WHITEHAWK

Cyber Risk Scorecard

On Company: Colonial Pipeline Company

Prepared for:

WhiteHawk

Prepared by:

Mike Ferris

Analyst

mike.ferris@whitehawk.com

Prepared on:

May 24, 2021

Table of Contents

WHITEHAWK

WhiteHawk Cyber Risk Scorecard

WhiteHawk's Cyber Risk Scorecard provides businesses and organizations a topline cyber risk snapshot as an indicator of a company's effectiveness at addressing the impacts of online crime and fraud. We use a risk rating ranging from 0 to 100 based upon over 20 cyber risk controls. Our Cyber Analysts provide context and analytics that augment the risk indicators obtained through Black Kite, enabling companies to take action to mitigate cyber risks to their revenue, reputation, and operations.

We developed this Cyber Risk Scorecard based on combined analytics from your risk rating. WhiteHawk presents key findings summarized as a prioritized list of options on which you can immediately act. All collected and analyzed open data sets are externally observable, and we do not conduct penetration testing of your company's internal networks with this scorecard.

WhiteHawk partners with top risk assessment companies to collect topline risk ratings and identify selective insight trends based on 20+ risk controls to prioritize risk indicators for enterprises.

– Data-driven, dynamic measurements of an organization's cybersecurity performance
– Derived from objective, verifiable information
– Material and validated measurements
– Created by a trusted, independent organization

WhiteHawk designed the Cyber Risk Scorecard to provide clients with actionable information to:

- Facilitate impactful budget-based, risk reduction decision-making based upon cyber risk vector indicators
- Enable timely actions
- Prevent online crime and fraud from disrupting business operations

WhiteHawk Cyber Analysts perform customized analytics to:

- Provide prioritized, affordable, and impactful options to mitigate cyber risks of small and midsize businesses and organizations
- Track key actions and mitigations to accept or address known risks
- Provide maturity planning in the form of an achievable risk reduction roadmap, thereby enabling data-driven decision making in terms of business risk and budgets
- Maintain informed and enable engagement

WHITEHAWK

Cyber Risk Scorecard Results Summary

We are pleased to present the results of the WhiteHawk Cyber Risk Scorecard. This section is an executive overview. Subsequent sections provide associated descriptions and context to our findings and solution options.

Company	Domain
Colonial Pipeline Company	colpipe.com

Security Rating

Ratings measure a company's relative security effectiveness.

C+ (78.0/100)	Advanced:	100 – 80
	Intermediate:	79 – 70
	Basic:	60 – 0

Risk Vector Performance

Risk Vector grades show how well the company is managing each risk vector.

Compromised Systems:	A	System Patching:	F
Communications Encryption:	B	Application Security:	B
Attack Surface:	A	Email Security:	B
		Public Disclosure:	D

Factor Analysis of Information Risk (FAIR) - Annualized Risk

Forecasted annualized loss magnitude risk of a potential loss to your company.

Most Likely:	$87,542.71
Minimum:	$9,080.38
Maximum:	$3,425,513.91

Prioritized Areas of Focus

WhiteHawk Cyber Analyst has identified top-3 Focus Areas the company should consider.

Focus Area 1:	System Patching
Focus Area 2:	Public Disclosure
Focus Area 3:	Application Security

Solution Options

Solution options that address primary business risks identified in the Cyber Risk Scorecard. Alternatives for each are included in the product details section.

Essential Bundle	Balanced Bundle	Premier Bundle
– *SmartBear: Test Execute*	– *ClearNetwork Services: SOC-As-A-Service*	– *Analyst1: Analyst1 Platform*
– *Mimecast: M2 Product Bundle*	– *McAfee: McAfee Virtual Network Security Platform*	– *Fortinet: FortiAnalyzer*
	– *Juniper Networks: SRX Series Services Gateways*	– *Ditno: Ditno Network Firewall*
		– *LookingGlass: On-Demand Single Investigation*

For more solution options, visit www.whitehawk.com/marketplace

WHITEHAWK

Cyber Risk Scorecard Results Detail

Cyber Risk Security Rating Results

Cybersecurity Ratings measure a company's security performance using proprietary algorithms that analyzes externally observable data with "hacker's view" of how to exploit this data. Ratings range from 0 to 100, with a higher rating equating to an overall better security posture with the ability to prevent cybercrime and fraud from negatively impacting your business. In addition to gaining insight into your critical cyber risks, companies can work with WhiteHawk Cyber Analysts to perform deeper analysis, including incorporating existing IT implementation baselines, to develop remediation strategies that align with your business model and objectives.

