CHECK POINT™
SERVICES

Cyber Security Consulting and Risk Assessment Services

October 30, 2023
v3.11

Prepared by:
Strategic Consulting Group
Global_Architects@checkpoint.com

Overview

Strategic Consulting is an integral component of our comprehensive portfolio of services offered under the umbrella of Infinity Global Services (IGS). Within the realm of IGS, Strategic Consulting plays a pivotal role in assisting our clients in the formulation and execution of informed decisions that align with their organizational goals and support decision-makers, engineering, and architecture teams through a combination of assessment, advisory and architectural services designed to leverage industry-standard techniques and help improvements in overall cyber security posture.

The Strategic Consulting group is pleased to release the following service catalogue as a reference for all services for which the group is responsible. By using cyber security techniques such as control-based assessment, threat modelling, threat intelligence, standard risk management terminology, the cybersecurity conversation can be presented to the whole organization, thereby changing the cybersecurity conversation to have a broader and more impactful appeal.

Cybersecurity 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 that focus on risk management, cost efficiency, operational and technology architecture, and solution accountability and address cyber security risk management throughout the whole organization, not just the technology sphere. Some of the services offered are.

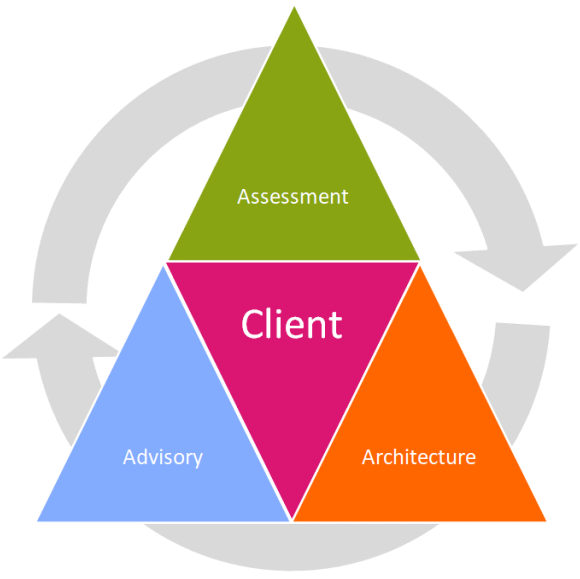
> *"The goal of strategic consulting is to perform advisory, assessment, and architectural work for, and on behalf, of our customers. We advise on all matters relating to cyber security, making assessments of the current security state and architecture to address gaps and improve overall posture."*

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 organisation understand its overall governance, cyber risk, and compliance posture and take the necessary steps to improve it.*

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

Architecture: *Architecture service focuses 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.*



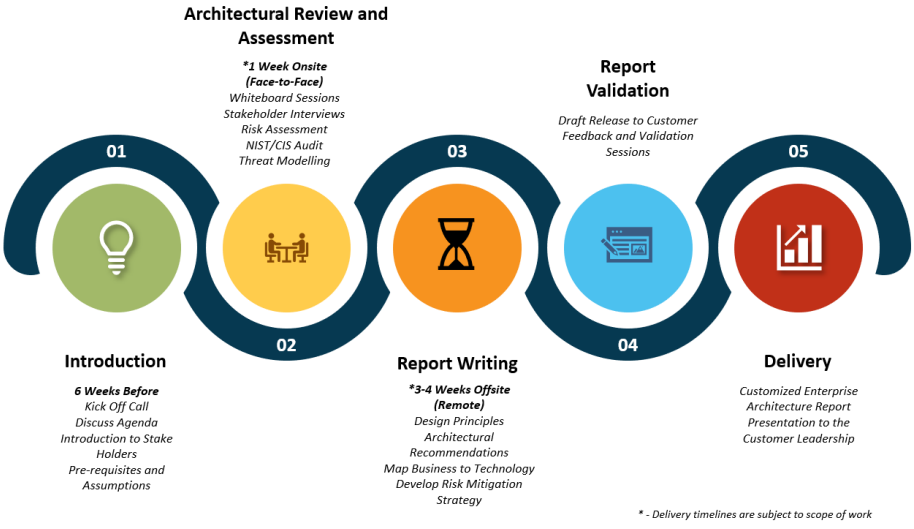
The following table provides a summary of the high-level services offered across the three pillars.

