CROWDSTRIKE

FALCON INTELLIGENCE

IN RESPONSE TO:

G-Cloud 15 Framework (Lots 1-3)

Service Description

150 206 E. 9th Street, Suite 1400, Austin, Texas 78701
TEL: (888)512-8906 | FAX:(949) 417-1289
www.crowdstrike.com

DOCUMENT CONTROL

Date	01/2026

CROWDSTRIKE CONTACT

Account Manager	Peter Carthew Regional Sales Director ukpublicsector@crowdstrike.com

LEGAL DISCLAIMER

CrowdStrike's solution, pricing and offer to provide services and products in this response is expressly conditioned on: (i) CrowdStrike's current understanding of the scope of the project based on the information in the RFI, RFP, RFQ, Security Questionnaires and otherwise available and provided to CrowdStrike; and (ii) the parties negotiating mutually agreeable final terms and conditions upon award.

The information contained in this Response marked "confidential" is considered by CrowdStrike to be proprietary and confidential to CrowdStrike. The information contained in this Response may be used solely in connection with the evaluation of the Response. To the extent that a claim is made under applicable law to disclose confidential information contained in this Response, CrowdStrike reserves the right to defend its confidential information against such claim. Subject to applicable law, you agree (a) to keep the information contained in this Response in strict confidence and not to disclose it to any third party without CrowdStrike's prior written consent and (b) your internal disclosure of the information contained in this Response shall be only to those employees, contractors or agents having a need to know such information in connection with the evaluation of the Response and only insofar as such persons are bound by a nondisclosure agreement consistent with the foregoing. You do not acquire any intellectual property rights in CrowdStrike's property under the Response and you agree to comply with all applicable export control laws and regulations to ensure that no confidential information is used or exported in violation of such laws and regulations. You may make a reasonable number of copies of this Response for your internal distribution for use solely in connection with the evaluation of the Response; otherwise, you may not reproduce or transmit any part of this Response in any form or by any means without the express written consent of CrowdStrike. By reading the Response, you have agreed to be bound by the foregoing terms

INTRODUCTION

COMPANY OVERVIEW

CrowdStrike is a leader in cloud-delivered, next-generation endpoint and cloud workload protection. CrowdStrike has revolutionized endpoint and workload protection by being the first company to unify NGAV, EDR and a 24/7 managed threat hunting service — all delivered through a single lightweight, intelligent agent. CrowdStrike is the pioneer of the first security cloud, which provides comprehensive visibility and protection at scale for every endpoint and workload. Powered by the proprietary CrowdStrike Threat Graph, the CrowdStrike Security Cloud within the Falcon platform regularly correlates trillions of endpoint-related events per week in real time across the globe.

The CrowdStrike Falcon platform provides robust threat prevention, leveraging AI and ML with advanced detection and response and integrated threat intelligence to protect against the modern threat landscape. The Falcon platform offers the following:

- Complete protection from malware and malware-free attacks
- Unrivalled visibility to discover and investigate current and historic endpoint activities
- Ease-of-use

Many of the world's largest organizations already put their trust in CrowdStrike, including 254 of Fortune 500, 526 of Global 2000, 15 of the Top 20 Global Banks, 5 of the Top 10 Largest Healthcare Providers and 7 of the Top 10 Largest Energy Institutions.

In June 2019, CrowdStrike conducted one of the most successful technology initial public offerings (IPOs), listing on Nasdaq.