Cyber Risk Ratings are categorized as Basic, Intermediate, and Advanced. While companies have different methods of assessing risk, these categories serve as a general best practice guideline and marker of the overall maturity of your cyber resilience.

This company falls into the Intermediate category, meaning its relative security effectiveness is fair, having an average security performance and medium risk.

Security Rating

78.0/100

Security Rating Categories and Approach

ADVANCED: 100 – 80
Relative security effectiveness is high, having a strong security performance and lowest risk

INTERMEDIATE: 79 – 70
Relative security effectiveness is fair, having an average security performance and medium risk.

BASIC 69 –0
Relative security effectiveness is moderate, having a weak security performance and high risk.

Security Ratings are calculated using a proprietary risk measurement algorithm that evaluates evidence of security outcomes and practices. Multiple risk vectors comprise the rating, and it is updated daily. To provide a simple look at the external security posture of a company, the Security Rating is organized into three categories.

WHITEHAWK

Cyber Security Risk Vector Results

As previously mentioned, security vectors and their outcomes are used to develop your company's Security Rating. Over 20 risk vectors are used in the Risk Rating determination. For simplicity, we have organized them into 7 groups. Below is each Risk Vector and the company's associated resulting grade. We provide WhiteHawk's Cyber Analyst notes for additional context.

Risk Vector Performance *Risk Vector grades show how well the company is managing each risk vector.*	
Compromised Systems:	A
Communications Encryption:	B
Attack Surface:	A
System Patching:	F
Application Security:	B
Email Security:	B
Public Disclosure:	D

A Compromised Systems

Compromised Systems measures multiple items. Company employees may download malicious applications from the Internet and may become infected as a member of a botnet. Blacklist providers may mark the company and the entire IP range as blacklisted, which may result in a loss of profit. Moreover, company employees sometimes register domains with their corporate emails and host them at servers with a bad reputation. Even worse, company admins register some domains on behalf of their company but forget to configure the resolving IP properly. Because the same IP address(es) host third-party applications with malware or are linked to malicious activities, the lack of IP/domain management may result in company-registered domains & IP addresses with a bad reputation.

WhiteHawk Cyber Analyst Note:

— Your company is doing exceptionally well in maintaining its IP reputation. Continue to monitor the reputation and categorization of your website to stay at this level.

B Communications Encryption

Encryption provides confidentiality and integrity of the data in transit. Encryption is important because it allows you to securely protect data that you do not want anyone else to access. Businesses use it to protect corporate secrets, governments use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft. Communications Encryption measures SSL/TLS protocols/algorithms like SSL v2.0, SSL v3.0, RC4, DES, 3DES, and integrity algorithms like SHA1; MD5 are considered old and not secure anymore.

WhiteHawk Cyber Analyst Note:

— Your company is performing well but has some shortfalls in its encryption standards. Upgrade to stronger protocols such as TLS protocols 1.1 and 1.2.

A Attack Surface

Attack surface is the technical analysis of critical open ports, out-of-date services, application weaknesses, SSL/TLS strength, and any misconfigurations. Attackers search for remotely accessible vulnerable network services. Common examples include poorly configured web servers, mail servers, file and print services installed by default on various device types, often without a business need for the given service. Many software packages automatically include and enable services as part of installing the main product without informing the user or system administrator. Attackers scan for and attempt to exploit these services, often trying default user IDs and passwords or widely available exploitation codes. This information is gathered from Censys and Shodan databases, and service/application versions are correlated with Passive Vulnerability Scan results.

WhiteHawk Cyber Analyst Note:

— Your company is doing well in its website security and reducing its attack surface. Continue to implement best security practices.

F System Patching

Hackers look for weak links in cyber defenses. Servers with known vulnerabilities are easy targets for them. Successful exploitation may result in data loss, bad reputation, loss of credibility, or financial problems. Systems Patching measures out-of-date servers accessible from the Internet that may have multiple vulnerabilities, either related to the application servers or the application framework. They can be design flaws or implementation bugs that enable attackers to compromise applications or the system itself.

WhiteHawk Cyber Analyst Note:

— Your company is significantly below its peers in patching vulnerabilities and has a poor patching cadence resulting in a significantly increased risk of incident occurrence. Monitor your systems for known vulnerabilities and apply the appropriate patches. Additionally, establish a frequency of vulnerability scanning and compare reported vulnerabilities with your inventory/control list.

B Application Security

Vulnerabilities and weaknesses related to web applications create risks for the users of these web applications. Hackers can exploit login forms without encryption, lack of bot detection or missing web application best practices to bypass authorization and authentication of company resources. Application Security measures application-level security problems, especially for web applications. Web Applications are tested against multiple web application security controls, including inadequate encryption strength, certificate validity, and proper use of HTTPS.

