CROWDSTRIKE

White Paper

CrowdStrike NIS2 Compliance Package

How CrowdStrike Can Help Businesses Comply with the Network and Information Systems (NIS2) Directive

Table of Contents

This mapping cannot be considered as legal advice, nor is it intended to be such. CrowdStrike cannot provide legal advice with respect to compliance with the NIS2 Directive; in particular with respect to the applicability, scope, requirements and potential sanctions resulting out of the NIS2 Directive, and what measures should be implemented under the NIS2 Directive. All CrowdStrike Customers are therefore advised to consult with their own competent legal professional to make their own legal determination and ensure compliance with the NIS2 Directive implementation in the respective jurisdiction the Customer is located in.

The European Union (EU) has implemented several cybersecurity regulations and directives aimed at enhancing the security of networks, information systems and data across member states. The first piece of EU-wide legislation on cybersecurity, the **Network and Information Systems (NIS) Directive**, aimed at boosting the overall level of cybersecurity across the EU. It required operators of essential services and digital service providers to take appropriate security measures and notify relevant national authorities about serious incidents. **The NIS2 Directive** is an update of the NIS Directive that broadens its scope and includes stricter supervisory measures, stricter enforcement requirements and higher sanctions. It also covers more sectors and types of entities. NIS2 aims to ensure a high common level of cybersecurity across these vital sectors in the EU.

With the NIS2 Directive, the EU has continued a long tradition of enhancing the security of networks, information systems and data through legislation, which also includes the **General Data Protection Regulation (GDPR)**. Although primarily focused on data protection, the GDPR has significant cybersecurity implications. It mandates organizations to implement appropriate technical and organizational measures to ensure a high level of security appropriate to the risk. This includes protecting data against unauthorized or unlawful processing and against accidental loss, destruction or damage. Through its measures, the GDPR significantly contributes to enhancing cybersecurity by ensuring that data protection is a central consideration for organizations handling personal data within the EU and beyond.

The EU's motivation for this regulation is outlined in the EU Cybersecurity Strategy. Cybersecurity is a key enabler for many critical sectors to successfully embrace digital transformation and fully grasp the economic, social and sustainable benefits of digitalization. The digital transformation of society, intensified by the COVID-19 crisis, has expanded the cyber threat landscape and is bringing about new challenges that require adapted and innovative cybersecurity measures from the public and private sectors. Although CrowdStrike cannot provide legal advice to its customers, this document will help customers learn and understand how CrowdStrike can support them in addressing key aspects of NIS2.

NIS2

The NIS2 Directive is in effect as of October 17, 2024. However, it's important to keep in mind that because NIS2 is a directive, it must be transposed into law in all EU member states. Some EU member states may include additional aspects only applicable to entities in the scope of their particular national laws.

In general, NIS2 represents a significant strengthening of the EU's cybersecurity posture, ensuring that both the public and private sectors are better equipped to handle the evolving landscape of cyber threats. It broadens the scope of entities covered compared to its predecessor and encompasses a wider range of sectors.

Determining Whether You Fall Within the Scope of the NIS2 Directive

Several factors determine whether you must comply with NIS2 requirements. By following the steps outlined below, you can assess whether your organization is subject to the NIS2 Directive and identify the actions required to comply with its provisions. For further assistance or specific details regarding the implementation of the NIS2 Directive in your country, CrowdStrike recommends consulting the appropriate national supervisory authorities or seeking legal advice from qualified professional advisors.[1]

Step 1: Identify Your Sector

First, check whether your organization falls under one of the sectors explicitly covered by NIS2.

Essential Entities Essential entities play a crucial role in maintaining critical societal or economic activities, and disruptions of their services could have a significant impact.	**Energy:** Electricity, oil and gas suppliers
	Transport: Air, rail, water and road transport providers
	Banking: Credit institutions
	Financial Market Infrastructure: Trading venues, central counterparties
	Health: Healthcare providers, such as hospitals
	Drinking Water: Water supply and distribution
	Wastewater: Entities involved in wastewater management
	Digital Infrastructure: Internet exchange points, domain name system service providers, top-level domain name registries
	Public Administration: Government and public service entities
	Space: Entities involved in the space sector
Important Entities Important entities are important for the economy or for society.	**Postal and Courier Services:** Services (including dispatch, transport and delivery of mail and packages) essential for communications and commerce, facilitating the movement of goods and information both domestically and internationally
	Waste Management: Range of services and operations that manage waste from its inception to its final disposal
	Manufacture, Production and Distribution of Chemicals: Creation and supply of chemical substances used across various industries, including pharmaceuticals, agriculture, manufacturing and consumer products
	Food Production, Processing and Distribution: Sector spans from the initial production of raw agricultural products to the processing and manufacturing of food items, and finally to their distribution and retail
	Manufacturing of Electronics, Computers and Optical Products: Sector spans a wide range of activities, from the creation of semiconductors to the assembly of consumer and industrial electronics and optical devices
	Digital Providers: Online marketplaces, online search engines and cloud computing services

[1] For Germany, the Federal Office for Information Security (BSI) has published an assessment tool at https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html.