OVERVIEW OF THE G-CLOUD SERVICE

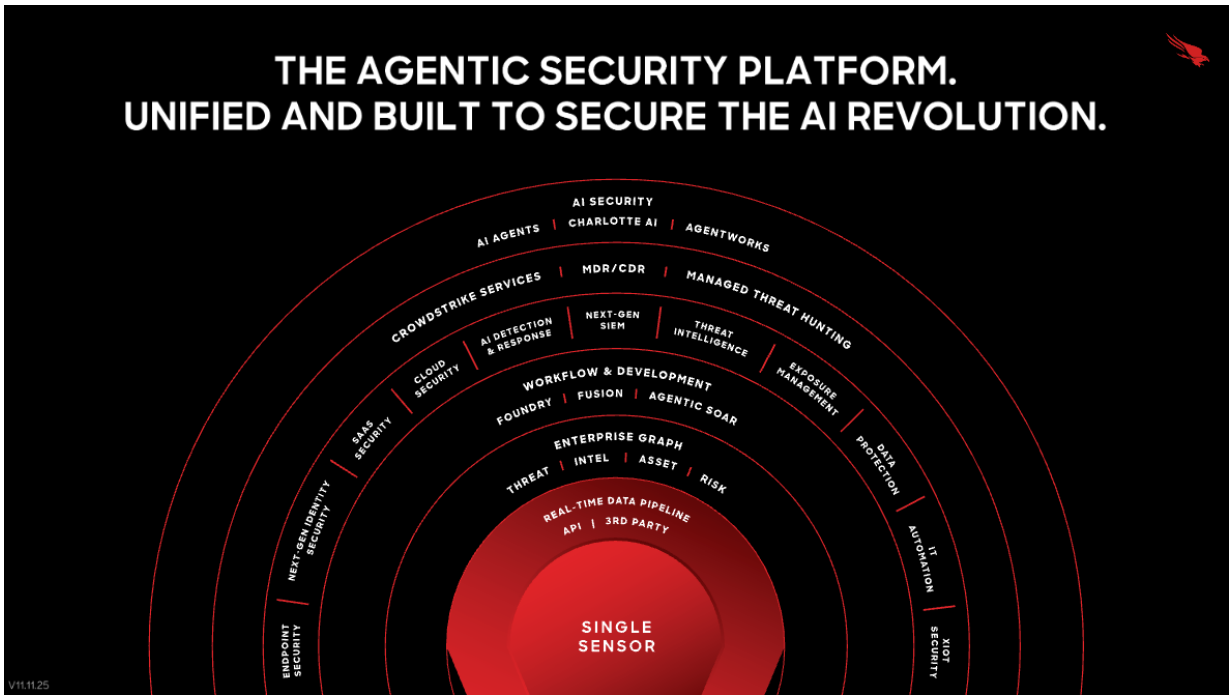
PLATFORM OVERVIEW

Streamlined, single agent architecture
CrowdStrike's single agent is built on a scalable cloud-native platform that's easy to deploy and manage. Say goodbye to managing multiple cybersecurity products with one, unified solution.

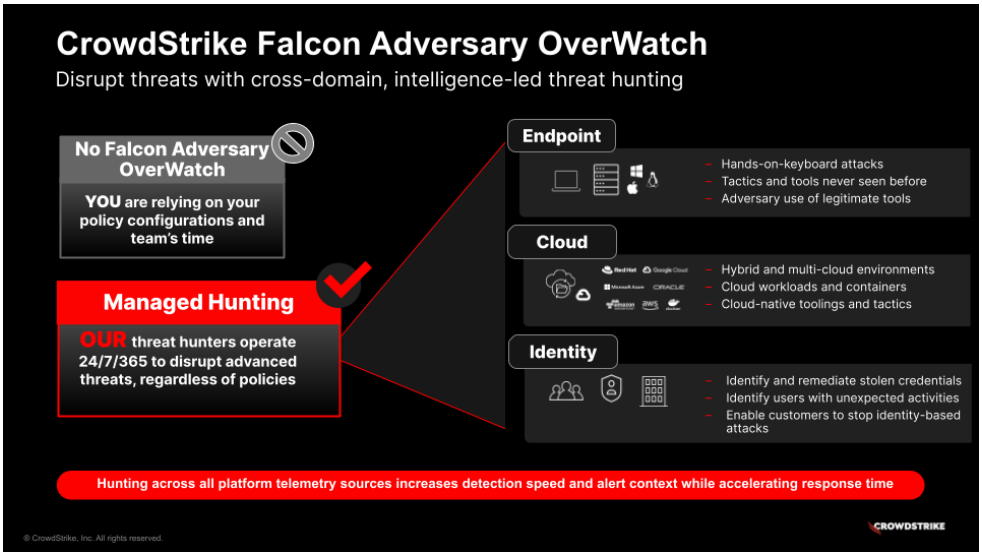
Infused with AI expertise
At CrowdStrike, AI is more than a feature — it's in our DNA. With models trained on trillions of data points every day, we predict and stop threats in their tracks.

Effortless workflows and automation
The power of native automation and generative AI workflows is woven into every corner of our platform. We do the heavy lifting, so you can act swiftly and confidently.