WhiteHawk Cyber Analyst Note:

— Your company is doing well but has some shortfalls resulting in the slight risk of an incident occurrence in its application security that prevents it from achieving the top grade. Continue to review your current encryption standards and website security.

WHITEHAWK

B Email Security

Email is one of the top entry points for cyberattacks of all sizes. Email Security measures the use of SPF, DKIM, and DMARC DNS records. These records identify which mail servers are permitted to send emails on behalf of your domain. They are also used to detect and prevent email spoofing, mitigating specific techniques often used in phishing and email spam, such as emails with forged sender addresses that appear to originate from legitimate organizations.

WhiteHawk Cyber Analyst Note:

— Your company is performing satisfactorily but faces some risk in its email security. Review your SPF, DKIM, DMARC and DNS records, and perform periodic reviews on your mail server and supporting network.

D Public Disclosure

Public Disclosure measures the protection of sensitive information from parties that are not supposed to have access to such information. These issues are not exploitable in most cases. Still, they are considered security issues because they allow attackers to gather information that can be used later in the attack life cycle to achieve more than they could if they did not access such information.

WhiteHawk Cyber Analyst Note:

— Your company is not implementing common best practices o keep sensitive information from leaking resulting in significant risk of incident occurrence. Ensure that all services running on the server's open ports do not reveal information about their build and versions, do not hard-code credentials, API keys, IP addresses or any other sensitive information, and always check whether each of the requests to create/edit/view/delete resources have proper access controls.

WHITEHAWK

Compliance Overview

Organizations that have already aligned their security programs to either one of the following cybersecurity frameworks may find this crosswalk helpful in identifying potential gaps in their programs. Taking specific action to address these gaps can bolster compliance and improve an entity's ability to secure sensitive information from a broad range of threats.

This compliance correlation is designed to be flexible, scalable, and technology-neutral, enabling it to accommodate integration with more detailed frameworks such as NIST 800-53, NIST 800-171, CIS CSC-20, and CMMC. The compiled results are an estimation based on the publicly visible output correlated using proprietary algorithms.

Although these results do not guarantee any compliance, the crosswalk provides an informative tool for companies to use to help more comprehensively manage security risks in their environments by deduplicating the workload across different similar standards and best practices. The mappings between the framework control items are intended to be an informative reference and do not imply or guarantee compliance with any laws or regulations. Companies that have aligned their security program to one of these standards should not assume that by so doing, they are in full compliance with the corresponding compliance standard.

The resulting compliance diagrams presented below are an estimation of your organization's overall compliance health. The estimates are based upon information collected by scans and information provided by your organization. All scores can be improved by providing WhiteHawk with current information security policies for evaluation. The results summary presents the following attributes of compliance:

COMPLIANCE

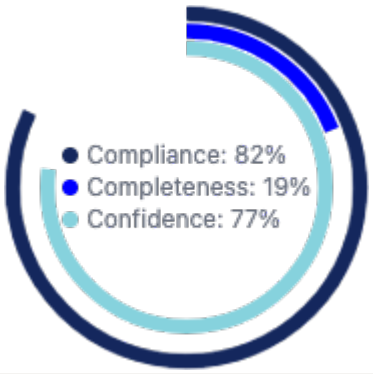
The overall compliance score is how much of the specified framework we believe you are following, based on platform validation and self-attestation.

CONFIDENCE

The level of confidence we have in our estimation. WhiteHawk does not have access to your internal systems and processes, so we can only provide a score based on the information available and how much it aligns with the controls in the framework.

COMPLETENESS

The degree to which the compliance requirements can be measured with the collected information. This score is generated by matching collected artifacts to framework control areas. Each area of the framework has requirements that can be met by policy or configuration

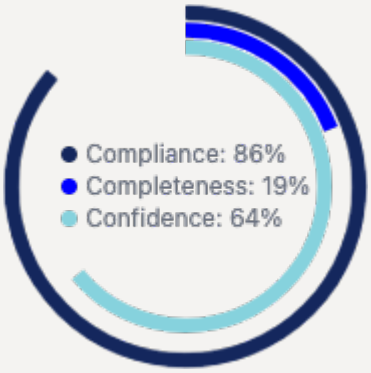


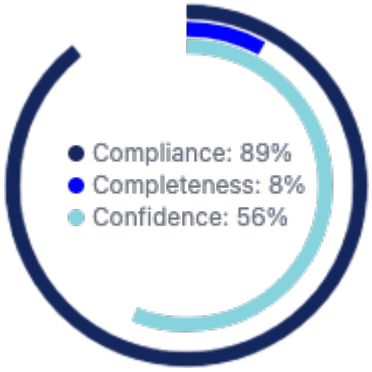
NIST 800-53

A framework required for federal government systems that have received a FIPS classification or systems that store sensitive federal data. These controls are required to comply with the Federal Information Security Management Act (FISMA) requirements and consist of a total of 900 controls that are encompassed in 18 control families.

