Cyber Security Architecture Assessment

With over three decades of unparalleled experience in cyberspace, Check Point brings a wealth of knowledge and expertise to the forefront. This extensive history allows us to excel in the realm of pure-play consultancy, offering unparalleled guidance and solutions to address your cybersecurity needs with confidence and precision. Check Point's Cyber Security architecture sessions are designed to support true vendor-agnostic discussion, planning, and conceptual design. Our dedicated design team acts as your independent technical design authority that follows industry standard processes, such as SABSA, and is a world-class cyber security architecture team ready to help you deliver on strategic cyber security goals.

Benefits

The security architecture assessment allows expert architects to discover and report on the health of the cyber security architecture, allowing a detailed evaluation of the "as-is" architecture. Based on this information, the team will develop a clear plan to achieve the desired "target" architecture.

- Assessment using an industry-recognized framework (CISv8) to establish a security baseline and GAP analysis
- Data gathering using questionnaires, interviews, and inspections (on-site).
- Audit the current security posture and document protective and detective technology.
- Focus on the target design for correct network segmentation driven by Zero Trust model
- Review and analyze the current architecture and capture the "to be" architecture.
- Identify and address immediate, mid-, and long-term security challenges.
- Make recommendations to improve security, decrease operational costs, and reduce gaps identified

The assessment output is designed to empower business leaders and deliver the following:

- **Align network security with industry best practices**, including segmentation and Software-define-Data Center architecture and modelling (e.g. Cisco ACI , VMWare NSX etc)
- **Provide documentation** that includes conceptual, contextual, physical, and logical design patterns.
- **Improve security** by ensuring appropriate security controls protect all critical assets.
- **Lower operational costs** and consolidate security controls into the Cyber Mesh Architecture

Methodology

Our Cyber Security architecture engagements align with two public bodies of work: the CIS v8 framework, selected for its practical and technical approach, and our own Check Point enterprise security framework (CESFv2), which provides our clients with an end-to-end practical approach to cyber security strategic planning and implementation.

We appreciate the importance of open-forum design conversations and the power of detailed white-boarding sessions, which is why, by default, all our design sessions are planned as face-to-face engagements. Based on our experience of 1000s of workshops, personal interactions often deliver the most effective and efficient results.

The process:

SCOPE	Plan and collect	Assessment	ANALSYIS	REPORT
NDA signed and controls aligned with relevant internal teams	Collect preliminary data, including attack surface scan data	Onsite interview and evidence gathering	Data gathering and interviews Whiteboarding and review.	Report delivery with findings analysis and remediation, including gap analysis and detailed recommendations.
4-6 weeks before	1 days	3 days	10 days	1 day

Delivery

- HLD Design Diagrams for "as-is" and "to-be" architecture
- Design documentation, including details of segmentation principles, data classification, service tiering, and data flow diagrams
- Plan of action and mitigation based on GAP analysis
- Adoption roadmap

Most relevant for

- Organizations that tackle complex architectural challenges
- Team augmentation for significant uplift projects
- Zero Trust or Digital Transformation initiatives
- Mergers and acquisitions

Contact Us

Schedule a consultation to discuss how we can fortify your cyber defenses.
https://www.checkpoint.com/services/infinity-global/contact-security-expert/