Powered by the CrowdStrike® Security Cloud and world-class AI, the 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.



FALCON ADVERSARY OVERWATCH: MANAGED THREAT HUNTING



CUSTOMER PROBLEM:

Adversaries have become faster and more sophisticated, consistently outpacing security teams and leaving organizations exposed to breaches. Being slower than the adversaries poses significant risks to your brand, reputation and financial standing. With adversaries' growing proficiency and speed in executing complex, cross-domain attacks to defeat endpoint, identity and cloud security solutions, it is imperative for defenders to stay one step ahead to proactively stop breaches.

WHAT'S NEEDED:

Organizations need an advanced security solution that offers real-time, comprehensive monitoring and proactive threat hunting. This solution needs to have visibility across and within clouds, identities and endpoints to stop every stage of a cloud attack — even as threats move laterally among different domains. It must continually adapt to evolving cyber threats through a blend of AI technology, ongoing threat intelligence and expert oversight, ensuring robust protection against both known and emerging threats.

UNIQUE APPROACH:

Disrupt the most sophisticated adversaries with CrowdStrike Falcon Adversary OverWatch. Powered by AI, threat intelligence and unrivaled human expertise, Falcon Adversary OverWatch delivers 24/7 protection across endpoints, identities and cloud workloads.

CrowdStrike's expert hunters leverage the world-class intelligence of the unified, AI-native Falcon platform. Falcon Adversary OverWatch actively monitors all customer environments to identify novel attacks, misuse of remote access tools, credential compromises, insider threats and more. The Falcon Adversary OverWatch team promptly applies these findings to your environment and provides you with real-time alerts to keep you well-informed about potential threats.

- Cross-domain hunting across endpoint, identity and cloud: Falcon Adversary OverWatch hunts 24/7 for adversaries targeting your business's endpoints, identities and cloud environments. As part of

the industry's leading cloud detection and response solution, teams can harness the unified cross-domain visibility of the AI-native Falcon platform to speed response across every stage of a cloud attack, even as threats move laterally from cloud to endpoint.

- World-class expertise powered by AI: Backed by security experts and cutting-edge AI, CrowdStrike's threat hunters are best in class at detecting and stopping the stealthiest adversaries. CrowdStrike proactively identifies novel threats in real time across the entire CrowdStrike customer base and instantly deploys new detections on your behalf.
- Native intelligence to speed up decision-making: Falcon Adversary OverWatch delivers industry-leading threat intelligence within the Falcon platform, making other CrowdStrike modules intelligence-aware on day one. With threat intelligence at your fingertips, you can make quick, confident and better decisions.

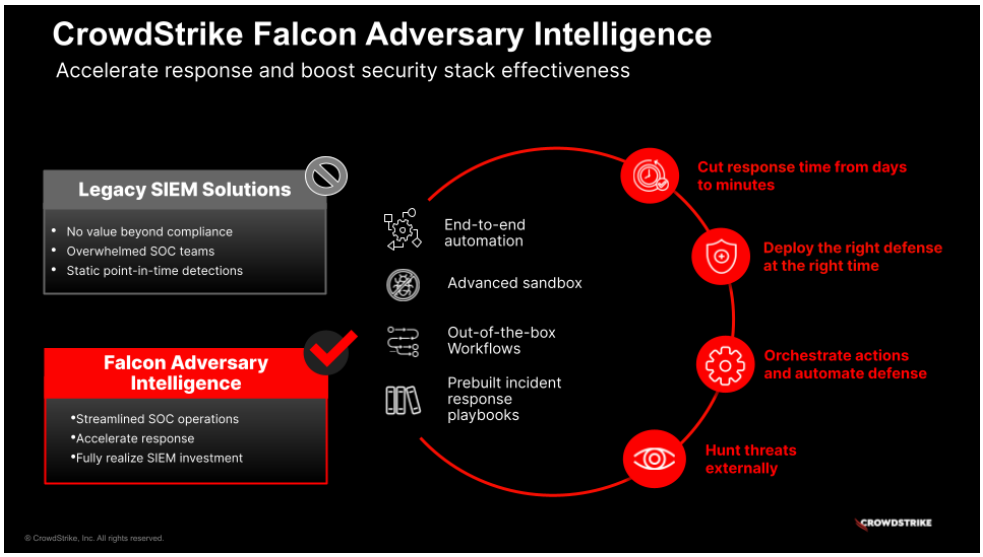
OUTCOME DELIVERED:

- **95%** reduction in threat hunting staffing costs[1]
- **85%** reduction in time spent researching new alerts[1]
- **80%** improvement in security posture[1]
- *"Having experts from Falcon Adversary OverWatch for 24/7 threat hunting provides peace of mind. Alerts have dropped by 500x, and 98% are true positives. There's no noise, no junk. If there's an alert, it's a problem, and we're investigating it."* — Brett Fernicola, Senior Director of Security Operations, Anywhere Real Estate

Product Page: https://www.crowdstrike.com/products/threat-intelligence/adversary-overwatch/

[1] *CrowdStrike BVA – CrowdStrike BVA numbers are projected estimates of average benefits based on recorded metrics provided by customers with 50 security team members and 6 analysts during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment*

FALCON ADVERSARY INTELLIGENCE: INTELLIGENCE AUTOMATION



CUSTOMER PROBLEM:

Adversaries have become faster and more sophisticated, consistently outpacing organizations and breaching their defenses. As endpoint surfaces harden with advanced security like endpoint detection and response (EDR) and Zero Trust, adversaries exploit new ways to break in and evade detection, further complicating defense efforts. Being slower than the adversaries poses significant risks to your brand, reputation and financial standing.

Smaller organizations rely solely on their security tools for protection, while larger entities invest heavily in traditional security information and event management (SIEM) tools to detect and investigate attacks. Unfortunately, legacy SIEM solutions aren't up to the task. One survey found that 61% [2]of security teams say they get more than 1,000 alerts daily, overwhelming understaffed and under skilled SOC teams and leading to slower operations and missed threats.

Additionally, 80% of organizations limit their understanding of threat intelligence to known threats. But intelligence must go beyond the basics — it must offer real-time insight into adversaries' methods and be applied in organizations' environments and SIEMs. Automation is key to shortening the time from detecting to responding, enabling immediate deployment of countermeasures.[3]

[2] *SIEM Data Analytics Challenges facing the SOC — Gurucul*

[3] *CrowdStrike BVA – CrowdStrike BVA numbers are projected estimates of average benefits based on recorded metrics provided by customers with 50 security team members and 6 analysts during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.*

WHAT'S NEEDED:

Eighty percent of organizations believe threat intelligence is simply a listing of known bad files, IP addresses and web domains. They must select intelligence that goes beyond that definition and provides real-time context on adversaries' tools, techniques and tradecraft. Additionally, organizations must apply this information to their environment (and SIEMs). This context must be seamlessly available in their analysts' daily workflows to accelerate understanding and decision-making. Organizations also need automation to shorten the time it takes to detect, investigate and respond to incidents

UNIQUE APPROACH:

CrowdStrike Falcon® Adversary Intelligence optimizes effectiveness for the entire security stack through automated intelligence orchestration, contextual enrichment and AI-powered investigative tools.

Falcon Adversary Intelligence delivers industry-leading threat intelligence into the CrowdStrike Falcon platform, making all modules intelligence-aware on day one. This integration seamlessly delivers the necessary context for confident decision-making into the daily workflow.

- **Streamline your SOC through automation:** Falcon Adversary Intelligence cuts response time from days to minutes across the entire security stack with end-to-end automation. Instantly submit potential threats to an advanced sandbox, extract indicators and deploy countermeasures — all while continuously monitoring for fraud and safeguarding your brand, employees and sensitive data.
- **Integrate seamlessly with third-party tools:** Access a prebuilt library of incident response playbooks, empowering teams to orchestrate actions and automate defenses. Streamline the process with preconfigured workflows, eliminating the need for complex integrations. Ensure timely and precise deployment of the right defenses to the right tools across the entire security stack.
- **Expand threat hunting to external sources:** Falcon Adversary Intelligence prevents external threats that could compromise identities, steal sensitive data and destroy your organization's brand. Disrupt adversaries with 24/7 monitoring and real-time alerts to potentially malicious activity across the open, deep and dark web.