CIS CSC-20

A framework that consists of twenty best practice guidelines that help companies establish a baseline to safeguard their systems and data from known cyber-attack vectors. The controls are sorted into three levels to prioritize the most effective actions to improve their cyber defense. This can help companies standardize and develop their security practices if they do not have an established security program set in place.



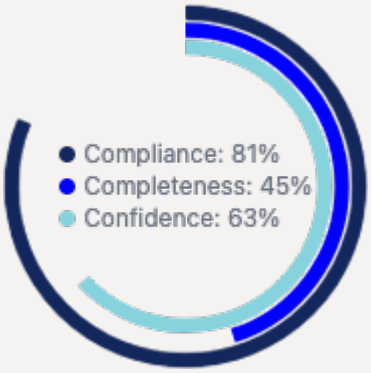


CMMC

A new framework established for the DoD's supply chain to follow to replace the self-assessment of NIST 800-171. Any company that plans to conduct business with the DoD will be required to undergo an audit by an authorized CMMC C3PAO auditor before bidding, winning, or participating in a contract or subcontracting to a prime. It encompasses all 110 NIST 800-171 Controls and an additional 20 controls, along with 17 control families in total and five levels of maturity.

NIST 800-171

A framework required for private sector organizations contracted under the federal government and do not interact with sensitive government data. Organizations must use this framework when establishing security requirements to protect Controlled Unclassified Information (CUI) confidentiality on non-federal systems. It consists of 110 controls, which are encompassed in 14 control families.



WHITEHAWK

FAIR Overview

Factor Analysis of Information Risk (FAIR), simply stated, is a quantitative risk analysis model that describes what risk is, how it works, and how to quantify it. It is the only international standard quantitative model for cybersecurity and operational risk. Unlike risk assessment standards that focus their output on qualitative color charts or numerical weighted scales, the FAIR quantitative risk analysis model specializes in financially derived results tailored for enterprise risk management.

FAIR proposes a model for calculating risk. This model uses Loss Event Frequency (LEF) and Loss Magnitude (LM) to calculate risk. LM answers the question "What will be the impact if there is a breach" while LEF calculates the likelihood of a breach. In other words, it is possible to consider a formula of **Annualized Risk Cost = LEF x LM.** Additional context is described below for LEF and LM.

- Risk (Annualized Risk Cost): The probable frequency and probable magnitude of future loss.
- Loss Event Frequency (LEF): The frequency, within a given timeframe, that loss is expected to occur. An organizations probability of a LEF is determined by factoring the probability of a Threat Event Frequency (average # of times vulnerability discovered times probability it can be exploited) by the Vulnerability Level (capability level of threats versus the strength of internal controls and response capabilities)
- Loss Magnitude (LM). The potential loss to your organization. This is determined by calculating Exposure (number of records shared in common) by the average cost for Primary Loss (Incident Response, Legal Fees, Victim Compensation) and Secondary Loss (Notification Costs, Fines, Share Price, Lost Business).

The FAIR measurements allow corporate leadership and stakeholders to understand cyber and operational risks in financial terms. Thereby providing added context and building blocks to developing and enhancing a risk management strategy across the entire company. Contact WhiteHawk and schedule a virtual consultation to review the FAIR results. During the consultation, we can also review additional areas that may of interest associated with the FAIR results, such as:

- Productivity Loss: Loss that results from an operational inability to deliver products or services
- Replacement Costs: Loss that results from an organization having to replace capital assets
- Competitive Advantage Loss: Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged
- Reputation Damage: Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased

We will also help align the FAIR findings with the cyber risk vector performance and compliance results from the previous sections to help better align solution options to mitigate your top risks. Contact us today.

WHITEHAWK

FAIR Results Summary

Based on the data processed and results of the FAIR model calculations, the below summarizes your company's financial risk posture.

Risk (Annualized)

$87,542.71

$9,080.38	—— Most Likely ——	**$3,425,513.91**
Min		Max

The forecasted annualized loss based on the given parameters below.

Loss Event Frequency (LEF)

0.026

How many times over the next year is the loss even likely to occur?

