CROWDSTRIKE

Ransomware Defense Assessment

Assess your ability to prevent, detect and respond to a ransomware attack

Keeping pace with continuously evolving ransomware attacks

The eCrime threat landscape is continuously evolving, including the tactics and techniques leveraged by ransomware operators. Organizations are challenged to keep pace with the latest threats from these increasingly sophisticated adversaries.

The CrowdStrike Ransomware Defense Assessment evaluates how your organization's cybersecurity controls and capabilities compare to the latest attacker techniques and the evolving best practices to prevent, detect and respond to ransomware attacks. Ransomware is the top concern for many security teams, and this assessment is designed to ensure your defenses are optimized to address the threats.

Targeted technical and programmatic improvements to your security posture

The Ransomware Defense Assessment takes a two-pronged approach to evaluating your organization's ability to prevent, detect, respond to and recover from ransomware attacks. First, CrowdStrike collects and analyzes technical data from your environment to identify configurations or vulnerabilities that are commonly exploited by ransomware adversaries. Then, CrowdStrike experts conduct a series of workshops designed to allow them to understand your organization's existing processes and share their understanding of best practices.

CrowdStrike's incident response and intelligence teams have a front-row seat for monitoring shifts in the ransomware landscape. This assessment applies the team's knowledge to help your organization avoid the worst outcomes. The result is an industry-leading approach to identifying technical and programmatic enhancements to minimize your ransomware risk.

Assessment benefits

Assess holistically: Combine in-depth technical analysis with workshops focused on key functions of the security program

Identify risk: Highlight areas of greatest risk and build a business case for improvements

Gauge preparedness: Determine the current state of your ransomware preparedness and get guidance on achieving your desired future state

Game-plan your approach: Receive a prioritized plan to maximize security risk reduction by making impactful improvements

Key capabilities

The Ransomware Defense Assessment is a targeted evaluation of your organization's security posture against ransomware attacker tactics and techniques. Recommendations focus on improving your organization's capabilities in the areas of:

- Threat Intelligence
- Endpoint Security
- Network Security
- Identity Security
- Cybersecurity Incident Response (IR)
- Disaster Recovery and Business Continuity (DRBC)

The CrowdStrike Services team guides you through a detailed assessment that delivers:

- **Engaging workshops:** During interactive workshops, CrowdStrike experts gather information on your existing security program while sharing intelligence and best practices.
- **Technical analysis:** Using the CrowdStrike Falcon® platform and additional tools, CrowdStrike analyzes the environment for technical hygiene issues and vulnerabilities leveraged by ransomware attackers.
- **In-depth reporting:** You receive a detailed, tailored report including technical and programmatic findings from the workshops, technical analysis, documentation review and follow-up discussions. The report highlights the areas of greatest risk and will help build a business case for improvements.
- **Prioritized areas for improvement:** CrowdStrike provides a prioritized plan to maximize security risk reduction with impactful improvements.

Why choose CrowdStrike?

CrowdStrike has assisted countless organizations in strengthening cybersecurity programs to address the specific factors that matter in today's targeted threat landscape.

Expertise: Unrivaled expertise drawn from the CrowdStrike Intelligence team and from experiences performing IR and endpoint recovery for ransomware attacks

Depth of analysis: Detailed analysis of technical and programmatic findings with accurate and meaningful improvement plans and recommendations for enhancements

Methodology and approach: Interactive workshops that promote open dialogue to help you understand the current threat landscape and your organization's strengths and opportunities for improvement

About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Advisory Services, Technical Assessments, Product Support and Training that help you prepare to defend against advanced threats, respond to widespread attacks, enhance your cybersecurity practices and controls and operationalize your technology platform.

We help our customers assess and enhance their cybersecurity posture, implement technologies, test defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike® Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike:

We stop breaches.

If you would like to participate in the CrowdStrike Ransomware Defense Assessment, please send an email to **services@crowdstrike.com**.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com