

WHITEHAWK

Cyber Risk Scorecard

On Company: Sample Corp.

Prepared for:

WhiteHawk

Prepared by:

Prepared on:



Table of Contents

WhiteHawk Cyber Risk Scorecard	3
Cyber Risk Scorecard Results Summary	4
Cyber Risk Scorecard Results Detail	5
Security Rating Results	5
Security Risk Vector Results	6
Compliance Overview	10
FAIR Overview	12
FAIR Results Summary	13
Path to CMMC	14
Recommendations	16
Top 3 Areas of Focus	16
Solution Options	17
About WhiteHawk	22

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

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			
Sample Corp			samplecorp.com			
Security Rating			Risk Vector Performance			
<i>Ratings measure a company's relative security effectiveness.</i>			<i>Risk Vector grades show how well the company is managing each risk vector.</i>			
C (76.0/100)	Advanced:	100 – 80	Compromised Systems:	B	System Patching:	B
	Intermediate:	79 – 70	Communications Encryption:	B	Application Security:	F
	Basic:	60 – 0	Attack Surface:	A	Email Security:	A
			Public Disclosure:		B	
Factor Analysis of Information Risk (FAIR) - Annualized Risk			Prioritized Areas of Focus			
<i>Forecasted annualized loss magnitude risk of a potential loss to your company.</i>			<i>WhiteHawk Cyber Analyst has identified top-3 Focus Areas the company should consider.</i>			
Most Likely:	\$87,482.95		Focus Area 1:	Application Security		
Minimum:	\$6,107.19		Focus Area 2:	Compromised Systems		
Maximum:	\$2,996,895.97		Focus Area 3:	Communications Encryption		
Solution Options						
<i>Solution options that address primary business risks identified in the Cyber Risk Scorecard. Alternatives for each are included in the product details section.</i>						
Essential Bundle		Balanced Bundle		Premier Bundle		
<ul style="list-style-type: none"> – Flexera Software: FlexNet Manager for Engineering Applications – Micro Focus Software Inc.: Identity Administration 12 Month 		<ul style="list-style-type: none"> – ClearNetwork Services: SOC-As-A-Service – Juniper Networks: SRX Series Services Gateways – Trend Micro: Deep Discovery Analyzer 		<ul style="list-style-type: none"> – Trend Micro: Trend Micro 24/7 Support – Micro Focus Software Inc.: Sentinel Enterprise – Cyber BDA: Cyber Sales Force TRAINING – Micro Focus Software Inc.: Aegis Adapter for AppManager 		
For more solution options, visit www.whitehawk.com/marketplace						

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

76.0/100

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.

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

B 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 well but has some shortfalls with slight risk of an incident occurrence. If possible, avoid using shared servers/IP's with other domains.

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 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.

B 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 passing but has some weaknesses in updating its servers. Review current server operating systems and periodically update them as needed.

F 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 not implementing standard best practices for securing its application security program resulting in a significant risk of incident occurrence. Check your encryption on web applications that require authentication or host sensitive information. Be sure to detect and block excessive login/submission attempts, avoid mixing HTTP and HTTPS contents that are susceptible to Man-in-the-Middle attacks, and consider applying security headers to your web applications.

A 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 outstanding in implementing SPF, DKIM, DMARC, and DNS records. Continue to use authenticated mail relay.

B 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 performing acceptably but has a slight risk of incident occurrence. Continue to review access control policies and ensure your web server does not send out response headers that reveal information about the backend technology type or version.

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.



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.