Loss Magnitude (MF)

$3,425,513.91

How much loss is your organization likely to experience as a direct result of a loss event?

Threat Event Frequency (TEF)

10.41

How many times will the organization face a threat action?

Vulnerability (VUL)

6,945%

What percentage of the threat events are likely to result in loss events?

Primary Loss (PL)

$1,324,981.21

How much money are you likely to lose from each loss event?

Secondary Loss (SL)

$2,100,532.71

How much loss as a result of secondary stakeholders?

Contact Frequency (CF)

100.43

How many times over the next year is the threat actor/agent likely to reach the organization?

Probability of Action (PoA)

2,351%

What percentage of threat/agent contacts with the asset are likely to result in threat events?

Threat Capability (TCap)

3,100%

How capable is the threat community of successfully carrying out the threat event?

Resistance Strength (RS)

6,046%

The strength of a control as compared to a baseline unit of force.

Estimated Costs If Breach Occurs

Detection and Notification: **$401,619.30**
Notification: **$224,396.82**
Response: **$527,842.51**
Loss to Business: **$946,674.07**

WHITEHAWK

Path to CMMC: Your Alignment

What is CMMC?

CMMC stands for Cybersecurity Maturity Model Certification, a cyber risk maturity framework for all companies and organizations to follow to smartly prevent and mitigate a breadth of risks from cybercrime, fraud, espionage, and disruption. The U.S. Department of Defense (DoD) has started to incorporate CMMC certification into the Defense Federal Acquisition Regulation Supplement (DFARS) and use it as a standing requirement for contract award beginning in 2020. CMMC is based upon five maturity levels that range from "Basic Cybersecurity Hygiene" to "Advanced/Progressive."

Official Background Information:

- Home Page: Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification
- CMMC V1.0 OSD Public Briefing Slides
- CMMC V1.02 Official Document - PDF

Who Needs CMMC?

CMMC is starting to be leveraged to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB) and, eventually, all Federal contractors. The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene. The CMMC approach also attempts to protect controlled unclassified information (CUI) in the DoD's industry partners' networks.

What is WhiteHawk's "Path to CMMC" and Your Alignment?

WhiteHawk's maturity models were initially built upon the Center for Internet Security (CIS) Framework, which maps to the NIST Framework and is meaningful down to the small and midsize business levels. Using WhiteHawk's online maturity models, we have mapped the CIS Framework to CMMC. By aligning multiple frameworks, WhiteHawk can deliver an easy-to-understand and documented path to CMMC compliance.

What Level Does My Company Need to Achieve?

CMMC Levels are mapped to the work your company does. DoD expects the majority of subcontractors to prime DoD contractors to be at Levels 1 and 2. An organization that handles CUI will need to achieve Level 3 and above.

WHITEHAWK

Your Mapping to CMMC

WhiteHawk helps you map to CMMC categories and controls to the CMMC maturity levels. CMMC's five different certification levels reflect the maturity and reliability of a government contractor's cybersecurity infrastructure to protect sensitive and high-level government information. The five levels (L1 – L5) build upon each other's technical requirements with the next level, including the previous level requirements. See the visual below to better understand where each CIS control maps to these new standards.

CMMC Category	Maturity Levels				
	L1	L2	L3	L4	L5
Access Control	●	●	●	●	●
Asset Management	n/a	n/a	●	●	n/a
Audit and Accountability	n/a	●	●	●	●
Awareness and Training	n/a	●	●	●	n/a
Configuration Management	n/a	●	●	●	●
Identification and Authentication	●	●	●	n/a	n/a
Incident Response	n/a	●	●	●	●
Maintenance	n/a	●	●	n/a	n/a
Media Protection	●	●	●	n/a	n/a
Personnel Security	n/a	●	n/a	n/a	n/a
Physical Protection	●	●	●	n/a	n/a
Recovery	n/a	●	●	n/a	●
Risk Management	n/a	●	●	●	●
Security Assessment	n/a	●	●	●	n/a
Situational Awareness	n/a	n/a	●	●	n/a
System and Communications Protection	●	●	●	●	●
System and Information Integrity	●	●	n/a	●	●

● *Meets or Exceeds All Expectations.* ● *Meets Some Expectations.* ● *Has Significant Shortfalls.*
'n/a ' *Category does not have required controls at this level.*

WHITEHAWK

Recommendations

WhiteHawk Cyber Analysts analyzed the security rating and risk vector performance results and recommends the following tailored solution options to prevent and mitigate online crime and fraud, thereby improving your company's overall cybersecurity posture. We base the solution options on externally available information about cyber resilience gaps. Internal processes and IT solutions currently in place may impact company actions. WhiteHawk presents this information to identify areas of focus for further investigation and potential action. Please go to www.whitehawk.com to schedule an appointment with one of our Cyber Analysts to further refine, prioritize, and take smart actions to mitigate your leading cyber risks.

