EMPOWERING A FEARLESS INTERNET

WHITEHAWK®

Cyber Risk Program

Pioneering Automated Risk and Compliance Solutions

Empowering Enterprises, Supply Chains, and Critical Infrastructure Entities with AI-Driven Risk and Compliance Solutions

www.whitehawk.com

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.

Executive Overview

Leadership has to know how a cyberattack can impact them and what to do first to prevent revenue and reputational loss from an adversary. Whether you are cyber sophisticated or a novice, cybercriminals are always targeting your weaknesses. The Cyber Risk Program stress tests your organization to identify holes in your cyber defense and then we work with you to mitigate risks before adversaries exploit them.

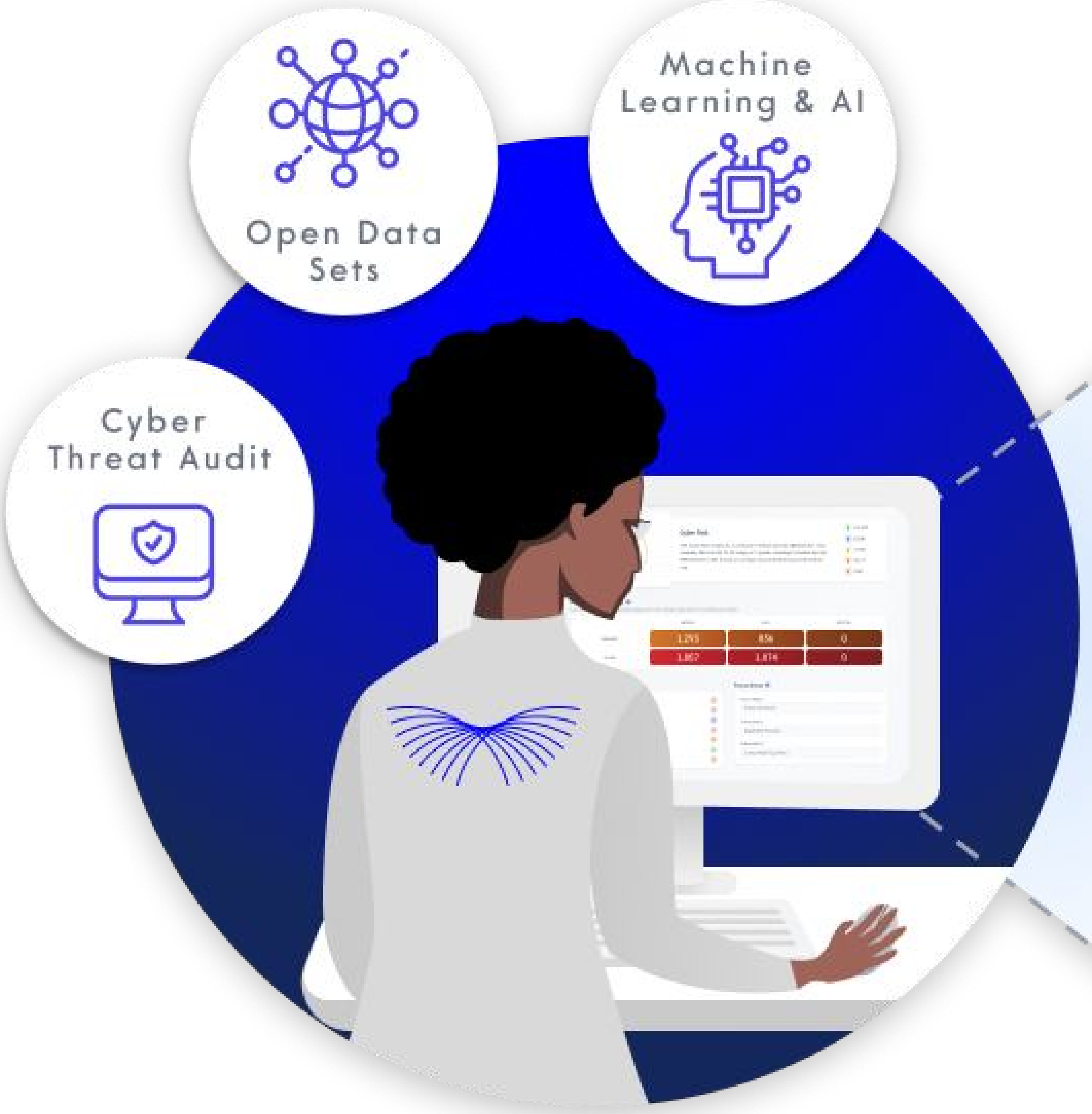
Start with Cyber Risk Monitoring & Prioritization of Risk Indicators

1. Know your sector's threat landscape and vector trends
2. Receive Cyber Risk Scorecard summation report on a quarterly basis
3. Leverage a real-time Red Team Assessment to validate all discovered and sector-wide risks
4. Conduct Dark Net Assessment of obfuscated IP addresses & lost data sets
5. Identify vetted, best of breed solution options to mitigate all validated cyber risks
6. Be accountable to the Leadership, leveraged by the CIO/CISO/IT Team
7. Ensure global reach, while tailoring and scaling to any size organization

Take the Cyber Risk Program Challenge

Implement an independent, expert risk assessment and mitigation strategy from an innovative risk team that utilizes best-of-breed technologies to empower time-sensitive decision making.

