concerns, and impacts exposing assets to cyberattacks.

Threat analysis

Perspecta Labs develops an adversary model in order to identify vulnerabilities and examine potential threats based on those vulnerabilities. The model is based on your industry and company environment. These include unclassified information that Perspecta Labs is privy to through its participation on government programs.

Threat sources: We use a broad range of threat sources from selectively identified internal sources and intelligence services, to external industry accepted and evaluated threat sources including: the National Electric Sector Cybersecurity Organization Resource (NESCOR), Department of Homeland Security (DHS), National Cybersecurity and Communications Integration Center (NCCIC), Idaho National Laboratory (INL), the Cloud Security Alliance, North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP) standards, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and Perspecta Labs industry domain expertise. Threat agent types are created to model nation-states, terrorists, industrial spies, organized crime groups, hacktivists, hackers and insiders—including those perpetrators with authorized privileges beyond basic user privileges such as employees, contractors, trusted partner staff and vendors. Our multifaceted threat categories each have their own capabilities, intent, and targeting characteristics which thereby generate independent likelihoods and impacts of a threat event.

Threat events and scenarios: Perspecta Labs develops customized attack trees to assess the sequence of actions adversaries may take across your network, hardware, software, and wireless domains. We identify a set of representative threat scenarios threat agents have been known to execute to exploit a vulnerability causing an adverse impact and we apply risk ratings per threat scenario.

Threat intelligence: Perspecta Labs assesses your threat intelligence efforts to determine if they are achieving the key mission to research and analyze emerging threats, trends and technical developments. Perspecta Labs subsequently applies this information to help your company understand threats and mitigation approaches to ultimately reduce enterprise risk and reduce incident recovery time. We look at all threat categories applicable to your industry—how you are gathering, assessing and distributing information—and if the appropriate feedback loops and continuous service improve processes are working. We look at attacker tactics, techniques and procedures. We assess your automated detection tools used to aggregate, correlate and analyze threat data to support defensive actions. The goal is to migrate customers to a predictive cybersecurity posture where better decision-making occurs both during and following incidents, as opposed to having to be reactive to threat occurrences.

People analysis

People are among a business' most valuable and dynamic assets, making them both potential vulnerabilities and security controls. Perspecta Labs includes people analyses as one of our core security services.

Security awareness: Perspecta Labs takes a holistic user-centric approach to security awareness. We work with you to understand your needs, problems and constraints to discover your current security awareness posture as a component of your bigger security program. We will help your policies and procedures with periodic simulation exercises, protection of communications, end-point protection and potential technology solution selection. Enabling you to determine what you should and can measure to establish effective ongoing metrics, how to decipher results and how to properly respond. Furthermore, Perspecta Labs can help you develop an effective training program that may include periodic live, on-line, and refresher training that instills employees with a sense that security is now everyone's role in this relentless cyber battle against unseen adversaries. We also examine your ability to ingest the evolving threat intelligence that should act as input to your continual service improvement program.

Social engineering assessment: Social engineering is the clever manipulation of the natural human tendency to trust a common action, in order to acquire sensitive business or infrastructure information, data and credentials to degrade service, damage assets or steal. It has become the most common and effective initial attack vector. Our social engineering assessment seeks to identify vulnerabilities due to insecure behaviors of employees and other personnel, often resulting from ineffective security awareness training. Perspecta Labs conducts phone-based social engineering and email phishing tests customized to your unique needs rather than providing a general subscription service with emails that are quickly recognized as phishing bait. We develop test scenarios to entice a representative sample of employees, including all levels of management, to open an e-mail and click on a URL or run commands on their computer to uncover their susceptibility to social engineering attacks. To provide realism to the scenarios, Perspecta Labs registers a domain name, sets up e-mail and creates a web page to support the claimed identity, while considering seasonal and cultural tendencies such as people's focus on holidays, sporting events and tax reporting.

Process analysis

Processes are as central to a strong cybersecurity posture as they are to business flows and quality assurance. Thus, Perspecta Labs looks at how your business applies your policies and standards, and properly uses and secures your data and your customers' data.

Security program assessment: Our enterprise-wide security assessment seeks to evaluate the effectiveness and pervasiveness

of your company's business risks in order to make informed decisions. We search for artifacts that demonstrate how your company is dutifully implementing those policies and controls in practice, and render an opinion about whether it has sufficient and effective coverage based on our findings, experience and industry best-practices. Perspecta Labs applies its proven assessment methodology and maturity model to objectively and independently evaluate your security program. Perspecta Labs assesses the adequacy and implementation of security policies and their use in daily operations by analyzing daily practices, critical policies and procedures, as well as holding in-depth structured interviews with stakeholders and key organizations. We apply our comprehensive security maturity model which addresses more than 30 areas. It incorporates principles from multiple standards frameworks including European Union consumer data regulations and recent state legislation in the U.S. concerning consumers' rights of the use and protection of their data. We highlight both strengths and weaknesses in your security program and present our key findings along with practical recommendations for improvement. This approach has proven effective to identify inconsistencies between what employees should be doing versus what they may be actually doing and why.

