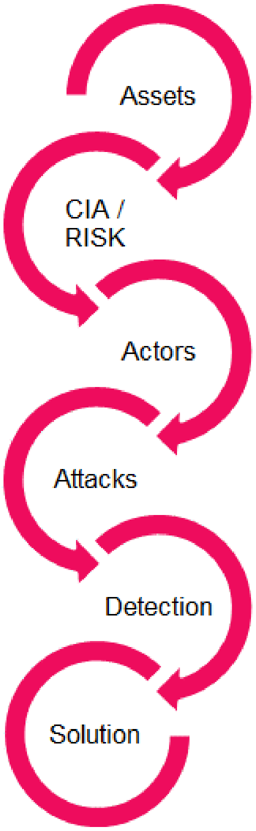
Ransomware Readiness Assessment

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 Ransomware Readiness Assessment is designed to assess how well your organization can protect itself from the risk of a successful ransomware attack, including the threats and vulnerabilities in your people, processes, and technology.

The outcome of this assessment will indicate what your risks are and what can be done to reduce them.



Ransomware readiness assessment benefits

The Check Point ransomware assessment is a true cross-functional assessment based on inputs from 3 distinct groups, each of which is uniquely positioned to add a specific data component to the overall assessment. By combining 3 different data models (threat intelligence, red teaming, and compliance), the assessment is able to focus on a practical and realistic analysis of current protective and detective measures, delivering real-world recommendations for real-world ransomware risk.

The core components of our unique assessment areas follow:

- An onsite **Ransomware Readiness Workshop** with Check Point Consultants, based on NISTR 8674 *"Ransomware Risk Management."*
- A customized **control-led assessment** based on the NIST CSF, NIST 800–53 and CISv8 IG3 control frameworks, led by the Check Point Operations team
- **Threat intelligence analysis** led by the Check Point Research Team on relevant (geographical or industry-specific) attachment groups and patterns to create realistic threat to.
- **External and Internal Attack Surface and Discovery scans** using best-of-breed penetration solutions
- **Threat modeling** of attack vectors based on combined data set following industry standard, methology

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

Threat Modelling

Assessment Team	Phase	Activity
Consultant	Assets	This is often referred to as the attack surface of your system. Identifying the users, data flows, and attack surfaces will allow you to identify potential risks and attacks on the system.
	CIA	To put it simply, the next step is to determine what could go wrong. What could happen that would impact the security of your system? The Confidentiality, Integrity & Availability (CIA) model can be useful here, providing a neat way to enumerate potential risks. Equally, you could also apply other approaches for categorizing threats or types of attack, e.g., the STRIDE model, for greater depth.
Research	Actor	Next, you should seek to understand the users or actors that might attempt to attack or maliciously affect your system.
Red Team	Attack	At this point, you can objectively explore each abstract risk. This is where the "how" of the attack is detailed. This can then be used to link a risk to a log source.
Red Team	Detection	Here, you identify and list any available log sources that could be used to indicate any attack that you have determined might occur within your system.
Consultant	Solution	Once competitive, you now need to align any gaps with a technology or service that mitigates the gap.

Deliverables

The delivery of our assessment includes a commitment by the consulting team to deliver the following artifacts and services.

1. The workshops will be conducted on-site as agreed upon between the Customer and Check Point.
2. Complete the NIST Assessment Report (Industry standard format).
3. Technology gap analysis
4. Failed control Register and recommendations to high-level design) technical depth. Where possible, the team will endeavor to provide a plan of action and milestones (POAM) that can be achieved using known or available resources.
5. C-level / Board room presentation delivered in person by the lead consultant
6. Access to the Check Point Assessment portal (valid for 1 year) to allow the client team access to all controls and analysis tools.

Most Relevant for

- Organizations seeking to understand their risk profile against ransomware risk
- Security Baseline and Capability Planning
- C-level are reporting
- Cyber Risk management

Contact Us

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