WHITEHAWK

Cyber Risk Radar

For Enterprise Supplier/Vendor Risk Management

www.whitehawk.com

Copyright © 2020 WhiteHawk CEC, Inc. All Rights Reserved.

The information presented here is for general informational purposes only. All information is provided in good faith; however, we make no representation or warranty of any kind, expressed or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information presented. Under no circumstances shall we have any liability to you for any loss or damage of any kind incurred as a result of the use of the information provided.

WHITEHAWK

Executive Overview

Our economic and political adversaries seek access to information systems most vulnerable, often leveraging discrete intersections to their advantage, gaining and holding root-level access in critical business and government systems.

As a result, there is a risk imperative to have continuous insight across your suppliers' and vendors' cyber and associated business risks to prioritize and address them in real-time, with limited resources. This White Paper discusses the Cyber Risk Radar process to assess, identify, monitor, prioritize, and mitigate business and cyber risks for companies and their supply chains.

- ✓ The WhiteHawk Cyber Risk Radar provides near real-time continuous monitoring, prioritization, and mitigation support of the cyber risks of an enterprise's teammates, vendors, and suppliers over time.
- ✓ The Cyber Risk Radar enables the establishment of a scalable strategy and an automated path to Cybersecurity Maturity Model Certification (CMMC).
- ✓ It is an annual Software as a Service (SaaS) subscription consisting of quarterly services that include Cyber Risk Scorecards, Cyber Risk Portfolio Reports, and online CMMC Cyber Analyst consultations.

WhiteHawk continues to work in each industry sector and implement Cyber Risk Radars to help organizations and companies with their enterprise multi-faceted business risks (to include Finance, Operations, Governance, Geographic, and IT risks) and cyber risks. We focus on core areas leveraging cutting edge technology solutions to provide transparency and understanding across a complex and ever-evolving risk environment.

WhiteHawk's Cyber Risk Radar for Supply Chains

WHITEHAWK

Cyber Risk Radar Key Features

How Can Companies/Organizations Optimally Combine Deep Tradecraft, All Publicly Available Data, and AI Analytics?

Risk programs can now fully leverage all company focused subscriptions (D&B, Gartner, Bloomberg, etc.), world wide web open data sets, AI-driven risk identification, risk tradecraft, and best practice analytics, in order to perform thorough business and cyber risk analysis.

WhiteHawk's Cyber Risk Scorecard maximizes data discovery and visualization via the following methods:

- ✓ **SCRM Portfolio Assessments** — Understand an organization's portfolio of all suppliers and vendors.
- ✓ **Risk Research and Discovery** — Collect, analyze, and correlate openly available data into actionable intelligence.
- ✓ **Continuous Risk Monitoring and Alerts** — Understand an organization's security performance and be alerted to impactful changes.
- ✓ **Focused Analytics** — Perform deep dives in the areas that need focus rather than into the entire dataset.
- ✓ **Ecosystem Maps** — Visualize the enterprise by understanding the supplier and vendor interconnections.
- ✓ **CMMC Risk Prioritization and Mitigation** — Prioritize risk mitigation and business actions based on CMMC levels for impact and performance.
- ✓ **Integration Into One Risk Management Dashboard** — Continuous situational awareness, tracking, mitigation, and management of the Supply Chain Risk Management (SCRM)/Vendor Relationship Management (VRM) program.

Cyber Risk Portfolio Reporting

The WhiteHawk The Cyber Risk Portfolio Report is an aggregated view across multiple suppliers or entities revealing current vulnerability trends and changes over time, across all included companies or organizations.

View Executive Level Trend Reporting:

- ✓ Gather and analyze cyber risk data and analytic outputs for each ‘supplier/vendor’ in the company’s portfolio
- ✓ Perform data collection, assessment, and analytics using externally-available open data

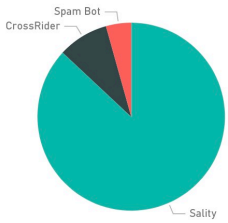
Cyber Risk Portfolio Reporting contains:

- ✓ Analytic summary across the entire supplier portfolio
- ✓ Summary of top-findings for prioritization & action
- ✓ Report of all suppliers/vendors: security rating scores and top risk vectors
- ✓ Historical context for Risk Rating scores for all companies in the portfolio
- ✓ Analyst Notes that summarizes all of the above