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)		
\$6,107.19	\$87,482.95	\$2,996,895.97
Min	— Most Likely —	Max
<i>The forecasted annualized loss based on the given parameters below.</i>		

LOSS EVENT FREQUENCY (LEF)
0.029
<i>How many times over the next year is the loss even likely to occur?</i>

LOSS MAGNITUDE (MF)
\$2,996,895.97
<i>How much loss is your organization likely to experience as a direct result of a loss event?</i>

THREAT EVENT FREQUENCY (TEF)
10.26
<i>How many times will the organization face a threat action?</i>

VULNERABILITY (VUL)
5,703%
<i>What percentage of the threat events are likely to result in loss events?</i>

PRIMARY LOSS (PL)
\$1,177,191.08
<i>How much money are you likely to lose from each loss event?</i>

SECONDARY LOSS (SL)
\$1,819,704.89
<i>How much loss as a result of secondary stakeholders?</i>

CONTACT FREQUENCY (CF)
182.89
<i>How many times over the next year is the threat actor/agent likely to reach the organization?</i>

PROBABILITY OF ACTION (PoA)
1,218%
<i>What percentage of threat/agent contacts with the asset are likely to result in threat events?</i>

THREAT CAPABILITY (TCAP)
3,100%
<i>How capable is the threat community of successfully carrying out the threat event?</i>

RESISTANCE STRENGTH (RS)
6,776%
<i>The strength of a control as compared to a baseline unit of force.</i>

ESTIMATED COSTS IF BREACH OCCURS
Detection and Notification: \$347,925.37
Notification: \$194,396.39
Response: \$457,273.34
Loss to Business: \$820,109.79

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.

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.

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: Application Security

Your company is not implementing standard best practices for securing its application security program resulting in a significant risk of incident occurrence. Check your encryption on web applications that require authentication or host sensitive information. Be sure to detect and block excessive login/submission attempts, avoid mixing HTTP and HTTPS contents that are susceptible to Man-in-the-Middle attacks, and consider applying security headers to your web applications.

Focus Area 2: Compromised Systems

Your company is doing well but has some shortfalls with slight risk of an incident occurrence. If possible, avoid using shared servers/IP's with other domains.

Focus Area 3: Communications Encryption

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

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.

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**.

ESSENTIAL BUNDLE

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.

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**.

PREMIER BUNDLE

ESSENTIAL BUNDLE

Application Security

Flexera Software — FlexNet Manager for Engineering Applications

FlexNet Manager for Engineering Applications helps improve engineering and design professionals' productivity, optimize software spend, accurately forecast usage, and negotiate vendor contracts. It tracks license usage, simplifies and centralizes license server administration for thousands of FlexEnabled and other concurrently licensed applications including AutoCAD®, MATLAB®, IBM® Rational®, CATIA®, and Petrel to automatically report on software usage and license denials, and maximize utilization of assets.

Flexera Software — AdminStudio Suite

Ensure Consistent and Reliable Application Deployment. AdminStudio Suite powers an enterprise's daily Application Readiness process for inventory, rationalization, packaging, planning, and compatibility testing of physical, virtual, and mobile applications, ensuring faster service delivery and predictable deployment.

or

Access Control

Micro Focus Software Inc. — Identity Administration 12 Month

Identity Governance is a comprehensive identity governance solution that provides a business-friendly interface built on a common governance model that spans all of your business processes relating to identity, access and certification. Demonstrate compliance and be confident your access recertification campaigns are done right using Identity Governance.

Mimecast — Email Signature Management

With Mimecast Email Signature and Disclaimer Management, administrators can control email branding, signatures and disclaimers from a single console complete with an image library and templates. Personalized content can be quickly added using Active Directory variables such as phone numbers and office locations, easing centralized management.

or

BALANCED BUNDLE

Incident Response

ClearNetwork Services — SOC-As-A-Service

Monitor Redefine visibility into your assets and devices. ClearNetwork integrates with your technology stack, providing 24/7 monitoring with real-time detection and reporting. Track and report user actions automatically. Our team does the work of discovering and securing your network assets so you don't have to. Review comprehensive alert logs in real-time. Our team categorizes alerts by severity so you can see the status of your network at any moment. Analyze Streamline security event investigation. We turn the complex, time-consuming task of event analysis into a readymade service. Re

or

WireX Systems — WireX Systems NDR Platform

We deliver comprehensive security intelligence in actual human readable form so you can save effort and time when validating alerts and responding to security incidents. Automate and Accelerate Your Incident Response with intelligence from network payloads that goes well beyond traditional logs. Powerful central hub to streamline the entire investigation and response processes and to accelerate knowledge sharing across team members. The framework includes integration points with the various SIEM vendors to import tickets details (as well as export them back at the end of the process)

Network Intrusion Detection System

Juniper Networks — SRX Series Services Gateways

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

Sophos — SG UTM Network Protection

Sophos UTM provides the ultimate network security package with everything you need in a single modular appliance. It simplifies your IT security without the complexity of multiple point solutions. The intuitive interface will help you quickly create policies to control security risks. And clear, detailed reports will give you the insight you need to improve your network performance and protection.