Top 3 Areas of Focus

Understanding and addressing cyber risks to your revenue, reputation, and operations can be overwhelming to most businesses and organizations today. WhiteHawk has taken your cyber risk rating results and performed additional analysis to present a prioritized list of affordable and impactful solution options for you to consider as a starting point. Today and into the future, online crime and fraud prevention and protecting your company's and customers' sensitive information is an ongoing business need requiring an active and ongoing maturity approach. Take smart action now, starting with the following focus areas based on the perceived risks derived from the risk rating and risk vector assessment:

Focus Area 1: **System Patching**

Your company is significantly below its peers in patching vulnerabilities and has a poor patching cadence resulting in a significantly increased risk of incident occurrence. Monitor your systems for known vulnerabilities and apply the appropriate patches. Additionally, establish a frequency of vulnerability scanning and compare reported vulnerabilities with your inventory/control list.

Focus Area 2: **Public Disclosure**

Your company is not implementing common best practices o keep sensitive information from leaking resulting in significant risk of incident occurrence. Ensure that all services running on the server's open ports do not reveal information about their build and versions, do not hard-code credentials, API keys, IP addresses or any other sensitive information, and always check whether each of the requests to create/edit/view/delete resources have proper access controls.

Focus Area 3: **Application Security**

Your company is doing well but has some shortfalls resulting in the slight risk of an incident occurrence in its application security that prevents it from achieving the top grade. Continue to review your current encryption standards and website security.

WHITEHAWK

Solution Options

In alignment with the above focus areas, WhiteHawk presents three bundled solution options for your company's consideration. Please schedule a quick call with one of our Cyber Analysts to refine and select the best options for your needs and business priorities. This process starts your cybersecurity maturity journey in context to your company's current IT implementation processes and implementations.

WhiteHawk presents three solution options with alternatives for each category for your consideration.

ESSENTIAL BUNDLE

The Essential Bundle supplies the **essential** cybersecurity products that fit your company's immediate cyber risk needs based on the Cyber Threat Readiness Questionnaire results and cyber risk rating. This bundle represents the minimum your company needs to be doing to **prevent or mitigate the most common cybercrime and fraud events**.

BALANCED BUNDLE

The Balanced Bundle offers cybersecurity products and services representing the **standard best practices for your company's online operations.** This bundle consists of key solution options for your business to address your priority cyber risks.

PREMIER BUNDLE

The Premier Bundle provides a **top-of-the-line maturity level** for cybersecurity products. This bundle achieves the level of cyber maturity that your company should be **striving towards to address a wide range of cybercrime and fraud vectors threatening your revenue, customers, and reputation.**

WHITEHAWK

ESSENTIAL BUNDLE

Patch Management

SmartBear — Test Execute		Trend Micro — Deep Security as a Service
TestExecute is a lightweight, fast, and easy-to-use runtime license that helps reduce testing time by splitting tests created using TestComplete or TestLeft on distributed infrastructure containing physical as well as virtual machines. It's perfect for setting up parallel test suites, specifying specific actions that need to be performed after each run, and the data that needs to be shared across tests.	*or*	Built on Trend Micro's industry-leading Hybrid Cloud Security solution, powered by XGenâ„¢, Trend Microâ„¢ Deep Securityâ„¢ as a Service is designed to augment cloud provider security with complete protection for cloud workloads. Deep Security provides a complete suite of security capabilities including intrusion detection and prevention, firewall, malware prevention with web reputation, predictive machine learning, sandbox analysis, integrity monitoring, log inspection, and multi-platform application control.

Email Filter

Mimecast — M2 Product Bundle		Mandiant — Security Instrumentation Platform
Comprehensive security and cyber resilience in a single integrated service with Targeted Threat Protection that defends against malware-less spear-phishing, weaponized attachments and malicious URLs, Data Leak Protection and Content Control protects against inadvertent or malicious loss of valuable information and Mailbox Continuity ensures employees have uninterrupted access to live and historical email even during primary system downtime.	*or*	Verodin Security Instrumentation Platform, (SIP) a cybersecurity risk assessment and management platform that enables teams to ensure their critical assets are always protected

WHITEHAWK

BALANCED BUNDLE

Incident Response

CrowdStrike — CrowdStrike Falcon		CipherCloud — CASB+
The Falcon agent (small and light) and cloud (big and powerful) work seamlessly to deliver real-time protection and visibility -- yes, even when the agent is not connected to the internet. The simplicity of CrowdStrike's architecture finally gives you the freedom to replace and retire the complicated, performance-robbing security layers that clutter your environment.	*or*	CipherCloud CASB+ enables seamless SaaS-mobile-remote security with agentless deployment, allowing organizations to scale fast with best-in-class performance and real-time data protection, without requiring any resource intensive installation of agents and expensive upkeep.

