CHECK POINT™

YOU DESERVE THE BEST SECURITY

Cyber Security Consulting and Risk Assessment Services

By The Check Point Strategic Consulting Group | Global_Architects@checkpoint.com

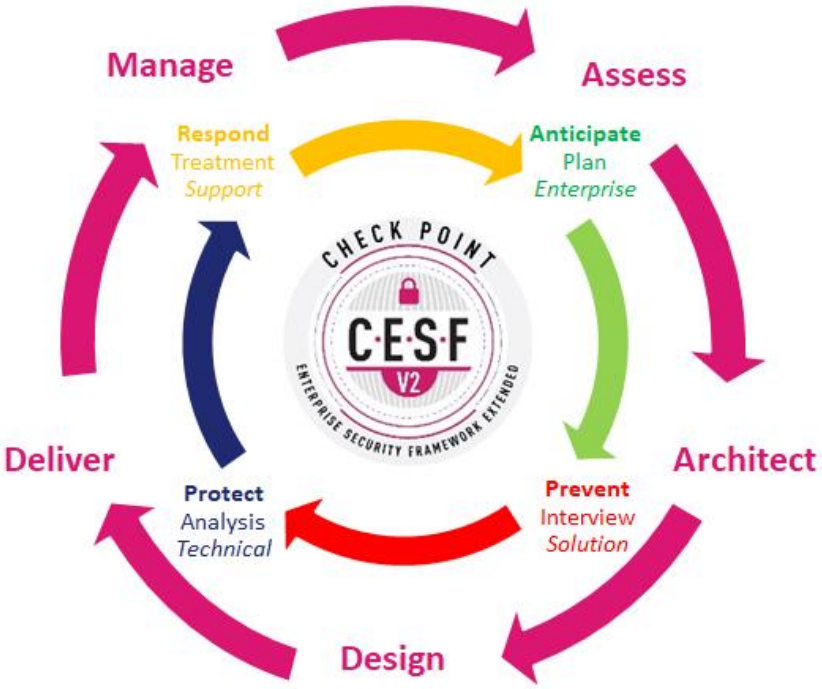
v3.5 (2023)

CHECK POINT™

YOU DESERVE THE BEST SECURITY

Introduction

The Check Point Strategic Consulting Group is pleased to release the following service catalog, which will act as a reference for the services it is responsible for.



The consulting group exists to support decision-makers, engineers, and architects. This is achieved through a combination of assessments and advisory and architectural services designed to leverage industry-standard techniques and help improve the client's overall cyber security posture.

Furthermore, the group aims to deliver recommendations based on real-world cyber security risks identified using industry-standard consulting practices.

By using well-versed cyber security techniques such as threat modeling, control-based assessments, and standard risk management frameworks, the cyber security conversation can be presented to the whole organization. This will give the cyber security conversation a broader and more impactful appeal.

Cyber security leaders know that cyber is not just a technology challenge; the cyber security program must capture people, processes, and technology elements to succeed. Because of this, we have developed services focusing on risk management, cost efficiency, operational and technological architecture, and solution accountability. We also address cyber security risk management throughout the whole organization, not just the technology sphere. Some of the services offered are:

- *Zero Trust Architecture and Advisory*
- *SABSA Enterprise Security Architecture Framework*
- *NIST Cyber Security Framework (CSF) Assessment*
- *NIST SP 800-53 and NIST RMF*
- *Risk and Threat Modeling*
- *Center for Internet Security*
- *CIS Critical Security Controls*
- *Cloud Security Alliance Cloud Controls Matrix*
- *MITRE ATT&CK Mapping*
- *Purdue and IoT Frameworks*
- *Check Point Best Practices*

The goal of strategic consulting is to perform advisory, assessment, and architectural work for, and on behalf, of our customers. We advise on all matters relating to cyber security, making assessments of the current security state and architecture to address gaps and improve overall posture.