Step 2: Evaluate Your Entity Size

If your organization falls under one of the sectors above, it's crucial to evaluate its size. This step will help determine your compliance obligations under NIS2, the specific requirements that apply to your organization and the mandatory measures you must implement.

Though **small entities** are generally exempt unless (i) a member state has opted to include them based on national security or other significant reasons or (ii) the total number of employees across the group exceeds the thresholds set for medium-sized and large enterprises, the NIS2 Directive removes previous exemptions for medium-sized enterprises, mandating that all medium-sized and large companies within the designated sectors must comply with the NIS2 Directive. This applies regardless of their specific impact or risk assessment, provided they meet or exceed the established thresholds for medium-sized enterprises. This **Size Cap Rule** will help ensure a robust cybersecurity posture across a larger segment of the internal market, addressing the reality that size does not always reflect the potential risk or impact of cybersecurity incidents on society and the economy.

Medium-Sized Entities

Pursuant to the EU Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EG), a medium-sized entity is defined as an enterprise with at least **50 employees** and an annual turnover or balance sheet exceeding **EUR 10 million** (Article 2).

Large Entities

Pursuant to the EU Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EG), a large entity is defined as an enterprise with at least **250 employees**, an annual turnover exceeding **EUR 50 million**, and/or an annual balance sheet total exceeding **EUR 43 million.**

Group of Companies

For a group of companies, if the total number of employees, the annual turnover or the balance sheet exceeds the thresholds set for medium-sized and large enterprises, then the entire group — including its smaller entities — may fall under the scope of NIS2. This is particularly relevant if a smaller entity handles critical functions or data that could impact the group's overall cybersecurity resilience.

Whether or not your organization falls within the scope of the NIS2 Directive, adopting the measures outlined in NIS2 is advisable for entities of all sizes in both the public and private sectors. These guidelines provide a reasonable baseline for improving cybersecurity and enhancing cyber resilience.

Requirements of the NIS2 Directive

The following NIS2 security requirements are designed to ensure that the organizations covered take a proactive and comprehensive approach to managing cybersecurity risks.

- ☐ **Risk Assessment and Mitigation:** Organizations are required to conduct thorough risk assessments to identify potential cybersecurity threats and vulnerabilities in their information systems and data infrastructures. This should cover both digital infrastructure and physical security. Based on these assessments, organizations must implement appropriate security measures to mitigate identified risks.

- ☐ **Technical and Organizational Measures:** The NIS2 Directive emphasizes the importance of adopting both technical and organizational measures to safeguard network and information systems. Tailored to the outcomes of your risk assessment, technical and organizational measures can include:

  - ☐ **System security:** Use firewalls, encryption, intrusion detection systems and secure software development practices.

  - ☐ **Data protection:** Ensure data integrity and confidentiality with robust data management policies and backup systems.

  - ☐ **Access control:** Limit access to sensitive information and systems to authorized personnel only.

  - ☐ **Policies and procedures:** Develop and maintain comprehensive security policies and procedures that are regularly updated.

  - ☐ **Incident response and recovery plan:** Establish an incident response plan that includes procedures for responding to and recovering from cybersecurity incidents. These plans should enable the timely detection, identification and management of cybersecurity incidents.

  - ☐ **Training and awareness:** Regularly train employees on cybersecurity best practices and raise awareness about potential cyber threats.

- ☐ **Supply Chain Security:** NIS2 extends security requirements to cover the relationships organizations have with their suppliers and service providers. Organizations must assess and manage the cybersecurity risks associated with their supply chain by ensuring that suppliers and service providers comply with appropriate cybersecurity standards, especially if they handle sensitive or critical data.

- ☐ **Audits and Assessments:** Organizations are expected to regularly test, audit and update their security policies and measures. This includes conducting regular security audits, vulnerability assessments and reviews of security policies.