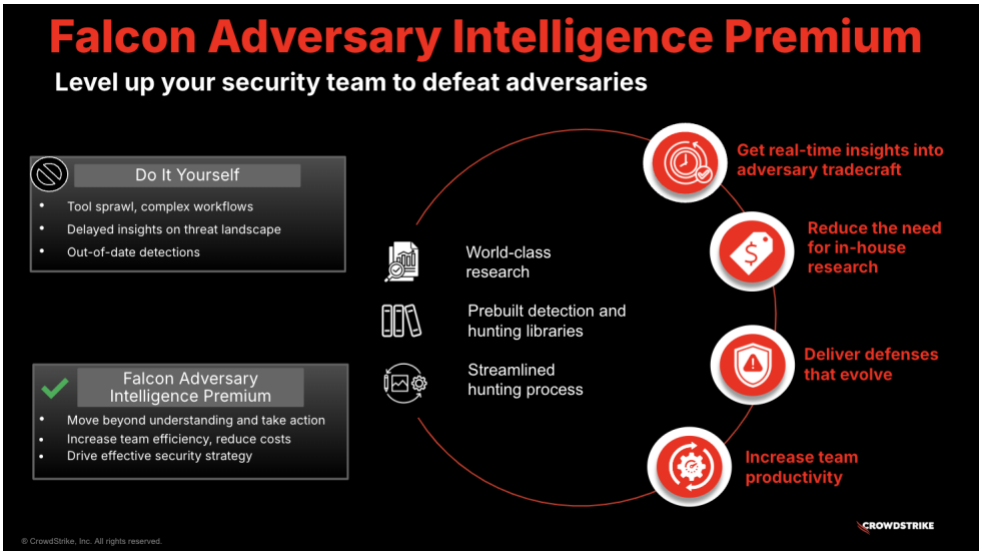
OUTCOME DELIVERED:

- **97%** reduction in time spent researching adversaries and emerging threats[4]
- **80%** reduction in time spent analyzing malware
- **79%** decrease in threat triage efforts
- *"CrowdStrike threat intelligence keeps Tabcorp updated on emerging threat actors, their motives, regions, and the latest techniques, giving invaluable insights on what to protect against and how to tackle threats." - Himanshu Anand, Head of Cyber Threat Management, Tabcorp*

Product Page: https://www.crowdstrike.com/platform/threat-intelligence/adversary-intelligence/

[4] *CrowdStrike BVA – CrowdStrike BVA numbers are projected estimates of average benefits based on recorded metrics provided by customers with 50 security team members and 6 analysts during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.*

FALCON ADVERSARY INTELLIGENCE PREMIUM: THREAT INTELLIGENCE



CUSTOMER PROBLEM:

Today's adversaries operate with unprecedented speed and sophistication. Defenders are struggling to keep up, as many rely on inefficient processes, resulting in false positives and out-of-date countermeasures. To mitigate increasing risks to their brand, reputation and financial stability, organizations require improved strategies for combating adversaries, such as obtaining threat research from trusted advisors and automating the process of adapting security controls to evolving threats.

WHAT'S NEEDED:

To keep up with the pace of modern adversaries, security teams need more than just tools — they require efficient processes and actionable intelligence. Challenges like scarce skills, irrelevant data and rising expenses are causing delays in decision-making and increasing breach risk. Teams are overwhelmed by low-fidelity detections and manual processes. What's needed is a streamlined solution that automates threat detection, reduces false positives and enhances response times, ensuring security teams can focus on what truly matters: preventing breaches and mitigating risks in real time.

UNIQUE APPROACH:

CrowdStrike Falcon® Adversary Intelligence Premium revolutionizes security defenses by delivering world-class research containing in-depth insights into the latest adversary tradecraft. By understanding how adversaries evolve their tactics, cyber threat intelligence teams can improve SOC effectiveness and shape their security strategy to stop breaches more effectively.

- **World-class intelligence reporting:** CrowdStrike tracks over 245 adversaries, exposing their activity, tools and tradecraft. Every year, we publish thousands of threat alerts, in-depth technical analyses and strategic insights into cyber threats targeting your organization, reducing the need for expensive in-house threat research.

- **Prebuilt hunting and detection libraries:** Enable in-house security engineering teams to evolve and defend against the latest adversary tactics and techniques. Utilize the built-in library of continuously updated hunting queries and detection rules to lower development and testing costs and better protect your business.