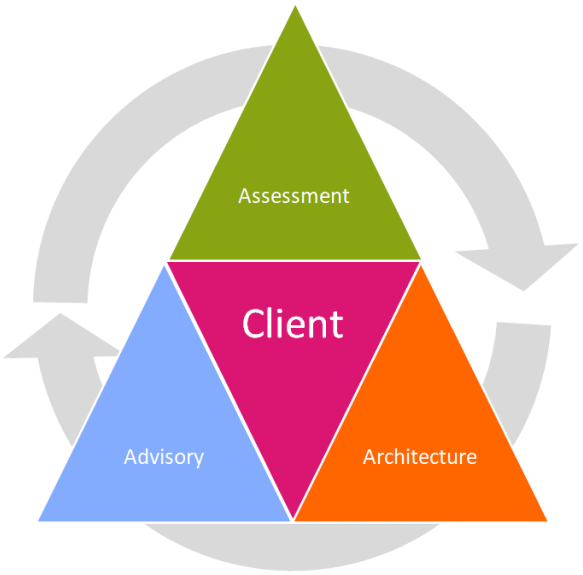
Service Pillars

Strategic Consulting is based on three (3) pillars: ***Assessment, Advisory, and Architecture****. It is designed in response to client requests for a single engagement point for all consulting services.*

Assessment: *The assessment focuses on governance, cyber risk, and compliance. This assessment aims to help the organization understand its overall governance, cyber risk, and compliance posture and take the necessary steps to improve it.*

Advisory: *Advisory services provide expert guidance and advice to organizations on protecting their systems and data from cyber threats. The focus is on strategy, digital transformation, new technology adoption, and alignment to industry standards such as Zero Trust, SASE, SSE, etc.*

Architecture: *Architecture services focus on the security aspects of an enterprise network. A security architecture review aims to identify and evaluate potential vulnerabilities, threats, and risks that may affect the system's security and provide a recommended "to-be" architecture based on the industry's best practices.*

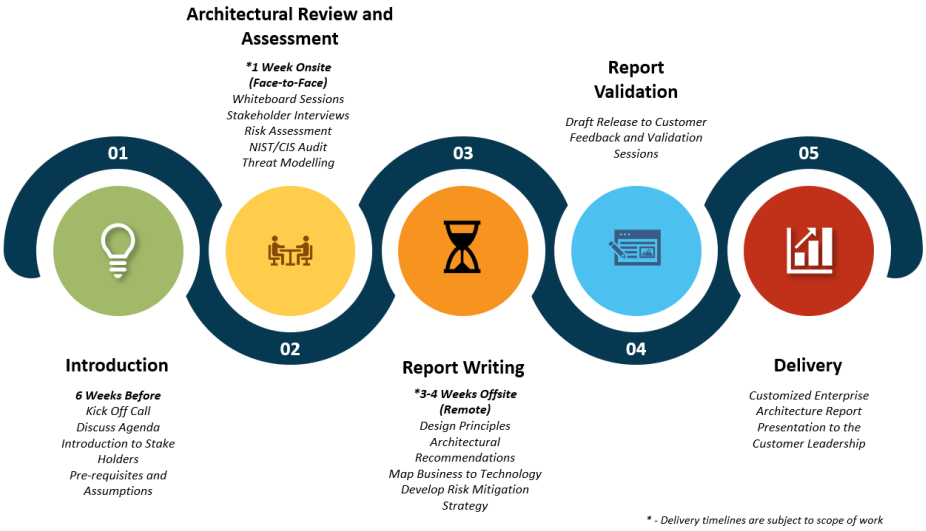


Service Pillars

Consulting Workshops

Regularly engaging in open-forum-focused face-to-face workshops is the most effective vehicle for building long-term relationships with our clients. This is why we place our workshops at the center of all our proposals and, wherever possible, include a series of advisory workshops. Such engements allow for the consulting team to build the necessary relationships with the relevant business stakeholders, and ensure a healthy partnership between the consultants and the needs of the organization. Specifically, *assessment* workshops are interview and evidence-based, *advisory* workshops are roundtable and open forum, and *architecture* workshops are whiteboard and design-focused.