Compromised Systems

Source Host Geo IP Location

Count of Infection by Infection



Count of Infection by Month

Compromised Systems

Risk Type	GeoIP Location	Infection	Detection Mechanism	Days	Year	Month	Day
Botnet Infections	United States	Sality	p2p	1	2018	August	25
Botnet Infections	United States	Sality	p2p	6	2018	November	21
Botnet Infections	United States	Sality	p2p	1	2018	November	25

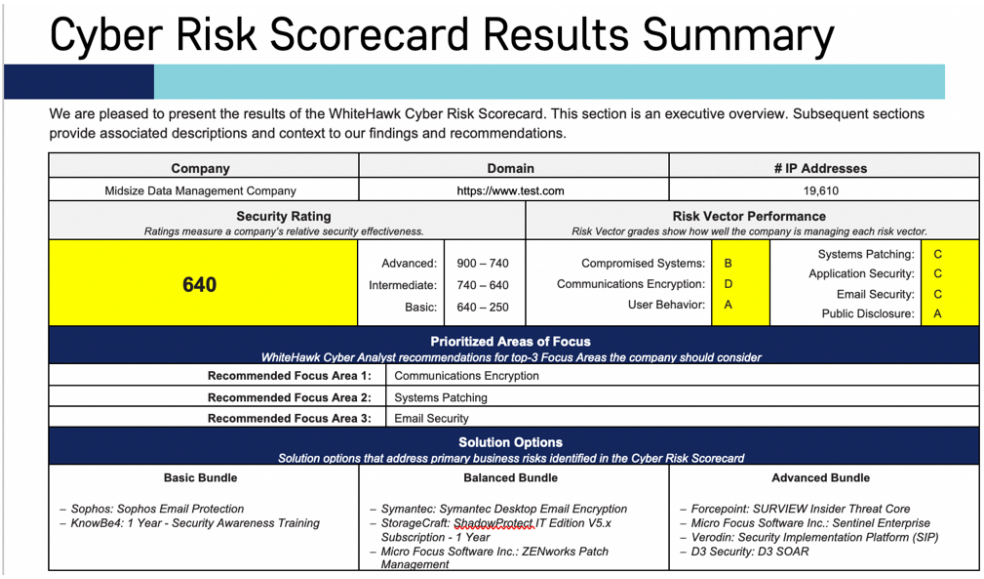
Spam Propagation - Most Recent

Vendors	Infection	Email Subject	Month
Northrop Grumman Corporation	Spam Bot		March

WHITEHAWK

Cyber Risk Scorecard

WhiteHawk's Cyber Risk Scorecard provides businesses and organizations a topline cyber risk report and summary of a company's effectiveness at addressing the impacts of online crime, fraud and disruption. We start with cyber risk continuous monitoring across 20-30 cyber risk controls. Our cyber global threat trend analytics and deep dives across hundreds of companies provide powerful trend context. This augments the risk indicators, enabling companies to take smart action to mitigate cyber risks to their revenue, reputation, and operations. To learn more about WhiteHawk's Cyber Risk Scorecard process, visit us on www.whitehawk.com.



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 recommendations.

Company	Domain	# IP Addresses
Midsize Data Management Company	https://www.test.com	19,610

Security Rating *Ratings measure a company's relative security effectiveness.*			Risk Vector Performance *Risk Vector grades show how well the company is managing each risk vector.*			
640	Advanced:	900 – 740	Compromised Systems:	B	Systems Patching:	C
	Intermediate:	740 – 640	Communications Encryption:	D	Application Security:	C
	Basic:	640 – 250	User Behavior:	A	Email Security:	C
					Public Disclosure:	A

Prioritized Areas of Focus
WhiteHawk Cyber Analyst recommendations for top-3 Focus Areas the company should consider

Recommended Focus Area 1:	Communications Encryption
Recommended Focus Area 2:	Systems Patching
Recommended Focus Area 3:	Email Security

Solution Options
Solution options that address primary business risks identified in the Cyber Risk Scorecard

Basic Bundle	Balanced Bundle	Advanced Bundle
– *Sophos: Sophos Email Protection* – *KnowBe4: 1 Year - Security Awareness Training*	– *Symantec: Symantec Desktop Email Encryption* – *StorageCraft: ShadowProtect IT Edition V5.x Subscription - 1 Year* – *Micro Focus Software Inc.: ZENworks Patch Management*	– *Forcepoint: SURVIEW Insider Threat Core* – *Micro Focus Software Inc.: Sentinel Enterprise* – *Verodin: Security Implementation Platform (SIP)* – *D3 Security: D3 SOAR*