- **Streamlined security engineering processes:** Falcon Adversary Intelligence Premium delivers integrated tools and workflows to speed the process of creating, customizing and refining hunting and detection libraries from a single platform. Improve your security posture, accelerate your security teams' productivity and proactively adjust security controls as threats evolve.

OUTCOME DELIVERED:

- **97%** reduction in time spent researching adversaries and emerging threats[5]
- **80%** improvement in security posture
- **65%** reduction in time spent creating detection rules
- *"With CrowdStrike, we detected a malicious actor and received all the information we needed to defend against them. We are able to do more comprehensive threat hunting for potential threats and respond better to active threats in our networks. We are able to cut down on analyst research and focus on the really critical issues."* — Threat Intelligence Analyst — Cyber Defense Operations, Multinational Telecommunications Company

Product Page: https://www.crowdstrike.com/platform/threat-intelligence/adversary-premium/

[5] *CrowdStrike BVA – CrowdStrike BVA numbers are projected estimates of average benefits based on recorded metrics provided by customers with 50 security team members and 6 analysts during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.*

FALCON COUNTER ADVERSARY OPERATIONS ELITE: A POWERFUL ALLY

CUSTOMER PROBLEM:

Today's adversaries are increasingly fast and elusive, continuously adapting their motives and tactics. Their evolving techniques represent a significant challenge in the modern threat landscape, and adversary breakout time continues to get faster.

As adversaries demonstrate greater proficiency and speed in targeting organizations, it is imperative that defenders stay one step ahead to proactively stop breaches.

WHAT'S NEEDED:

Many organizations face severe challenges in addressing cybersecurity threats. A shortage of security staff affects 67% of organizations, and 92% of security teams lack critical cybersecurity skills[6]. Moreover, 80% of organizations focus solely on known threats, leaving critical visibility gaps in their defenses. [7]To stay ahead of evolving adversaries, it's essential to strengthen security teams' skills, expand visibility across all potential attack vectors and ensure that threat intelligence is comprehensive and proactive. Organizations need solutions that can bridge these gaps by providing tailored, real-time insights and expert guidance.

[6] *ISC2 Workforce Study 2023*

[7] *ESG Attributes of a mature security program*

UNIQUE APPROACH:

A truly effective cybersecurity program requires relevant, timely and actionable threat intelligence, but tracking scores of adversaries and analyzing their tradecraft requires a massive effort. CrowdStrike Falcon® Counter Adversary Operations Elite was created to help you focus on what matters most: threats targeting your organization.

UNIQUE APPROACH:

A truly effective cybersecurity program requires relevant, timely and actionable threat intelligence, but tracking scores of adversaries and analyzing their tradecraft requires a massive effort. CrowdStrike Falcon® Counter Adversary Operations Elite was created to help you focus on what matters most: threats targeting your organization.

- **Assigned Falcon Counter Adversary Operations Elite analyst**: The Falcon Counter Adversary Operations Elite team is staffed by seasoned analysts with unsurpassed expertise battling nation-state, eCrime and hacktivist adversaries. A Falcon Counter Adversary Operations Elite analyst works directly with your team to learn the unique cybersecurity challenges your organization faces. This understanding enables the analyst to help you apply threat intelligence more effectively, defeating the adversaries targeting your organization. The analyst is your point of contact for intelligence research, threat hunting, detection engineering and personalized threat briefings. The analyst also provides proactive notifications of threats against your organization, going beyond consultation to become an extension of your team.
- **Requests for information (RFIs)**: Threat intelligence research can be difficult, and CrowdStrike can provide assistance. An RFI is a request for CrowdStrike to perform research, on your behalf, into a specific threat to your organization. You can have up to five RFIs per year, and additional packs are available for purchase. The research is performed by a domain expert who delivers a custom response.
- **Priority intelligence requirements (PIRs)**: PIRs align the activities of threat intelligence teams to the goals and strategies of your organization. Your Falcon Counter Adversary Operations Elite analyst helps you create PIRs — or leverage knowledge of existing PIRs — to provide proactive notifications of threat activities that may target your organization, employees or infrastructure. Examples of PIRs include:

    - Which nation-state actors are targeting your region or industry?
    - Are there threats to your organization from criminal underground sites monitored by CrowdStrike?
    - Which tactics and techniques are adversaries likely to use to exploit your infrastructure?