- ☐ **Reporting:** The NIS2 Directive includes stricter and more specific requirements for reporting cybersecurity incidents. Companies must report significant incidents to the relevant national authorities within **24 hours** of becoming aware of the incident **(early warning)**, with more detailed information to follow after **three days (incident notification)** and **one month (final report)**.

- ☐ **Accountability and Training:** Organizations must maintain detailed documentation of all cybersecurity policies, risk assessments, incidents and compliance efforts. This documentation will be crucial for demonstrating compliance during audits or inspections from regulatory authorities. In addition, the NIS2 Directive requires entities to engage with cybersecurity and legal experts to ensure their measures align with legal requirements and best practices. This can help entities navigate complex regulatory landscapes and implement effective cybersecurity strategies. Organizations must also have senior management accountable for cybersecurity, ensuring that it is integrated into the corporate governance structure. The NIS2 Directive also emphasizes the need for regular training and awareness campaigns for all employees.

NIS2 Journey with CrowdStrike

CrowdStrike's offerings can help organizations comply with important elements of the NIS2 Directive, especially with Article 20 (Governance), Article 21 (Cybersecurity risk-management measures) and Article 23 (Reporting obligations). CrowdStrike's offerings can support organizations with the following:

□ **Risk Assessments:** CrowdStrike helps organizations identify potential cybersecurity threats and vulnerabilities in their information systems and data infrastructures by providing tools and services designed to proactively manage and mitigate cybersecurity risks. In particular, the **CrowdStrike Counter Adversary Operations team** delivers comprehensive threat intelligence services and detailed analyses of the tactics, techniques and procedures (TTPs) used by threat actors. This team also provides context-rich intelligence reports, deep and dark web monitoring, and indicators of compromise (IOCs), helping organizations understand the broader threat landscape and anticipate potential attacks. In addition, through **CrowdStrike Falcon® Exposure Management**, CrowdStrike delivers vulnerability management technology that enables organizations to discover and prioritize vulnerabilities in real time without impacting system performance. This module helps identify potential attack paths and weaknesses that attackers can exploit, aiding in proactive risk management and remediation efforts. With the increasing adoption of cloud services, CrowdStrike also provides specific tools for cloud security — such as cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), data security posture management (DSPM), cloud workload protection (CWP) and application security posture management (ASPM) — through its modules. CrowdStrike's CSPM offering monitors cloud-native applications and infrastructure to detect misconfigurations, compliance violations and malicious activity, thus safeguarding cloud environments.

□ **System Security:** The **CrowdStrike Falcon® platform** is specifically designed to provide holistic security, utilizing innovative technologies to offer security that adapts to ever-evolving risks. These technologies include artificial intelligence, advanced machine learning (ML), a cloud-native and cloud-delivered architecture, and a graph database capable of handling and analyzing trillions of events per day. The Falcon platform offers deep analytics for this enriched telemetry to automatically prevent known attack methods and intrusions. It also identifies new and unknown malicious activity and delivers proactive measures to stop attacks before they are executed. Machine learning and artificial intelligence detect known and unknown malware and ransomware, and behavior-based indicators of attack (IOAs) prevent sophisticated fileless and malware-free attacks. Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities. Threat intelligence prevention blocks activities known to be malicious. Together, these capabilities provide the speed and scale necessary to power the Falcon platform and offer state-of-the-art prevention[1] and high levels of protection with a simple, lightweight and immediately operational solution. The Falcon platform is designed to stop breaches from happening in the first place and maintain the integrity and confidentiality of data. Moreover, the Falcon platform offers enterprise-wide insight into the security events affecting endpoints, virtual machines and cloud environments to enable accountability for data protection. For further information on the Falcon platform and the modules available, see **Appendix I**.

□ **Data Protection:** The **CrowdStrike Falcon® Data Protection** module can help organizations manage and protect data. This module is designed to understand data flows and safeguard sensitive information, aiming to ensure that organizations have robust measures in place to prevent, detect and respond to data-related security incidents. It includes data loss prevention capabilities that help prevent unauthorized access to and disclosure of sensitive data. By monitoring data usage and movement both within the organization and in transit, Falcon Data Protection can help ensure that only authorized personnel have access to critical information, in line with NIS2's requirements for access control and data confidentiality.

[1] For reference, view the IT Security Association Germany's (TeleTrusT's) and the European Union Agency for Cybersecurity's (ENISA's) guidelines on state-of-the-art technical and organizational measures under the German IT Security Act and the GDPR: https://www.teletrust.de/fileadmin/user_upload/2021-09_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf.