A global enterprise architecture team always leads engagements in conjunction with local and regional solutions architects and subject matter experts. The timeline (right) shows how a typical workshop is planned and executed.

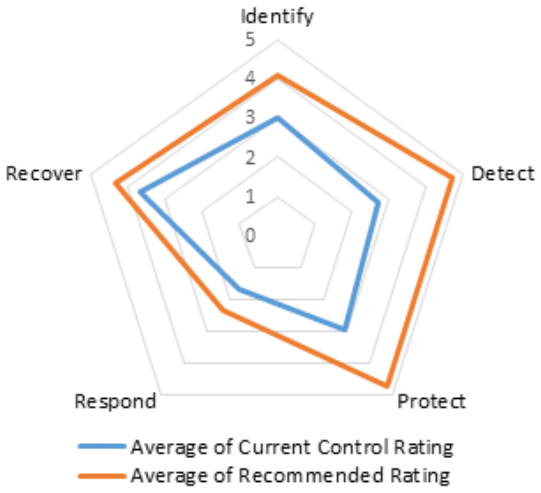


Consulting Services

Assessment: *Our assessment workshops are interview and evidence-based, our advisory workshops are roundtable and open forum, and the architecture workshops are whiteboard and design-focused.*

- ***Framework-Based Assessment – NIST CSF, NIST 800-53, CIS Benchmarking, etc.***
  The key objective of this assessment is to evaluate the cyber security posture against industry standard frameworks. Such can include the Cyber Security Framework (NIST CSF) developed by the National Institute of Standards and Technology and the CISv8 from the Center of Internet Security (CIS). These control-based assessments are delivered using industry-standard techniques, the output of which is an overall capability score and a detailed set of implementable recommendations.

  A compliance-based assessment is very useful for understanding the likelihood of a successful cyber-attack and, therefore, an important component of a cyber risk assessment.

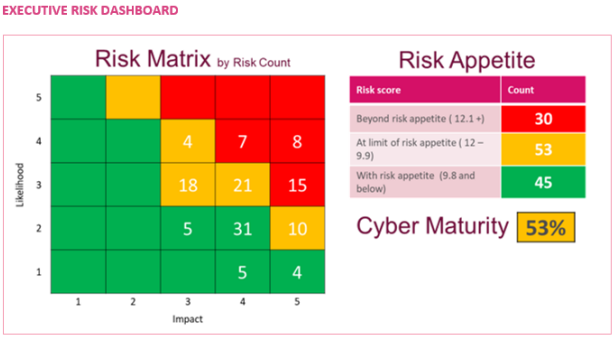


- ***Zero Trust Maturity Assessment***
  We perform a targeted Zero Trust maturity assessment to evaluate an organization's readiness to adopt and implement the Zero Trust framework or to measure the completeness of the existing Zero Trust adoption. This assessment typically involves reviewing the

organization's current security posture against open standards such as CISA and NIST 800-35, and identifying areas where design principles can be applied. The assessment also includes a review of the organization's existing security policies, procedures, and controls, as well as its security infrastructure and technologies.

- ***Cyber Risk Assessment***
  Our Cyber Risk Assessment aims to address the challenges of implementing aspects of an effective cyber risk management strategy and propose recommendations that increase its efficiency. In addition, the program is geared towards supporting C-level decision-makers using industry-standard RISK calculations and tools.

  Reducing risk using quantitative analysis is sometimes a challenge. However, for those responsible for minimizing the financial impact of cyber security events, it's a necessary calculation and a valuable tool in communicating risk. The standard risk calculation we use is based on the following formula:
  RISK (R) = LIKELIHOOD (L) x IMPACT (V)



- ***Compliance-Based Assessment – HIPAA, GDPR, PCI-DSS, etc.***
  This assessment focuses on ensuring that the organization follows the relevant laws, regulations, and policies that apply to its industry and operations. Our team can assist with data privacy, health and safety, and financial regulations such as HIPAA, PCI-DSS, etc. The results of this assessment can help identify areas where the organization may be non-compliant and develop a plan to address any identified issues.