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

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

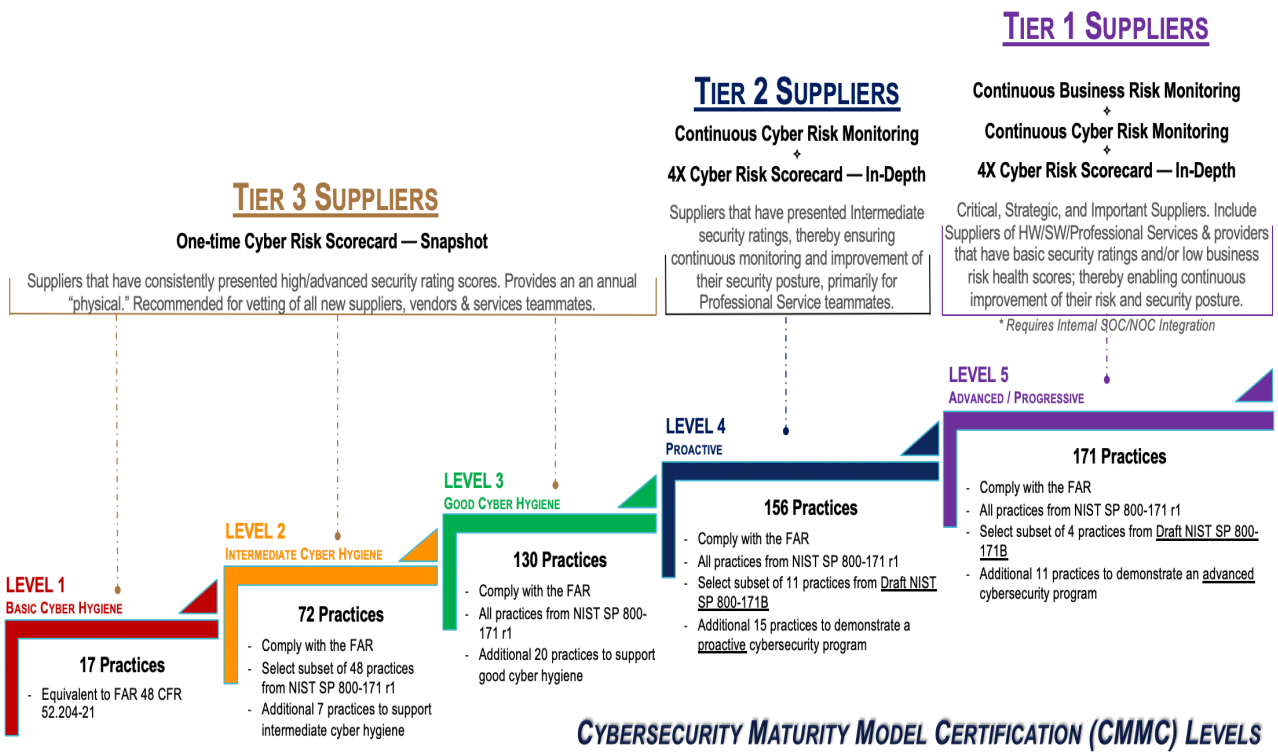
WhiteHawk Cyber Analysts perform customized analytics to:

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

Achieving CMMC Levels

The WhiteHawk Cyber Risk Radar enables an automated path to the Cybersecurity Management Model Certification levels for companies of all sizes.

Below shows the mapping of how the Cyber Risk Radar Level options provide an automated path to achieving CMMC. WhiteHawk includes recommendations for Cyber Risk Radar Levels for each tier of suppliers.



WHITEHAWK

About Us

Easily find out where the biggest risks are

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

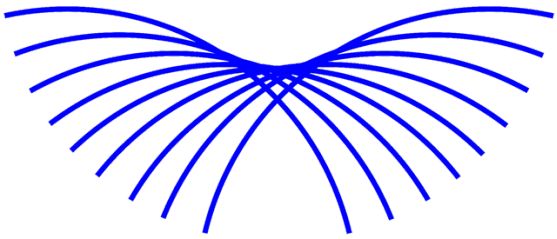
Get alerted to new threats that are targeting you

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 then 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.

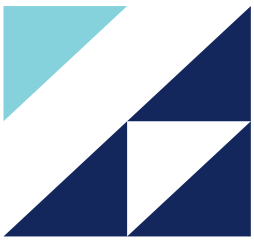
WhiteHawk CEC, Inc.
Terry Roberts - Founder, President, & CEO
consultingservices@whitehawk.com



WHITEHAWK®

Cyber Risk Radar

www.whitehawk.com



Copyright © 2020 WhiteHawk CEC Inc. All Rights Reserved.