Host-Based Intrusion Prevention System

McAfee — McAfee Virtual Network Security Platform		Sonicwall — SOHO Network Security Firewall
McAfee Host Intrusion Prevention safeguards businesses against complex security threats that may otherwise be unintentionally introduced or allowed by desktops, laptops, and servers. It leverages a three-part threat defense â€" signature analysis, behavioral analysis, and system firewall â€" all easily managed from one central console, the McAfee ePolicy Orchestrator (ePO) platform.	*or*	Designed for small networks including remote and branch offices, the TZ Series offers five different models that can be tuned to meet your specific needs. Advanced unified threat management (UTM) security, networking and management features plus optional 802.11ac Wi-Fi ensure your network and data are protected from the latest threats over wired and wireless connections.

Network Intrusion Detection System

Juniper Networks — SRX Series Services Gateways		Check Point — Thret Prevention Security Suite
Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of your network to detect and stop potential incidents.	*or*	Increasing your enterprise security often means increasing your complexity and management challenges in kind. Check Point delivers a multi-layered line of defense to help you maximize your security while minimizing challenges and closing gaps.

WHITEHAWK

PREMIER BUNDLE

Orchestration

Analyst1 — Analyst1 Platform		D3 Security — D3 Soar
Reduce “time to act” through automation, and shift to a proactive defensive posture. Created by cybersecurity analysts, Analyst1 provides Intelligence, SOC, Incident Response, Vulnerability analysts and CISOs the actionable insight needed to protect their enterprise.	*or*	D3 Security’s NextGen SOAR Platform is the first and only security orchestration, automation, and response (SOAR) platform that combines automation and orchestration across 300+ integrated tools with the proactive response capabilities of MITRE ATT&CK. D3’s codeless playbooks automate enrichment and remediation tasks, while making it easy for anyone to build, modify, and scale workflows for security operations, incident response, and threat hunting. • Automated event enrichment and triage • Incident/case management • Codeless response playbooks • MITRE ATT&CK TTP correlation • Orchestration across 300+ integrated tools.

Security Information and Event Management

Fortinet — FortiAnalyzer		Micro Focus Software — Sentinel Enterprise
FortiAnalyzer platforms integrate network logging, analytics, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine tune your policies.	*or*	Here's a security solution that isn't as complex as the problem. Sentinel is a full-featured Security Information and Event Management (SIEM) solution that simplifies the deployment, management and day-to-day use of SIEM, readily adapts to dynamic enterprise environments and delivers the true "actionable intelligence" security professionals need to quickly understand their threat posture and prioritize response.

— ***Premier Bundle Solution Options Continued on Next Page*** —

WHITEHAWK

PREMIER BUNDLE - CONTINUED

Network Intrusion Prevention System

Ditno — Ditno Network Firewall		Juniper Networks — SRX Series Services Gateways
Ditno Network Firewall provides a single pane of glass to visualize and manage all of your servers consistently, significantly reducing requirements for specialist FTE's and high operating costs. We sit on the kernel of every host meaning we can access everything that is happening on each server and quickly track and stop malicious activities.	*or*	Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of your network to detect and stop potential incidents.

Threat Intelligence

LookingGlass — On-Demand Single Investigation		ProcessUnity — Third-Party Risk Management
Single request from among the list of on-demand investigations and analyses.	*or*	ProcessUnity Vendor Cloud is a software-as-a-service (SaaS) application that identifies and remediates risks posed by third-party service providers. Combining a powerful vendor services catalog with risk process automation and dynamic reporting, Vendor Cloud streamlines third-party risk activities while capturing key supporting documentation that ensures compliance and fulfills regulatory requirements.

WHITEHAWK

About Us

Easily find out where the biggest risks are

In near real time make the changes you need to protect your organization

Get alerted to new threats that are targeting you

Track how your network vulnerabilities change over time

WhiteHawk, Inc., is the first online Cybersecurity Exchange based on a platform architecture that is Artificial Intelligence (AI)-driven, with a focus on identifying, prioritizing, and mitigating cyber risks for businesses of all sizes. WhiteHawk continually vets and assesses risk-focused technologies, methodologies, and solutions that are impactful, affordable, and scalable to stay up to date on current cyber threat vectors to businesses, organizations, family offices, and individuals. We have an online approach to determining your key cyber risks through a Cyber Threat Readiness Questionnaire, and as appropriate, a cyber risk assessment. Using this information, we match tailored risk mitigation solution options to companies and organizations based on current threat trends across key sectors. Our Cyber Consultants on staff help build a tailored cyber maturity plan customized to meet your business or mission objectives.