Assessment	Cyber Risk Assessment	Cloud Security Maturity Assessment	Zero Trust Maturity Assessment	OT/IoT Security Assessment
	Security Controls Gap Analysis (NIST/CIS)	NIS2 Readiness Assessment	Penetration Testing & Red Teaming Exercises	Threat Intelligence & Threat Modeling
Advisory	Zero Trust Advisory	Automation, PaaC, and DevSecOps Advisory	CISO Advisory	SOC Readiness and Transformation
Architecture	Security Architecture Review (DC/OT/Cloud)	Cyber Security Mesh Architecture Maturity Analysis	Zero Trust Design Modeling	SDN/SDDC Target Design

For more information on Cyber Security Consulting and Risk Assessment Services, please visit the below link.
https://www.checkpoint.com/services/infinity-global/
https://www.checkpoint.com/support-services/security-consulting/

Delivery Method

We believe that 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 these are the center of all our proposals and, wherever possible, include a series so that the consulting team can act as a trustworthy advisor in the capacity for which we are engaged; assessment workshops are interview and evidence-based, the *advisory* workshop is roundtable and open forum, *architecture* workshops are whiteboard and design focused. The timeline shows how a typical workshop activity is planned and executed.



Framework

The cornerstone of all our work is the ***Check Point Enterprise Security Framework.*** This proprietary model is used to evaluate and communicate the process that governs our top-down approach. The CESF model represents the various stages of enterprise security architecture; assess and collect data, review the applied architecture models, for example, "as-is" and "to-be", complete a design, deliver the design, and then provide the correct operations architecture to support it. We maintain that informed architectural, business-driven decisions are more cost-effective and provide sustainable, scalable security architecture and this goal is only reached through a methodical approach. Enterprise architecture would not be complete without addressing operational aspects, namely those people and process elements that are fundamental to any robust cyber security architecture.

The CESF framework was inspired and derived from the SABSA (Sherwood Applied Business Security Architecture) open framework and publicly accessible to all cybersecurity professionals. It enables organizations of all sizes and industries to envision a security architecture that evolves with the changing security landscape while embracing well-formulated processes. The framework consists of several layers, each focusing on a different domains and audience.

Layer	View	CESF	Process	Customer Representative
Context	*Business*	Assess	Business Goals, Security Assessment, Risk Analysis	Leadership – CIO/CISO/Directors
Concept	*Architect*	Architect	Gap Analysis, Zero Trust Maturity, Architecture and Controls Review	Security Architects
Logical & Physical	*Engineer*	Design	High-Level Design and Target Architecture	Lead Engineers and Design Teams
Component	*Builder*	Delivery	Low-Level Design and Configuration	Implementation Engineers
Management	*Operations*	Manage	Security Services	Operations and SOC Teams

For more information about the CESF framework, please refer to the below link:
https://resources.checkpoint.com/cyber-security-resources/check-point-enterprise-security-framework-version-2

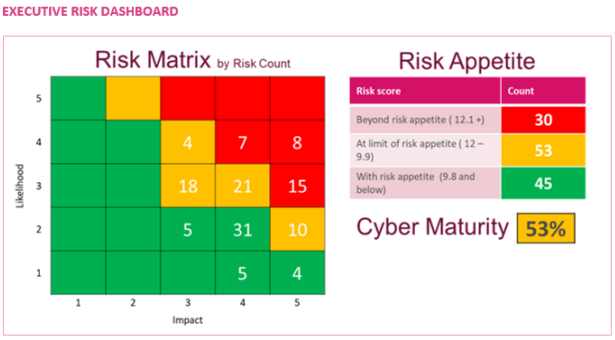
Services

Assessment: *The assessment concentrates on governance, cyber risk, and compliance, and its goal is to assist the organisation in comprehending its current governance, cyber risk, and compliance status and take the necessary actions to enhance it.*

- ***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.