- ***Threat Modeling – STRIDE, PASTA, DREAD, etc.***
  Threat modeling is a proactive approach that aims to identify vulnerabilities and weaknesses in systems, networks, or applications that attackers could exploit. The approach also takes steps to reduce the risk of those vulnerabilities being exploited. Our team can assist in recognizing the best approach depending on the specific needs and resources of the organization using techniques such as STRIDE, PASTA, etc., and assist in identifying vulnerabilities, prioritizing resources, improving security, complying with regulations, and reducing risk.

- ***MITRE ATT&CK Mitigation***
  Our team relies on the MITRE ATT&CK framework to understand and evaluate cyber adversaries' tactics, techniques, and procedures (TTPs). This exercise is complimented with the threat modeling exercise to ensure the implementation of countermeasures against the TTPs identified in the MITRE ATT&CK framework. This can include technical measures such as firewalls and intrusion detection systems, as well as non-technical measures such as employee training and incident response planning.

- ***Supply Chain and Merger Assessment***
  Our experts work with organizations to evaluate the risks and vulnerabilities associated with an organization's supply chain and any potential mergers or acquisitions. This includes evaluating the potential risks, cyber security practices, and hidden red flags of the organization's suppliers, and developing strategies to mitigate the identified risks.

- ***Zero Trust Maturity Assessment***
  We perform a targeted Zero Trust maturity assessment to evaluate an organization's readiness to adopt and implement the Zero Trust framework. This assessment typically involves

reviewing the organization's current security posture and identifying areas where design principles and architectural best practices outlined in the Zero Trust framework can be applied. The assessment also includes a review of the organization's existing security policies, procedures, and controls, as well as its security infrastructure and technologies.

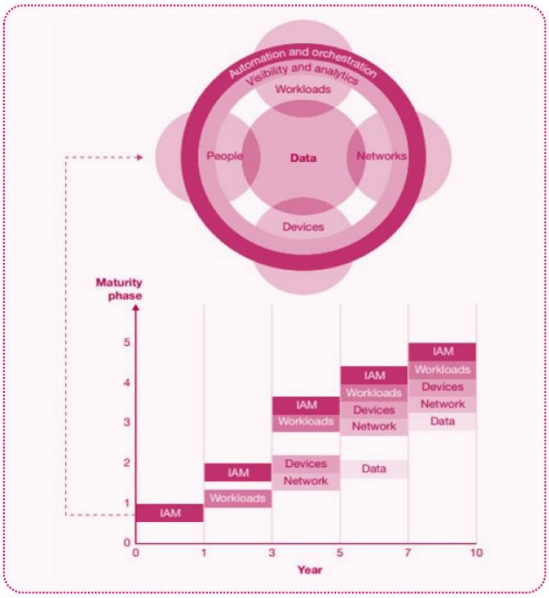
CHECK POINT™

YOU DESERVE THE BEST SECURITY

Advisory: *Our advisory service offers expert support and counsel to organizations on safeguarding their systems and data from cyber threats. There is also an emphasis on strategy, digital evolution, adoption of new technologies, and adherence to industry standards like Zero Trust, SASE, SSE, etc.*

- ***Zero Trust Advisory***
  Our team is experienced in conducting Zero Trust advisory workshops, where we can help organizations understand the principles of Zero Trust and how they can be applied to their specific environment. During the workshop, we work with organizations to understand their specific needs and help to develop a plan for implementing the least privilege principle and increased visibility across their systems and data. During the workshop, we also perform a Zero Trust maturity assessment and review the current state of the security design.

  This may include identifying users and devices that require access, determining what access they need, and implementing controls to ensure that access is granted and monitored appropriately. Additionally, we focus on increasing visibility, providing organizations with complete visibility into all their systems and data, including data center and cloud environments, as well as all users, devices, and applications that access them.