□ **Incident Response and Recovery Planning:** CrowdStrike can aid in incident response and recovery planning through various tools and services that help establish robust incident response plans, focusing on the procedures necessary for responding to and recovering from cybersecurity incidents. The Falcon platform provides endpoint detection and response (EDR) capabilities that are fundamental to any incident response plan. This technology allows for the continuous monitoring of endpoints, early detection of malicious activity and automatic responses to identified threats. The platform can pinpoint the source and scope of an attack, providing crucial data that helps in the quick containment and remediation of incidents. In addition, CrowdStrike offers professional incident response services that can be engaged in the event of a significant security incident. CrowdStrike's team of experts can provide emergency response support, helping to manage the incident effectively. This includes performing forensic analysis to understand the attack vectors, affected systems and data compromised as well as developing a recovery strategy that minimizes downtime and operational impact. After an incident, CrowdStrike also assists with recovery and remediation efforts to restore operations and prevent future attacks. This includes guidance on system restoration, data recovery and strengthening security posture to resist similar threats.

□ **Supply Chain Security:** CrowdStrike offers various tools and services that can help organizations assess and manage cybersecurity risks within their supply chain. The **CrowdStrike Falcon® Cloud Security** module is designed to monitor cloud environments continuously. It assesses the security posture of cloud deployments, including those used by suppliers and service providers. This helps identify and remediate potential vulnerabilities or misconfigurations that could expose the organization to risks. Additionally, the external attack surface management capabilities of **CrowdStrike® Falcon Surface℠** identify and evaluate the risks posed by the external-facing assets of suppliers. This helps organizations understand how attackers might target the supply chain and enables proactive security measures and monitoring of the external attack surface, which is critical in supply chain security. CrowdStrike also offers cybersecurity assessment and consultation services to evaluate the security practices of suppliers and develop strategies for mitigating risks. These assessments can help ensure that suppliers adhere to agreed-upon security standards and practices.

□ **Audits, Assessments and Training:** CrowdStrike delivers technical assessments, training and advisory services that help customers defend themselves against advanced threats, respond to widespread attacks and enhance their cybersecurity practices and controls. CrowdStrike also helps customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations and recover from a breach with speed and precision. Additionally, CrowdStrike offers tools and services for simulation and training, such as tabletop exercises and red team exercises. These activities help organizations test their incident response plans in simulated environments, identifying gaps and areas for improvement. This training ensures that all team members understand their roles during an incident and can act quickly and effectively. You can find more information about CrowdStrike Professional Services in **Appendix II**.

□ **Accountability:** CrowdStrike can help with accountability by providing customers with detailed documentation of risk assessments and incidents.

Measures	CrowdStrike Solution	Technology	Service
Polices on Risk Analysis and Information System Security	Falcon Exposure Management – Asset Management | Vulnerability Management | EASM | Security Posture	✓	
	Falcon Cloud Security – CSPM | CIEM | ASPM	✓	
	Falcon for XIoT/OT – Falcon Discover for IoT and Falcon Insight for IoT	✓	
	Falcon Threat Intelligence – Digital Risk Protection | Intel Reports | RFIs | Access to Analysis	✓	✓
	Falcon Identity Threat Detection and Response | FREE Active Directory Risk Review	✓	FREE
	Security Program in Depth | Maturity Assessment | Security Enhancement Program | SOC Assessment		✓
	Technical Risk Assessment | Cloud Security Assessment | Identity Security Assessment		✓
Incident Handling	Falcon Complete – MDR | MXDR | Managed Identity Protection | Managed Cloud Security	✓	✓
	Falcon Adversary OverWatch – Managed Threat Hunting		✓
	Incident Response (DFIR)		✓
	Compromise Assessments		✓
	Tabletop Exercise | Adversary Emulation		✓
Business Continuity	Enpoint Recovery Service		✓
	Tabletop Exercise		✓
Supply Chain Security	Falcon Threat Intelligence – Falcon Recon | Falcon Adversary Intelligence Premium	✓	
	Falcon Exposure Management – Asset Management | Vulnerability Management | EASM | Security Posture	✓	
	Falcon for XIoT/OT – Falcon Discover for IoT and Falcon Insight for IoT	✓	
	Falcon Device Control | Falcon Firewall Management	✓	
Security in Network and Information Systems	Falcon AI-native XDR Platform | Falcon LogScale | Falcon Next-Gen SIEM | Data Protection | IT Automation	✓	✓
	Falcon Exposure Management - Asset Management | Vulnerability Management | EASM | Security Posture	✓	
	Falcon Cloud Security – CSPM | CIEM | ASPM | CWP	✓	
	Falcon for XIoT/OT – Falcon Discover for IoT and Falcon Insight for IoT	✓	
	Falcon Device Control | Falcon Firewall Management	✓	