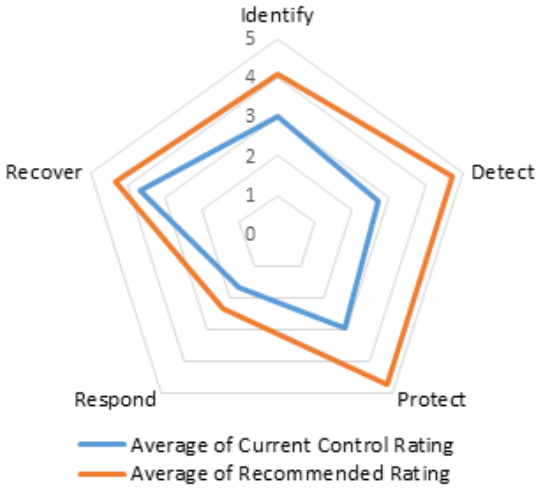
  Reducing risk using quantitative analysis is sometimes a challenge. However, for those responsible for minimizing the financial impact of cyber security events, it's a necessary calculation and a valuable tool in communicating risk. The standard risk calculation we use is based on the following formula:

  Risk (R) = Likelihood (L) x Impact (V)



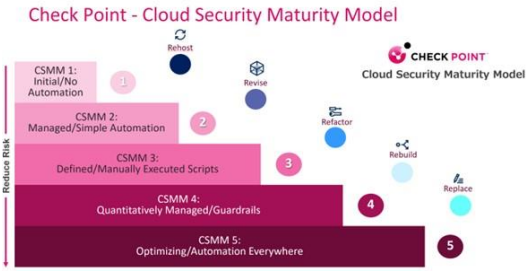
- ***Control-Based Assessment – NIST CSF, NIST 800-53, CIS Benchmarking, etc.***
  The key objective of this assessment is to evaluate cybersecurity posture against industry standard frameworks, such as the Cybersecurity Framework (NIST CSF) developed by the National Institute of Standards and Technology or 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.



- ***NIS2 Readiness Assessment***
  With a deep understanding of the Network and Information Systems Directive 2 (NIS2) and extensive experience in cybersecurity and compliance, we offer a NIS2 Readiness assessment to evaluate and enhance your compliance with NIS2 regulations. Our assessments include thorough examinations of your network and information systems, risk management practices, incident response procedures, and cross-border cooperation capabilities. We work closely with your team to identify vulnerabilities, develop mitigation strategies, and ensure that your organization meets NIS2 requirements.

- ***Cloud Security Maturity Assessment***
  Our team specializes in offering comprehensive Cloud Security Maturity Assessments, tailored to your organization's unique needs. We will thoroughly evaluate your cloud infrastructure, policies, and practices to provide a detailed analysis of your current security posture. Our assessment will identify vulnerabilities and areas for improvement, enabling you to make informed decisions to enhance your cloud security. With our expertise, you can confidently navigate the dynamic landscape of cloud security, ensuring that your data and operations remain protected and resilient.

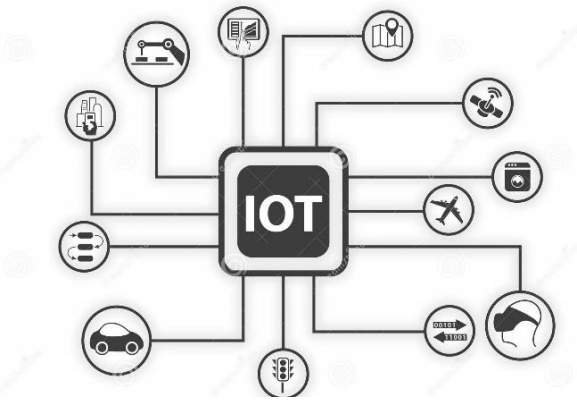


- ***Penetration Testing & Red Teaming Exercises***
  Our skilled and experienced team is proficient in penetration testing, a crucial element in ensuring the security of your digital assets. With a deep understanding of cybersecurity vulnerabilities and cutting-edge techniques, we can identify and address weaknesses in your systems, applications, and networks before malicious actors do. Our team's rigorous testing methods and ethical hacking expertise enable us to provide comprehensive assessments, helping you fortify your defenses and protect your sensitive data. Whether you're looking to safeguard your business from potential threats or meet compliance requirements, our penetration testing capabilities can help you stay one step ahead in the ever-evolving realm of cybersecurity.

- ***Threat Intelligence Services***
  Our team is equipped to deliver comprehensive threat intelligence services that offer a multi-faceted approach to safeguarding your organization. We provide a daily digest of reports culled from diverse sources, including open web and dark web, to keep you informed of emerging threats. Our advisories highlight major vulnerabilities, ensuring you stay ahead of potential risks. With a keen focus on areas of interest and the identification of new malware strains, we offer proactive protection measures. Additionally, we furnish you with Indicators of Compromise (IOCs) to fortify your security stance. For a personalized touch, our "analyst as a service" feature offers expert insights and support, tailored to your unique security requirements.