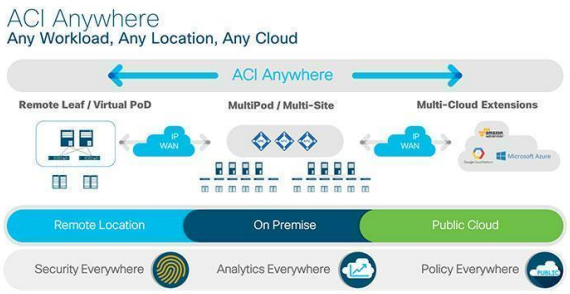


- ***Cloud Security and Architectural Design Principles***
  Our vendor-agnostic approach allows us to recommend security best practices that can be applied across multiple cloud providers. Our team has expertise in architectural design principles and can help organizations design their cloud infrastructure in a secure and scalable manner while optimizing cost and increasing performance efficiency. From serverless technologies, security expertise around applications, code, and runtime environments, securing databases to defining best practices for identity and access management (IAM), our team's extensive experience in multi-cloud security can provide insights and guidance to create a roadmap for better operational excellence and sustainability.

- ***DevSecOps and Application Security***
  Our team is skilled in providing workshops on DevSecOps practices and application security, utilizing industry-standard frameworks to ensure the highest level of security for your systems. By utilizing frameworks such as CNAPP and the 4Cs model, our team can provide robust and effective security measures for your applications and infrastructure, helping to protect against potential threats and vulnerabilities. Whether an organization is looking to secure a new development project or needs to assess and improve the security of an existing system, our team is ready to assist.

- ***Field CISO***
  Organizations can enlist the help of the Field Chief Information Security Officer (CISO) service. The field CISO works with the organization's leadership team to develop and implement a long-term cyber security strategy and provides on-site cyber security expertise. The field CISO

can also help organizations strengthen their cyber security posture and protect against potential threats by conducting cyber security assessments, identifying and mitigating vulnerabilities, and managing incident response efforts.



- ***Data Center Transformation***
  Our team is outfitted to assist with data center transformation, which involves evaluating and improving the processes, systems, and technologies that support an organization's data center operations. This may include modernizing legacy systems, optimizing resource utilization, and improving efficiency and agility. Our team is skilled and can make recommendations when working with niche technologies such as ACI (Application Centric Infrastructure) and NSX (Network Security Extension), which are specialized solutions designed to enhance performance and transform data center environments.

- ***Service Edge Technologies – SASE, SD-WAN, SSE, etc.***
  Our team offers expert advisory services on a variety of edge network and security technologies, including SASE (Secure Access Service Edge), SD-WAN (Software-Defined Wide Area Network), and SSE (Secure Services Edge). Our experts can also help organizations develop a deep understanding of the complexities and challenges associated with these technologies and can provide guidance on how to implement them effectively in different use cases. The team will also highlight the benefits of each of these technologies, while working with the organization to create a customized strategy that aligns with their specific requirements and budget.

- ***Automation and Orchestration***
  Our team specializes in providing workshops in automation and orchestration using widely used automation tools such as Ansible, Python, and Chef. These workshops are designed to empower an organization with the knowledge and skills needed to reduce operational overhead and automate tasks. Through our workshops, organizations can gain a deeper understanding of the various automation and orchestration tools and practices available and learn how to use them effectively to improve the efficiency and reliability of their systems.

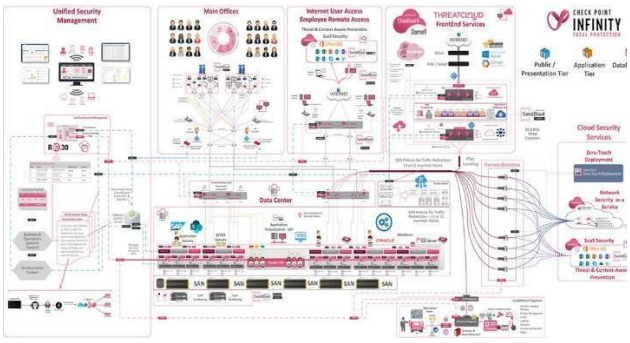
- ***Policy and Process Review***
  Our team is experienced in conducting policy and process reviews from a cyber security point of view, with a focus on helping organizations align their cyber security practices with their long-term business objectives. We review an organization's existing policies and procedures to identify any areas where they may be vulnerable to cyber-attacks or data breaches, and assess the organization's current cyber security posture, looking for any weaknesses or gaps in their defenses. Based on our findings, we provide recommendations for improving the organization's policies and procedures to better protect against potential cyber threats. These recommendations are tailored to the organization's specific business objectives and consider the unique challenges and risks that the organization faces.