- **Proactive and tailored threat hunting**: Facing ever-evolving adversaries, your assigned analyst detects new and sophisticated intrusions in real time, using custom hunts specifically designed for your environment.

OUTCOME DELIVERED:

- **97%** reduction in time spent researching adversaries and emerging threats by cutting down in-house research and focusing on critical issues[8]
- **85%** reduction in the effort of triaging and investigating incidents by off-loading resource-intensive tasks to CrowdStrike experts
- **80%** improvement in risk posture by delivering curated intelligence relevant to your business
- *"CrowdStrike Falcon Counter Adversary Operations Elite provides the necessary intelligence to inform stakeholders and leadership to make strategic, operational, or tactical decisions and reduce risk to the organization. We are more prepared against threat actors that leverage legitimate tools we see every day."* — Leading Financial Services Organization

Product Page: https://www.crowdstrike.com/en-us/blog/announcing-crowdstrike-falcon-counter-adversary-operations-elite/

[8] *CrowdStrike BVA – CrowdStrike BVA numbers are projected estimates of average benefits based on recorded metrics provided by customers with 50 security team members and 6 analysts during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment*

DATA PROTECTION

INFORMATION ASSURANCE

CrowdStrike has obtained several compliance certifications that position the company at the top of the security vendor space. These include both ISO27001:2022 and SOC2 Type II. A summary/breakdown and certificates can be provided upon request. For a full breakdown please visit: https://www.crowdstrike.com/why-crowdstrike/crowdstrike-compliance-certification/

DATA BACKUP AND RESTORATION

The offering from CrowdStrike is a SaaS platform and hence localised backups are all covered as part of the native service offering. All information needed about data management is outlined in the Business Continuity section of this Service Definition.

If the customer wishes they can also retrieve all data from within the platform and store it at an alternative location, this data can be retrieved in near real time or weekly in bulk. Several API's exist that allow data to be extracted more surgically for backup or other purposes.

BUSINESS CONTINUITY

CrowdStrike has a documented Business Continuity Plan (BCP). The plan covers every aspect of restoring and recovering the service given a catastrophic data centre failure as well as protecting the confidentiality and integrity of the data. Disaster recovery provisions are included within our BCP.
CrowdStrike hosts the Falcon platform across multiple discrete and redundant data centre's; each data centre has its own power, networking and connectivity, and is housed in separate facilities. High speed, low-latency networks between data centre's support near real-time replication of data, and transparent fail-over in the event of a single data centre outage. The entire process is seamless and transparent to customers.
A summary of the BCP plan elements can be shared with the customer upon request.

PRIVACY BY DESIGN

The CrowdStrike Falcon Platform was designed not only with privacy in mind but as a platform to protect organizations data. Additionally, cybersecurity plays a key role in data protection and GDPR compliance. CrowdStrike's next-generation product offerings, professional services, and global expertise can help organizations meet their GDPR obligations.

CrowdStrike understands that organizations must consider regulatory requirements when choosing vendors. That is why CrowdStrike helps customers enhance their cybersecurity and data protection posture while meeting a wide range of compliance needs. Choosing CrowdStrike as a vendor can be a critical component for helping fulfil GDPR compliance.

- Proudly protects many of the world's largest organisations
- Participates in and has certified its compliance with the EU-U.S. Data Privacy Framework to ensure the adequacy of cross-border transfers
- Meets TRUSTe's Privacy Certification requirements
- We abide by the EU's General Data Protection Regulation (GDPR), and as a data processor,

we provide our customers with a GDPR compliant data processing addendum, which we will need to incorporate in the Call Off Contract. In particular, CrowdStrike Products are hosted on a data centre located in the EU. CrowdStrike's Affiliates worldwide, and its Sub processors, may remotely access Buyer's Data for the purposes described in Exhibit A to the CrowdStrike Terms and Conditions and the CrowdStrike Data Protection Addendum. CrowdStrike Products also leverage a crowdsourcing model for certain customer data to improve its offerings for the benefit of all customers, as described fully at the CrowdStrike Terms and Conditions, Exhibit A, Section 2. CrowdStrike is available to answer any customer questions about this and to ensure this is accurately described in any Call Off Contract.
Please contact CrowdStrike if you require further information.