Measures	CrowdStrike Solution	Technology	Service
Policies and Procedures to Assess the Effectiveness of Cybersecurity Risk Management Measures	AI-Native Falcon Cybersecurity Platform | Falcon LogScale | Falcon Next-Gen SIEM	✓	✓
	Falcon Exposure Management – Asset Management | Vulnerability Management | EASM | Security Posture	✓	
	Falcon for XIoT/OT – Falcon Discover for IoT and Falcon Insight for IoT	✓	
	Falcon Cloud Security – CSPM | CIEM | ASPM | CWP	✓	
	Tabletop Exercise | Adversary Emulation Exercise | Red Team / Blue Team Exercise | Penetration Testing		✓
	Technical Risk Assessment | Cloud Security Assessment | Identity Security Assessment		✓
Basic Cyber Hygiene	Falcon Identity Threat Protection and Prevention	✓	
	Falcon Exposure Management – Asset Management | Vulnerability Management | EASM | Security Posture	✓	
	Falcon for IT – IT Automation (and Patch Management)	✓	
	Falcon Data Protection	✓	
Policies and Procedures Regarding the Use of Cryptography and, Where Appropriate, Encryption	Falcon Discover	✓	
	Falcon Surface	✓	
	Penetration Test		✓
Human Resource Security, Access Control Policies and Asset Management	Falcon Threat Intelligence – Falcon Recon | Falcon Adversary Intelligence Premium	✓	
	Falcon Exposure Management – Asset Management | Vulnerability Management | EASM | Security Posture	✓	
	Falcon Identity Threat Detection and Prevention	✓	
	Falcon Complete – Managed XDR | Managed Identity Protection	✓	✓
The Use of Multifactor Authentication or Continous Authentication Solutions	Falcon Complete – Managed XDR | Managed Identity Protection | Managed Cloud Security	✓	✓
	Falcon Identity Threat Detection and Prevention | Zero Trust	✓	
	Identity Security Assessment		✓

People, Processes and Technology

Despite all of the support CrowdStrike can provide to its customers, compliance with the NIS2 Directive involves a comprehensive approach that encompasses people, processes and technology. Each of these components plays a critical role in establishing a robust cybersecurity framework that meets the directive's stringent requirements. A successful NIS2 compliance strategy requires integrating the right people, processes and technology into a cohesive framework. This integration should be guided by a clear understanding of the directive's requirements, the organization’s specific risk landscape and the overall cybersecurity strategy.

People
Technology
Processes

Entities cannot outsource risk management or governance

Appendix I — The CrowdStrike Falcon Platform

The Falcon platform enables enterprises to identify unknown malware, detect zero-day threats, pinpoint advanced adversaries and attribution, and prevent damage from targeted attacks in real time. Using big data technologies, CrowdStrike's cloud-based next-generation threat protection platform leverages execution profiling and predictive security analytics instead of focusing on malware signatures, IOCs, exploits and vulnerabilities. The core of the Falcon platform is a global network of endpoint-based agents (**Falcon agent**) driven by state-of-the-art cyber threat intelligence to provide real-time detection, identity protection and threat prevention capabilities to governments and organizations of all sizes worldwide. By storing and analyzing threat event data in a scalable, elastic cloud, the Falcon platform enables organizations to pinpoint attackers and their tradecraft in real time, allowing them to prevent destructive attacks and the loss of personal data and intellectual property.

The Falcon platform does the following:

- Detects zero-day threats and prevents damage from targeted attacks in real time
- Identifies unknown malware and adversary-in-motion lateral movement activities and provides damage assessments and attacker attributions
- Provides a flexible range of responses to raise the cost and risk to the adversary
- Leverages a cloud-based platform and a global network of event-driven security agents
- Powers additional first- and third-party security modules available in the CrowdStrike Marketplace

The AI-native CrowdStrike Falcon platform leverages real-time IOAs, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the organization to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Instead of focusing on malware signatures, indicators of compromise, exploits and vulnerabilities, the Falcon platform identifies the mission objectives of adversaries by leveraging the kill chain model, which is mapped to the MITRE ATT&CK® framework.