For more information, visit www.whitehawk.com.

WhiteHawk CEC Inc.
Terry Roberts - Founder, President, & CEO
consultingservices@whitehawk.com

WHITEHAWK

Disclaimer for Cyber Risk Scorecard

The Cyber Risk Scorecard and its contents and use are expressly subject to the WhiteHawk Terms and Conditions contained at https://www.whitehawk.com/terms-conditions. Acceptance of this Cyber Risk Scorecard, or use of any information contained herein, by any party receiving this Cyber Risk Scorecard (each "Recipient") shall constitute an acknowledgement and acceptance by such Recipient of, and agreement by such Recipient to also be bound by, the following:

Background: WhiteHawk's proprietary open analytic approach to understanding the cyber risk landscape globally, tracking threat vectors that impact each Public and Private Sector, and mapping to discoverable risk activity being experienced by a specific organization or company result in a current (and therefore dynamic) cyber risk profile based upon vetted and published risk standards and frameworks (including, but not limited to the Center for Internet Security [CIS]/National Institute of Standards and Technology [NIST]/Cybersecurity Maturity Model Certification [CMMC]). All identified risk data sets, impacting a specific company or organization with a uniquely registered internet domain address, are then prioritized, and mapped to key areas of focus and potential risk mitigation options, in a tailored and easy to understand and actionable Cyber Risk Scorecard.

(1) This Cyber Risk Scorecard was created by WhiteHawk CEC Inc. for the entity named herein (the "Company") and is based on publicly accessible information, not within the control of WhiteHawk. In preparing this Cyber Risk Scorecard, WhiteHawk has conducted cyber risk analytics that are assumed to be as complete and correct as an external assessment can be. In preparing this Cyber Risk Scorecard, the WhiteHawk platform and team leverages a broad set of publicly available cyber risk related data sets and cyber threat information regarding companies, organizations, vendors, and suppliers. When WhiteHawk is given permission to work directly with companies then additional Digital Footprint information can be voluntarily provided via the WhiteHawk online Cyber Threat Readiness Questionnaire and a virtual consult. This added information is then incorporated into an updated Cyber Risk Scorecard. As a result of the foregoing and the nature of Digital Age Risk, WhiteHawk stands behind the use of Its Cyber Risk Scorecard to prioritize discoverable risks and to make initial vetting decisions. Cyber risks, however, can only be conclusively validated by a Red Team or on-premises sensors or inspection. The information contained in this Cyber Risk Scorecard is a guideline based upon publicly available risk indicators and proven risk standards and best practices and is a sound basis for formulating an initial risk mitigation plan. Cyber risk and fraud can be smartly reduced but cannot be completely prevented nor eliminated.

(2) TO THE FULLEST EXTENT PERMITTED BY LAW, WHITEHAWK'S TOTAL LIABILITY, ON A CUMULATIVE AND AGGREGATE BASIS, TO THE COMPANY AND ALL RECIPIENTS AND OTHER PARTIES, RESULTING FROM WHITEHAWK'S ACTIONS IN RELATION TO THE CREATION AND DISSEMINATION OF THIS CYBER RISK SCORECARD, WILL BE LIMITED TO THE AMOUNT OF COMPENSATION ACTUALLY RECEIVED BY WHITEHAWK FROM THE COMPANY FOR THE CREATION OF THIS CYBER RISK SCORECARD.

IF ANY RECIPIENT IS NOT WILLING TO ACKNOWLEDGE AND ACCEPT, OR AGREE TO, THE TERMS SET FORTH ABOVE, IT MUST RETURN THIS CYBER RISK SCORECARD TO WHITEHAWK IMMEDIATELY WITHOUT MAKING ANY COPIES THEREOF, EXTRACTS THEREFROM OR USE (INCLUDING DISCLOSURE) THEREOF. A RECIPIENT'S FAILURE SO TO RETURN THIS CYBER RISK SCORECARD SHALL CONSTITUTE ITS ACKNOWLEDGEMENT AND ACCEPTANCE OF AND AGREEMENT TO THE TERMS SET FORTH ABOVE.

Cyber Risk Scorecard

WhiteHawk CEC Inc.

www.whitehawk.com