Policy and architecture review: Perspecta Labs helps organizations architect and deploy practical, defense-in-depth security strategies. Beginning with business needs and environmental assessments, we help you establish the primary technical and operational security requirements for your organization. Based on these requirements, we formulate a cohesive set of security policies tailored to your organizations' unique needs using industry best practices. We help you implement these policies with robust security architectures, solution assessment and selection, operational procedures, training, and enforcement programs to effectively ingrain a higher level of security into your day-to-day operations. Our objective position allows us to provide forthright opinions about product selection, program effectiveness and cost-benefit trade-off.

Operations benchmarking: With vast experience in government and enterprise network operations centers, we can evaluate your staff's effectiveness compared to similar enterprises, as well as the operating procedures they use to detect, respond to, and contain malicious events and network failures. Our cyber intrusion exercise is a unique Perspecta Labs security services offering. In it, we orchestrate a realistic series of cyber events based on your network that are played out in an interactive table-top environment. The goal is to assess and improve the effectiveness of the network operations center staff by training them to correlate information from a variety of sources in order to diagnose malicious cyber problems; identify a multipart attack from independent, random events; effectively communicate inside and outside the organization; and organize a response and perform in high-stress situations.

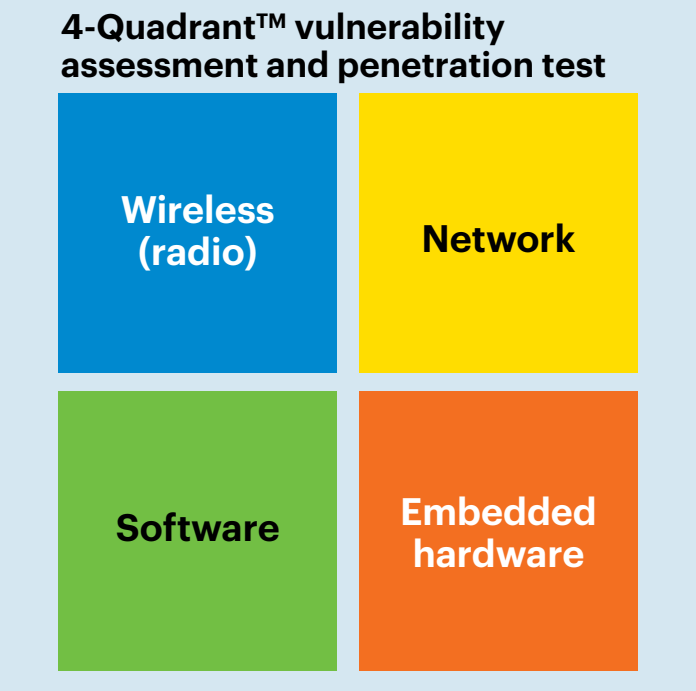
Technology analysis

Our suite of technology security analyses applies Perspecta Labs' deep and broad experience, and customized methodologies and tools with the focused needs of the public and commercial sectors to provide customers with a comprehensive view of their security posture, possible solutions to fill gaps and insights into trends to help prepare for the future.

4-Quadrant vulnerability assessment and penetration testing: Leveraging our invaluable knowledge and insight, Perspecta Labs has developed state-of-the-art vulnerability assessment and penetration testing services which employ a comprehensive systematic approach that includes targeted manual assessments of policies, processes and procedures to address multiple environmental factors. Perspecta Labs runs automated scans against systems, networks, and access capabilities in addition to manual analysis. Our penetration testing seeks to simulate a real-world attack on your networks, systems, and data to evaluate the risk profile of your environment. This includes understanding the level of skill required and time needed for an attacker to exploit each vulnerability and the level of impact to your organization if the attack is successful. For its deep analyses, Perspecta Labs' utilizes its innovative 4-Quadrant™ Assessment Methodology, a honed and proven approach to go beyond traditional IT security vulnerability assessments and penetration testing. It provides a holistic, integrated evaluation of security weaknesses across each of the quadrants of a customer's environment to expose and mitigate critical risks not apparent when looking at one quadrant at a time. These quadrants are:

- Service and management applications software
- Network infrastructure and access
- Wireless communications and modulation scheme and coding
- Embedded hardware and firmware

To assist customers in selecting methods of migration , breaking industry standardization, Perspecta Labs creates attack trees to illustrate vulnerabilities, exploit paths and dependencies.