- ***Threat Modelling – STRIDE, PASTA, DREAD, etc.***
  Threat modelling is a proactive approach that aims to identify vulnerabilities and weaknesses. in systems, networks, or applications that attackers could exploit and take 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 organisation using techniques such as STRIDE, PASTA, etc., and assist in identifying vulnerabilities, prioritizing resources, improving security, complying with regulations, and reducing risk.

- ***OT/IoT Assessments***
  Our team excels in offering comprehensive OT/IoT assessments to secure your operational and Internet of Things (IoT) environments. With a deep understanding of industrial control systems and IoT devices, we conduct in-depth evaluations to identify vulnerabilities, assess network security, and review device configurations. We then provide strategic recommendations to fortify your systems against cyber threats, ensuring the resilience and safety of your critical infrastructure. Trust our expertise to safeguard your OT and IoT environments in an increasingly connected and digitized world.

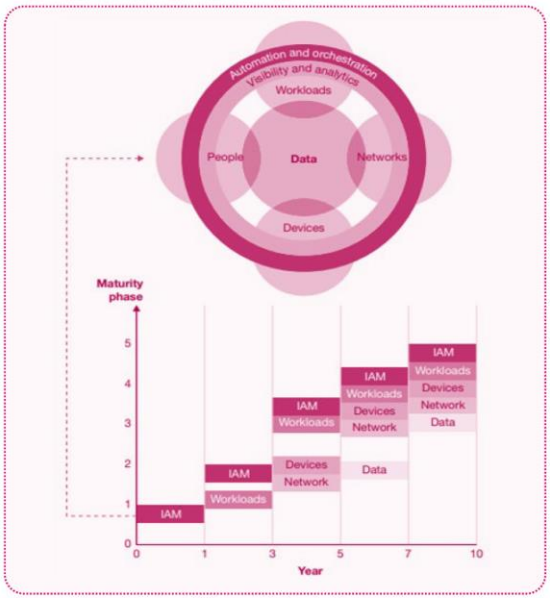


- ***Zero Trust Maturity Assessment***
  We perform a targeted Zero Trust maturity assessment to evaluate an organization's readiness to adopt and implement the Zero Trust framework. This assessment typically involves reviewing the organization's current security posture and identifying areas where design 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.

Advisory: *Our advisory service offers expert support and counsel to organizations on safeguarding their systems and data from cyber threats, emphasizing 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 can work with organizations to understand their specific needs and help you develop a plan for implementing the least privilege principle and increased visibility across their systems and data. During the workshop, we are going to perform Zero Trust maturity assessment and review the current state of the security design.

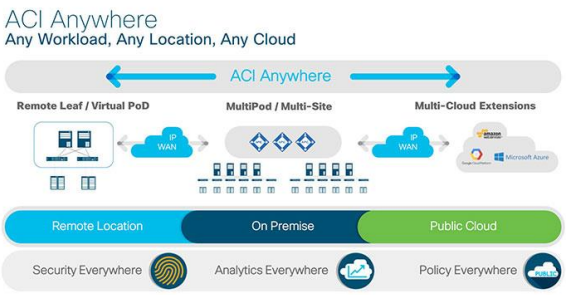
  This may include identifying users and devices that require access, determining what access they need, and implementing controls to ensure that access is granted and monitored appropriately. Additionally, we focus on increasing visibility, meaning that organizations need to have complete visibility into 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 a 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 4C's 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.

- ***SDN/SDDC Transformation***
  Our team is outfitted to assist with SDN/SDDC 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.



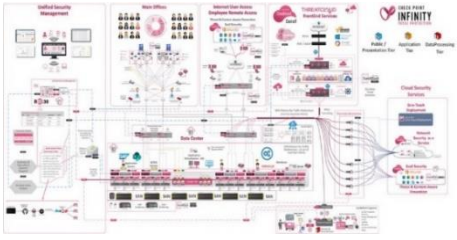
- ***Automation and Orchestration***
  Our team specializes in providing workshops in automation and orchestration using widely used automation tools such as Ansible, Python, Chef, etc. These workshops are designed to empower an organization with the knowledge and skills needed to reduce operational 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 your systems.