Utilizing the Falcon agent, the Falcon platform empowers enterprises with the power and knowledge to answer the following security questions:

- What suspicious programs have been executed?
- What suspicious processes have run across my systems with different file names?
- Which programs are surreptitiously listening for network connections?
- Which machines and users were affected by an intrusion?
- What were the attackers attempting to accomplish?
- What malicious programs are attempting to maintain persistence?
- What sensitive data is leaving the endpoint?

Through the single, lightweight Falcon agent, the CrowdStrike Falcon platform provides a wide range of cloud-based security offerings, including CrowdStrike® Falcon Prevent™ next-generation antivirus (NGAV), CrowdStrike Falcon® Insight XDR (unified EDR/XDR), CrowdStrike Falcon® Adversary OverWatch threat hunting, CrowdStrike Falcon® Adversary Intelligence, CrowdStrike Falcon® Discover IT hygiene, CrowdStrike Falcon® Spotlight vulnerability management, CrowdStrike Falcon® Data Protection and CrowdStrike Falcon® Device Control to detect unauthorized use of portable storage devices.

	Falcon Pro *Replace legacy AV with market-leading NGAV and integrated threat intelligence and immediate response*	**Falcon Enterprise** *Unified NGAV, EDR, XDR, managed threat hunting, and integrated threat intelligence*	**Falcon Elite** *Full endpoint and identity protection with threat hunting and expanded visibility*	**Falcon Complete** *Fully managed 24/7 protection for endpoints, cloud workloads, and identities*
Falcon Prevent Next-Generation Antivirus	✓	✓	✓	Managed Detection and Response, delivered by CrowdStrike's team of experts, backed with the industry's strongest Breach Prevention Warranty
Falcon Adversary Intelligence Threat Intelligence	+	+	+	
Falcon Device Control USB Device Control	+	+	+	
Falcon Firewall Management Host Firewall Control	+	+	+	
Falcon Insight XDR Detection and Response for Endpoint and Beyond		✓	✓	
Falcon Adversary OverWatch Threat Hunting		+	+	
Falcon Discover IT Hygiene			✓	
Falcon Identity Protection Integrated Identity Security			✓	
CrowdStrike Services Incident Response and Proactive Services	Optional	Optional	Optional	

Flexible bundles: ✓*Included Component* +*Elective Component*

Appendix II — CrowdStrike Professional Services

CrowdStrike Professional Services teams deliver incident response, technical assessments, training and advisory services that help customers defend themselves against advanced threats, respond to widespread attacks and enhance their cybersecurity practices and controls. CrowdStrike also helps customers assess and enhance their cybersecurity posture, test their 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, CrowdStrike Professional Services helps customers protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks.

The following CrowdStrike Professional Services offerings can help support customers:

Endpoint Security Services

Cloud Security Services

Identity Protection Services

Network Monitoring Services

Advisory Services

Prepare

for Advanced Attacks

Tabletop Exercise

Adversary Emulation Exercise

Red Team/Blue Team Exercise

Penetration Testing

Breach Services

Respond

to Widespread Breaches

Incident Response (DFIR)

Endpoint Recovery

Compromise Assessment

Adversary Exposure Assessment

Network Detection Services

Advisory Services

Fortify

Your Cybersecurity Practices and Controls

Technical Risk Assessment

Cybersecurity Maturity Assessment

SOC Assessment

AD Security Assessment

Cybersecurity Enhancement Program

Security Program in Depth

Plus: Services Retainer, Falcon Gold Standard, Falcon Operational Support, Falcon Training and Certificate (CrowdStrike University)

Prepare	Respond	Fortify
Advisory Services	**Breach Services**	**Advisory Services**
Prepare for Advanced Threats	**Respond to Widespread Attacks**	**Fortify Your Cybersecurity Posture**
We help you prepare and train to defend your organization against sophisticated threat actors.	We help you respond to attacks and recover from widespread incidents with speed and precision.	We provide actionable recommendations to fortify your cybersecurity practices and controls.
Prevent Breaches from Disrupting Your Business	**Recover from a Breach with Speed and Precision**	**Reduce the Risk of a Cybersecurity Breach**
• Tabletop Exercise • Adversary Emulation Exercise • Red Team/Blue Team Exercise • Penetration Testing Services	• Incident Response (DFIR) • Compromise Assessment • Endpoint Recovery • Network Security Monitoring	• Cybersecurity Maturity Assessment • Technical Risk Assessment • SOC Assessment • AD Security Assessment • Security Program in Depth • Cybersecurity Enhancement Program

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/