Automated, Impactful Cyber Risk Program



WhiteHawk provides you with a hacker's view of your organization's cyber posture, aligned to compliance and resilience frameworks enabling you to enhance defenses against online crime and fraud.

- OT SYSTEMS
- NETWORKS
- SOFTWARE
- PHYSICAL SECURITY

Cyber Threat Audit

Expert, Independent, Hacker View of Risks, Threats - Continuous Digital Age Assessment

Enable IT Managers/CIOs/CSOs/CISOs, and Executive Teams to Understand and Validate:

- ✓ An independent assessment about your organization's cyber resilience in its current state
- ✓ Internal team/managed service provider/security vendor's cyber resilience to know threats and vulnerabilities
- ✓ Where to place your next cyber resilience investment and how to make smart cost reductions
- ✓ How you have accomplished your cyber due diligence and setting risk mitigation resourcing priorities, communicating all to leadership on a quarterly/monthly basis

Key Features

- Independent Cyber Risk Assessment
- Cyber Risk Monitoring
- Pen Testing Red Team Assessment
- Dark Net Reconnaissance
- Actionable Quarterly Executive Level Reviews

Capabilities Statement

WhiteHawk's mission is to automate and scale Cyber Compliance, Maturity and Resilience for Enterprises, Supply Chains and Critical Infrastructure Sectors, by fully leveraging publicly available data sets and AI risk/threat analytics.

Core Competencies

- ENTERPRISE SOLUTIONS Automated Enterprise Cyber Risk SaaS and PaaS Subscriptions
- SMB SOLUTIONS Cost effective Cyber Risk Profile, CMMC, Virtual Consult and Scorecard
- VIRTUAL CONSULTING CMMC Registered Practitioner & Commercial WhiteHawk Cyber Analysts
- TECH LEADERSHIP Vetting of Innovation and Solution Providers
- PRODUCT LINES Cyber Risk PaaS, Cyber Risk Program, Cyber Risk Radar, Cyber Risk Scorecard
- AWS PARTNERSHIP NETWORK Cyber Risk Scorecards and Services via the AWS Marketplace
- DUN & BRADSTREET PARTNERSHIP Dun & Bradstreet Cyber Compliance Powered by WhiteHawk

Key Past Performance

- DOE CIO; ODNI CIO
- DHS CISA
- Federal, State & Local CIO's & CISO's
- Top U.S. Financial Institutions; Top Tier Defense Industrial Base Company
- Global Consulting Groups; Top Tier Global Manufacturers

SMB Clients

- Government Contractors and Suppliers
- Professional Firms (small-to-mid)
- Financial & Insurance Firms Business Clients
- Family Offices

Enterprise Clients

- Federal Contractors and Consulting Firms
- Government Departments and Agencies
- Financial Institutions
- ISPs, MSPs, and MSSPs
- Insurance Groups
- Professional Firms

Influencers

- Sector Professional and Non-Profit Associations
- Client Focused Risk Executives
- Government, Industry, Academia, Cyber, Risk, and Procurement/Supply Chain Executives and Managers
- Risk Professionals: CSO's, CRO's, CISOs
- Sector Social Media: LinkedIn, Facebook

Differentiators

- Online, automated, scalable, and effective cyber risk monitoring and mitigation one-time or continuous service
- Continuous Advancement of SaaS/PaaS Product Lines, with in-house development and data science team
- Continuous access to and integration with Innovative Technologies and Services, via weekly vetting of new solutions
- PaaS and SaaS subscriptions that are globally accessible, impactful and cost-effective solutions, tailorable to organizations and businesses of all sizes
- Virtual Cyber Risk Consults, Automated Assessments and Action Plans, enabling Clients to take smart action immediately
- Make Cyber Resilience Easy and Affordable

The Leadership Team

CHIEF EXECUTIVE OFFICER, PRESIDENT & FOUNDER

Terry Roberts

Cyber Executive across government, academia and industry. Previously Deputy Director of US Naval Intelligence, TASC VP for Intelligence and Cyber, an Executive Director of Carnegie Mellon Software Engineering Institute, Global Cyber Risk Thought Leader, Non-Profit Board Member and Chair with an MSSI in Strategic and Artificial Intelligence.

CHIEF OPERATING OFFICER

Soo Kim

A career Technology Director, Software Architect and Engineer. Previously Cybersecurity, Technology Strategy expert at Accenture Federal Services, Hewlett Packard and TASC VP for Intelligence Group. Over 30 years' experience in technical and business leadership, tactical execution, business operations and solution delivery.

CHIEF TECHNOLOGY OFFICER

Michael Good

Retired Army Cyber Warfare Officer and Technical Program Manager with over 30 years of experience in cyber operations and technology development for military, government, and commercial cybersecurity solutions. Previous assignments include Raytheon, Vencore, L3 Communications and the US Census Bureau.

CHIEF INFORMATION OFFICER

Mike Ferris

A career IT and cybersecurity professional with nearly 20 years of experience, leading cybersecurity initiatives, building IT infrastructure, and managing internal R&D. Previous roles include serving as a Technical Controller in the United States Marine Corps, IT and security positions in healthcare and biotech, and leading major cybersecurity and supply-chain risk programs within the federal government.