CHECK POINT™

YOU DESERVE THE BEST SECURITY

Architecture: *Our architecture service concentrates on the security aspect of a company's network. The primary objective of a security architecture review is to detect and evaluate any potential vulnerabilities, threats, and risks that may compromise the system's security, and offer a suggested architecture based on industry best practices.*

- ***Security Design and Architecture Review***
  Our team specializes in security design and architecture. We can assist with reviewing and evaluating your current "as-is" architecture, while providing recommendations for a more efficient and secure "to-be" architecture. Our focus is on reducing complexity and improving cost efficiency while integrating best practices from the industry. We have the expertise and experience necessary to help ensure that your security design and architecture effectively protect your systems and data.



- ***Zero Trust Design Modeling***
  Our experts are well-versed in Zero Trust design modeling and can assist with implementing this approach to security. The team can help you design and implement a Zero Trust model that fits your unique needs and requirements, providing an additional layer of protection for your systems and data with the correct implementation of the "Least Privilege" principle.

- ***Cyber Security Gap Analysis***
  Our team of experts is well-equipped to assist with cyber security gap analysis, using a combination of industry best practices and customized approaches to help organizations identify and address their cyber security needs. Whether an organization is looking to improve its current cyber security posture, meet regulatory requirements, or simply wants to understand where it stands compared to its peers, we can provide the insights and guidance to help the organization make informed decisions about its cyber security investments.

- ***Target Operating Model (TOM) Recommendations***
  Organizations often look for a blueprint to document how they intend to operate in the future and align their resources and capabilities with their strategy to ensure that all stakeholders work towards a common vision. Our team can assist with developing a Target Operating Model (TOM), using a combination of industry best practices and customized approaches to help organizations define and implement the processes, systems, and capabilities needed to support their desired operating model. We can provide the insights and guidance needed to create a roadmap for success!

- ***Infinity Architecture Customization***
  Infinity Architecture Customization is an offering specifically for Check Point clients that allows them to tailor the Infinity Architecture to their specific needs and requirements. This customization process is designed to help organizations optimize their security investments and align their security with their business needs. By working closely with our experts, clients can develop a customized security architecture that fits their unique environment and meets their specific security needs.

- ***Security Operations Transformation***
  Security operations transformation is the process of aligning an organization's security operations with its overall business strategy and objectives. It involves evaluating and improving the processes, systems, and capabilities that support security operations, with the goal of enhancing efficiency, effectiveness, and agility. Our team of experts can assist organizations with implementing a SOC framework that combines monitoring and analysis platforms and threat intelligence services, helping them to build a solid foundation for their security operations and respond to risks quickly and effectively.

- ***IoT Assessment – ICS Purdue, ENISA IoT Security, OWASP IoT Project, etc.***
  Our team specializes in conducting Internet of Things (IoT) assessments to help organizations understand the potential risks and vulnerabilities associated with their IoT deployment. The team focuses on protecting against cyber-attacks and data breaches by implementing best practices with respect to IoT infrastructures using industry frameworks such as the ICS Purdue model, ENISA IoT Security, OWASP Internet of Things (IoT) Project, etc. This ensures that their IoT systems are reliable and secure.

- ***Risk Assessment and Mitigation – CIS RAM, NIST RMF, etc.***
  Our team is skilled in conducting risk assessment and mitigation workshops to help organizations identify and address potential risks to their operations. These workshops typically involve a detailed analysis of the organization's current risk profile, including both internal and external risks. We use a variety of techniques from industry frameworks such as CIS RAM (Center for Internet Security Risk Assessment Method) and NIST Risk Management Framework (RMF) to identify and evaluate risks. Once we have identified the organization's risks, we work with the organization to develop strategies for mitigating those risks.