- ***CISO Advisory***
  Organizations can enlist the help of our CISO advisory service. Our seasoned architects, in collaboration with an experienced field CISO, can assist an organization's leadership in formulating a comprehensive, long-term strategic vision. This collaborative approach ensures that technology, security, and business objectives are seamlessly integrated into a cohesive plan. By leveraging their combined expertise, organizations can craft a resilient roadmap that not only anticipates emerging challenges but also harnesses opportunities for growth and innovation in the ever-evolving digital landscape.

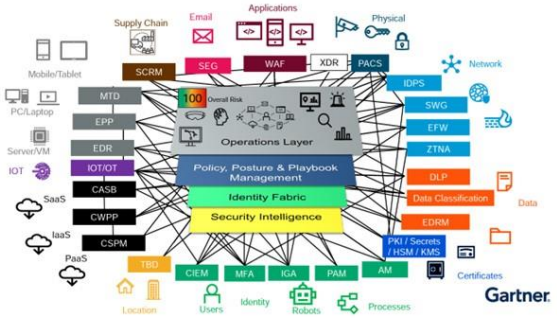
- ***Security Operations Transformation***
  Security Operations Transformation is the process of aligning an organization's security operations with its overall business strategy and objectives. It involves evaluating and improving the processes, systems, and capabilities that support security operations, 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.

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 security of the system and offer a suggested architecture based on industry best practices.*

- ***Security Design and Architecture Review***
  Our team specializes in security design and architecture can assist with reviewing and evaluating your current "as-is" architecture and provide 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 are effective in protecting your systems and data.



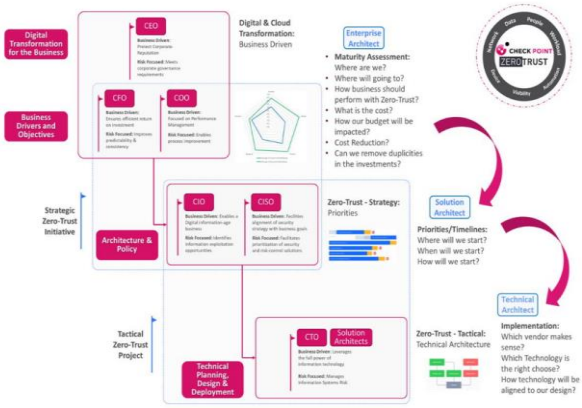
- ***Cyber Security Mesh Architecture (CSMA) Analysis***
  Our team is well-equipped to provide comprehensive architectural sessions on Cyber Security Mesh Architecture. We offer in-depth insights, expertise, and guidance to help organizations navigate the complexities of this cutting-edge security framework, ensuring a robust and adaptive approach to safeguarding their digital assets.



- ***Infinity Architecture Customization***
  The 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.

- ***Target Operating Model (TOM) Recommendations***
  Organizations often look for a blueprint to document how it intends to operate in the future and align their resources and capabilities with their strategy to ensure that all stakeholders are working towards a common vision. Our team can assist with the development of 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.

- ***Zero-Trust Design Modelling***
  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.



Service Model

The Strategic Consulting service functions as a retained service model, which remains valid for up to one year. It consists of five distinct service groups: ***Assessment, Architecture, Advisory, Red Teaming, and Threat Intelligence*** services. Each of these groups is thoughtfully designed to serve clients from various industries and verticals.

Services are meticulously scoped, and we provide clients with a transparent effort estimate, indicating the number of days required for each service. To ensure an accurate understanding of the time and effort required, as well as to establish a proper Statement of Work (SOW) and pricing, all activities begin with a scoping call led by an Enterprise Architect in collaboration with the client.

The following guidelines apply during the service selection and pricing process:

- The final commercial offer can be provided only after a scoping session with the Enterprise Architect who will determine the scope of work and apply relevant service SKU based on the overall scale, complexity, and effort in weeks to deliver the required services.

- We offer flexibility to bundle services together into packages, and these packages are offered as a single SKU, which is determined by the scope of work and aligns with the estimated effort. For instance, customers have the option to group Cyber Risk Assessment and Security Controls Gap Analysis into one package, identified as *CPTS-WORKSHOP-100* SKU. This option is available if the total effort required does not exceed two weeks. If the effort estimate exceeds, then the Enterprise Architect would suggest another appropriate SKU.
- If additional effort is required, the customer should opt for higher-tier SKUs or make use of Daily service SKUs.
- The matrix below presents service recommendations and the corresponding SKUs to consider. Nevertheless, it's important to keep in mind that the ultimate offer should be discussed and finalized with the experts.
- Services such as penetration testing, threat intelligence, and CISO advisory are offered as an add-on on top of the Assessment, Architecture and Advisory pillars. These services require a custom quote and can be provided by the Enterprise Architect.