Predisposing conditions and existing controls: Perspecta Labs assesses predisposing conditions, which may be vulnerabilities or factors influencing threat opportunities in either a positive or negative direction. They may include geography and environmental factors, regulatory and compliance, financial, personnel, technology, supply chain, or contractual constrains or opportunities. We customize for your business needs, the taxonomy structure outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 to assess their pervasiveness and security impacts to your business.

Physical infrastructure analysis

Perspecta Labs looks at the aspects of the physical environment within, which your process and supporting technologies operate.

Physical site assessment: Perspecta Labs typically performs a security site assessment as the physical infrastructure component of a vulnerability assessment. Sites can include the data centers in which the software and hardware operate, disaster recovery sites, operations and call centers, customer accessible service centers, office complexes and specialized sensitive data processing facilities.

Resilience analysis: This analysis focuses on the implementation of resilience thinking and includes a variety of approaches from assessing resilience and developing new methods to quantify resilience unique to your business, to detecting thresholds and guiding the development of plans, which contributes to understanding how to put resilience into practice in your specific environments. We use a framework that considers metrics with absorptive, adaptive and restorative capacities to support investigation of deep resilience uncertainties.

Geographic analysis: A fundamental aspect of risk assessment is that natural or industrial hazards are location dependent. Furthermore, generally reliable historical and location specific data are available regarding failures, potential damages and GIS techniques that can be central to risk identification, quantification and evaluation. Our geographic analysis help managers make decisions that may not otherwise be apparent (e.g., recognition of relationships, patterns and trends). This information is typically factored into an enterprise risk assessment.

Risk assessment

Perspecta Labs typically provides a risk analysis as the final and key component of an enterprise risk management program assessment. It presents a ranking of the likelihood of a negative incident occurring and the possible range of consequences should it occur. We use your risk ranking tool or provide one to help you better understand your company's risk posture and make wise management decisions to formulate countermeasures. Customizing the risk assessment framework in NIST 800-30 for your needs, Perspecta Labs draws from its customizable security maturity model to identify potential operational, safety, reliability, privacy, financial, compliance, reputation risks and integrity threats. We tailor the risk model to the unique aspects of your company structure and operation based on a criticality analyses, and Perspecta Labs knowledge of the industry and standards. We assess adverse impacts to your organization, the likelihood of loss (defining the various threat agents' means, motivations, and opportunities), and finally, assess your organizational risk.

Feedback and countermeasure planning

To reduce the likelihood that threat events will result in adverse impacts, Perspecta Labs helps customers assess threat intelligence and current countermeasures, and plan future safeguards and countermeasures proportional with the risks appropriate for their business.

Countermeasure identification: Once threats and vulnerabilities are identified and ranked, Perspecta Labs helps customers explore alternative tactical and strategic countermeasures for their risk reduction capabilities and meet their security program's prevent-detect-respond goals and enterprise appetite for risk. We finish with addressing the needed feedback to your continual service improvement program.

Cost-benefit analysis: We help you develop a realistic cost-benefit model and recommendations that synchronize with your company's business goals and compliance requirements and work with you through the decision-making process. We'll help you assess which technologies best help you reach your high priority goals.

Countermeasure implementation: Using our plan, design, build and operate model, we help customers negotiate the new technology insertion process including using agile methods from development of prioritized requirements with stakeholders, issuing and assessing solicitations and manage vendor trials through value realization. We'll help you determine the risks and value of cloud services versus native capabilities, and when and how to engage third-party providers.

Summary

Reading through our security service descriptions you should have noticed several themes—Perspecta Labs has successfully supported diverse customers with high-value cybersecurity consulting services. We have conducted assessments and improved security for management and business processes, supply chain and staff, hardware and software, as well as critical network infrastructure, services, applications, media, data and information. Some of the markets we serve include:

- Transportation
- Telecommunications
- Electricity, water, waste water, energy and other utilities
- Defense and critical infrastructure
- Finance, banking and insurance
- Federal, state, regional and municipal
- Health care and pharmaceuticals
- Entertainment and media

Built on decades of prominent research and cybersecurity experience in public and commercial sectors—Perspecta Labs has an unmatched security perspective—we understand an enterprise's end-to-end security needs and can help you develop the optimum plan for your business.

We understand the importance to your business of customizing the growing number of cybersecurity standards, regulation and legislation emerging as the use of data grows exponentially and threat agents proliferate—we understand one size does not fit all and can help you customize solutions to meet your unique needs.

We bring to bear leading-edge knowledge and exposure of the best practices across multiple industries to help improve your security posture and keep your networks secure in these increasingly challenging environments—we know what works well and what does not work well in different environments to help you get it right the first time.

We appreciate the value of data to all your business processes, the data related attack surfaces they present and the increased focus on data security by regulators—we treat data as its own domain equal to people, processes and technology to help you comply with regulations and maintain your customers' confidence.