Service Model

The Strategic Consulting service acts as a retained service model that can be provided to existing strategic Check Point clients and/or new-net clients looking for a trusted advisor to help them make their cyber security more robust and business-risk driven.

The service model is broken into three different categories. Each category is carefully designed to cater to clients from different industries and verticals. All activities require a scoping call to better understand the estimated time and effort required. Depending on the type of engagement, a subject matter ***ESA*** (Enterprise Security Architect) may be assigned to deliver the work.

Consulting *Pro* / *Plus*
A dedicated architect is assigned to clients who have purchased the ***Pro*** or ***Plus*** service. The architect is chosen based on the industry vertical to provide the client with valuable knowledge and field experience to develop a comprehensive understanding of their short and long-term business goals and objectives. The architect further acts as a single point of contact for the client for all consulting activities and may or may not be accompanied by different enterprise architects based on the client's requirements.

Consulting *Standard*
The ***Standard*** service is a one-time engagement that provides clients with dedicated enterprise architects or consultants, depending on the type of engagement requested by the client. The client may select one cyber security service to be delivered within a short timeframe.

	Consulting *Pro*	Consulting *Plus*	Consulting *Standard*
SKU	CPTS-3D-WORKSHOP-1000*	CPTS-3D-WORKSHOP-500*	CPTS-3D-WORKSHOP-100
Services included	Multiple engagements, 1-year subscription with access to all cyber security services including: - *Cyber Risk Assessment* - *Gap Analysis* - *Security Architecture Review* - *Zero Trust Advisory* - *CISO Services* - *Cyber Resilience* - *Security Advisory*	Multiple engagements, limited time access to all services including: - *Cyber Risk Assessment* - *Gap Analysis* - *Security Architecture Review* - *Zero Trust Advisory* - *CISO Services* - *Cyber Resilience Security Advisory*	Select one service from below for a one-time engagement: - *Security Architecture Review and Zero Trust Advisory Workshop* *OR* - *Cyber Risk Assessment and Gap Analysis*
Days on-site	**Up to 20 days**	**Up to 3 days**	**1 day**
Delivery SLA	**----**	**2 weeks**	**1 week**

For pricing, please refer to the Check Point product catalog.
** https://www.checkpoint.com/services/infinity-global/*

FAQ

1. Can an ESA assist with non-Check Point related technologies?

Yes, the Check Point Enterprise Security Architecture team is an independent and vendor-agnostic team. The team focuses on defining cyber security in terms of risk and mapping business requirements to technology.

2. What are the lead times for all security architecture and assessment activities?

The official lead time for all security architecture and assessment engagements is up to 21 days. ***Pro*** and ***Plus*** clients have the flexibility of engaging in an activity on a need basis subject to an advance notice of 7 days being provided. ***Standard*** clients may experience longer wait times in case of limited availability of consultants or resources.

3. Does the Enterprise Security Architecture team provide low-level design documents?

No, the scope of all architectural discussions is limited to high-level design documents and reports only. The Check Point Professional Services team can provide low-level design documents at an additional cost.

4. How many *Pro, Plus and Standard* days will be used for each project?

Each project is scoped prior to its actual engagement. The estimated number of days is provided along with the agenda mutually agreed on between the architect and the client.

5. Can on-site/off-site days be exchanged?

Yes, the off-site (remote) days can be exchanged for on-site (face-to-face) days. However, a purchase order to cover the travel expenses is required. In case a purchase order for travel expenses cannot be supplied, additional days amounting to the travel expenses may be deducted.

6. Can the ESA days be interchanged with PS, Diamond and ATAM days offered by Check Point?

No, if ESA days are exhausted, additional ESA packages can be purchased. ESA days cannot be exchanged with PS, Diamond, or ATAM days. Please contact the local Enterprise Security Architect in your region for scoping.

LEARN MORE AND BOOK ENGAGEMENT

https://www.checkpoint.com/support-services/security-consulting/