Malware Analysis

Trend Micro — Deep Discovery Analyzer

Deep Discovery Analyzer extends the value of existing security investments from Trend Micro and third-parties (through a web services API) by providing custom sandboxing and advanced analysis. It can also provide expanded sandboxing capabilities to other Trend Micro products. Suspicious objects can be sent to the Analyzer sandbox for advanced analysis using multiple detection methods. If a threat is discovered, security solutions can be updated automatically.

or

Symantec — Blue Coat Malware Analysis Appliance

The Blue Coat Malware Analysis Appliance is a key component of Blue Coat's Advanced Threat Protection solution, providing actionable intelligence that combines static, dynamic, and reputational analysis techniques. Integrated with the Blue Coat Content Analysis System or the Blue Coat Security Analytics Platform with ThreatBLADES, it provides a highly scalable solution for detecting and analyzing unknown, advanced, and targeted malware.

PREMIER BUNDLE

Security Network Engineering

Trend Micro — Trend Micro 24/7 Support

Take advantage of our superior support services to keep your security strong, minimize threats, and free up your valuable IT resources for other critical functions. How do we know our support is best? We're Trend Micro "100% security, 100% focused, 100% of the time. We're global SECURITY experts and completely dedicated to helping your organization exchange digital information safely.

Flexera Software — FlexNet Normalized Inventory for Clients

or

FlexNet Normalized Inventory for Clients enables enterprises to gain visibility and control of their IT estate by providing a comprehensive inventory of deployed desktop and laptop hardware and associated software assets.

Security Information and Event Management

Micro Focus Software Inc. — Sentinel Enterprise

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.

or

Fortinet — FortiAnalyzer

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.

— Premier Bundle Solution Options Continued on Next Page —

PREMIER BUNDLE - CONTINUED

Managed Security Services

Cyber BDA — Cyber Sales Force TRAINING

Rendition Infosec — Rendition Infosec - Red Team Assessment

Our sales-focused TRAINING services offers added value to your client and partner network. This service empowers your team with knowledge of how your cyber products and services are applied to Federal government customer requirements. As an example, we tailor our introductory class to focus on cyber.

or

Offensive services include: Custom crafted phishing campaigns that target specific business functions, Network and Web Application vulnerability assessment and exploitation to help establish baselines, Mobile, Wireless, and IoT exploitation, 3rd Party provider assessments, Physical penetration testing

Compliance Reporting

Micro Focus Software Inc. — Aegis Adapter for AppManager

Vendor Risk Management — Vendor Risk Management

Aegis® is an IT Process Automation (ITPA) platform that enables you to define, automate, measure and improve routine IT tasks and processes. With Aegis, you can improve efficiency through reduced manual labor, reduce service delivery time through self-service and automation, demonstrate compliance with enforcement and automated records Improve service consistency by reducing human error.

or

Powerful automation and analytics platform to manage, monitor, and mitigate vendor risks.

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

Disclaimer for Cyber Risk Scorecard

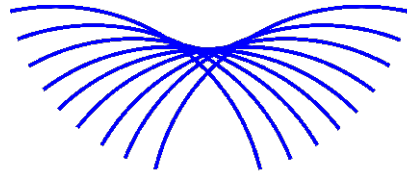
The Cyber Risk Scorecard and its contents and use are expressly subject to the WhiteHawk Terms and Conditions contained at <https://www.whitehawk.com/terms-conditions>. Acceptance of this Cyber Risk Scorecard, or use of any information contained herein, by any party receiving this Cyber Risk Scorecard (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.



WHITEHAWK®

Cyber Risk Scorecard

WhiteHawk CEC Inc.

www.whitehawk.com