The below table summarizes the service model and provides a high-level overview of the services that can be delivered under a particular SKU.

<table>
<tr><th>Group</th><th colspan="4">Service Offered</th><th colspan="3">Recommended Product Catalog SKU</th></tr>
<tr><td rowspan="2">Assessment</td><td>Cyber Risk Assessment</td><td>Cloud Security Maturity Assessment</td><td>Zero Trust Maturity Assessment</td><td></td><td rowspan="2">CPTS-WORKSHOP-100
(2 weeks)</td><td rowspan="2">CPTS-WORKSHOP-500
(3 weeks)</td><td rowspan="3">CPTS-WORKSHOP-1000
(4 weeks)</td></tr>
<tr><td>Security Controls Gap Analysis (NIST/CIS)</td><td>NIS2 Readiness Assessment</td><td>OT/IoT Security Assessment</td><td></td></tr>
<tr><td>Architecture</td><td>Security Architecture Review (DC/OT/Cloud)</td><td>Cyber Security Mesh Architecture Maturity</td><td>Zero Trust Design Modeling</td><td>SDN/SDDC Target Design</td><td>CPTS-WORKSHOP-100
(2 weeks)</td><td></td></tr>
<tr><td>Advisory</td><td>Zero Trust Advisory</td><td>Automation, PaaC, and DevSecOps Advisory</td><td>CISO Advisory</td><td>Enterprise Security Architect as a Service</td><td colspan="2">CPTS-3D-DAILY-WORKSHOP
(9 hours)</td></tr>
<tr><td rowspan="2">Red Teaming</td><td colspan="4">External Network Cyber Resilience Testing, up to 32 IP Addresses</td><td colspan="3">CPTS-PROF-PENTEST-INFRS-1Y</td></tr>
<tr><td colspan="4">Penetration Testing Daily SKU for Custom CRT Engagements</td><td colspan="3">CPTS-PRO-CRT-1Y</td></tr>
<tr><td rowspan="4">Threat intelligence</td><td colspan="4">Monthly Intelligence Reports - Subscription to a Tailored Monthly Report</td><td colspan="3">CPTS-CPR-REPORT-MONTHLY-1Y</td></tr>
<tr><td colspan="4">Daily OSINT Digest - Subscription to Daily OSINT Reports</td><td colspan="3">CPTS-CPR-OSINT-DAILY-1Y</td></tr>
<tr><td colspan="4">Indicators of Compromise (IoC) List- Weekly Report for One Country or Sector</td><td colspan="3">CPTS-CPR-IOC-LIST-1Y</td></tr>
<tr><td colspan="4">Analyst as a Service - hourly rate</td><td colspan="3">CPTS-CPR-ANALYST-Hour</td></tr>
</table>

For more details, please visit the below link so that one of our security experts can reach out to you.
https://www.checkpoint.com/services/infinity-global/contact-security-expert/

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 is the lead time on all Security Architecture and Assessment activities?

The official lead time for all security architecture and assessment engagements is up to 21 days.

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. Low-level design documents can be provided by the Check Point Professional Services team at an additional cost.

4. How many weeks will be used for each project?

Each project is scoped prior to its actual engagement. The estimate number of weeks are provided along with the agenda that was mutually agreed between the architect and the client.

5. Do the SKU's cover travel?

One-time round trip is covered under the ***CPTS-WORKSHOP-100/500/1000*** SKU's. The ***CPTS-3D-DAILY-WORKSHOP*** SKU requires a separate T&E SKU (***CPTS-3D-TE-WORKSHOP***) to be added if the engagement is on-site.

6. Can On-Site/Off-Site days be exchanged?

Yes, the Off-Site (Remote) days can be exchanged for On-Site (Face-to-Faces) days. However, a Purchase Order to cover the travel expenses is required. In case, a Purchase Order for travel expenses cannot be supported, additional days amounting to the travel expenses may be reduced.

7. 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.
