WHITEHAWK

October 2020

WHITEHAWK TOP 20 INNOVATIVE CMMC COMPANIES

At a Glance One Pagers CMMC Edition

Cybersecurity Maturity Model Certification (CMMC) Control Mapping Indicated by Cobalt Blue Hyperlink for Each Vendor and Solution
(CMMC Key Provided At End of Publication)

WHITEHAWK

PREVEIL

SOLUTION: Secure email and file sharing for CMMC, ITAR, HIPPA and Financial Services

PROBLEM/PAIN POINT SOLVED: Fastest, most inexpensive way to comply with CMMC (CUI) + ITAR Data Storage and Sharing Regulations **(CMMC Level 1, 4 and 5)**

- PreVeil Email - send and receive encrypted emails using your existing email address
- PreVeil Drive - End-to-end encrypted file sharing and storage, files are automatically encrypted and stored in the cloud
- Admin console that allows IT admins to manage your organization
- Trusted Communities - protect organizations from external phishing and spoofing attacks by selectively whitelisting users

COMPANY OVERVIEW

PreVeil is a cybersecurity company born out of MIT. It provides an end-to-end encrypted email and file sharing system for storing and sharing information subject to CMMC, ITAR, HIPPA and Financial Regulations. The system is differentiated by its strong security, ease of deployment and use. It costs a fraction of the alternative approaches to achieve compliance.

PREVAIL PRICING MODEL

- PreVeil Email & Drive for Gov Community (DIB) - $30 per user, per month billed annually
- PreVeil Email & Drive for Business - $20 per user, per month, billed annually

ADDITIONAL INFORMATION

- Website
- CMMC Information
- Free Download
- CMMC Whitepaper

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SAFERNET
Creating A Safer Internet

SOLUTION: Protecting any device using CyberSafety technology

PROBLEM/PAIN POINT SOLVED: Securing Wi-Fi and Cellular anywhere in the world **(CMMC Level 1)**

- Cloud-Based Dashboard - provides you with a command center for your account and an overview of all activity
- Best-in-class security protects users from all malware, spyware, adware, ransomware, and keyloggers
- Safety Score - each user is given a safety score depending on how safe their activity has been online
- Have complete control over whitelisted/blacklisted websites
- GPS Tracking - track location of devices on your account
- 256-bit Military-grade VPN keeps you safe from attackers and prying eyes

COMPANY OVERVIEW

SaferNet creates the simplest and safest technology that empowers people and organizations to protect themselves online. They believe that everyone has the right to choose how they connect to their digital world without putting their personal habits and information at risk, so they can live the life they hope for with complete freedom and security.

SAFERNET PRICING MODEL

- $3.99 Per Device Per Month

ADDITIONAL INFORMATION

- Website
- App Downloads

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SOLUTION: Protect and defend against most malicious cybersecurity threats

PROBLEM/PAIN POINT SOLVED: Helping organizations improve their cybersecurity posture (CMMC Level 1 and 4)

- **Digital Forensics & Incident Response -** data breaches can be costly events, Impacting your customers and bottom line. Rendition has the forensics expertise to assist in any investigation
- **Red Team & Offensive Based Operations -** Sometimes the best defense is a great offense. Rendition believes that using offensive methods for identifying vulnerabilities and risks will move your company from a reactive model to a proactive one
- **Training -** Rendition provides a line of training offerings based on public/private demand that are offered on campus or in-house
- **Manage/Detection/Response Services -** Rendition operations a 24/7 SOC that focuses on managing client security Infrastructure.

COMPANY OVERVIEW

Rendition is founded and staffed by former NSA, DoD, and US Cyber Command operators. Our unique experiences in some of the most challenging security environments on the planet allow us to provide our clients with unparalleled capabilities to protect and defend against the most malicious cybersecurity threats. After all, who better to find the most dangerous cyber adversaries than those who have been the most dangerous cyber adversaries?

RENDITION INFOSEC PRICING MODEL

- Incident Response Services - $3,500
- Trainings- $3,650.00
- Red Team Assessments - $12,500

ADDITIONAL INFORMATION

- Website
- Blog

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

GETVISIBILITY

SOLUTION: Governance, Risk & Compliance Platform

PROBLEM/PAIN POINT SOLVED: Gain complete situational awareness of extended enterprise environment (**CMMC Levels 1-5**)

- **CMMC Assessment -** Will specifically scan for CUI for CMMC using AI and machine learning to classify unstructured data across large data landscapes
- **Insider Threat -** Detect Insider threats relating to documents and emails before any data leakage occurs using Getvisibility Focus and Getvisibility Synergy
- **Data Classification -** Getvisibility Focus automatically scans and classifies millions of documents
- **Data Governance -** Discovers and catalogues your data under your company's taxonomy and shows the data location
- **Monitoring Data Access -** Focus platform responds to new data or modified data events

COMPANY OVERVIEW

Getvisibility is a leader in the delivery of data visibility and control. Our unified GRC platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environment and Getvisibility helps reduce operational risk to their data. Our products deploy quickly for effective real-time discovery and classification of every piece of data across the network. Leading companies across EMEA and North America now rely on Getvisiblity's infrastructure-agnostic solution to reduce the risk associated with unclassified data. Our job is to ensure and demonstrate data security compliance, improve governance, and reduce risk. We use Getvisibility Focus for legacy data at rest and Getvisibility Synergy at the endpoint level and allows the user to directly integrate with the ML on the classification of documentation on the fly.

GETVISIBILITY PRICING MODEL

- Getvisibility's Core Engine: $40,000
- Additional User Licenses: $60 Per Seat / Per Year (1-500 Licenses)

ADDITIONAL INFORMATION

- Website
- Webinars
- Request a Demo
- Blog

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

RUBICA

SOLUTION: Personal Cybersecurity app for Remote Workers & Virtual Environments

PROBLEM/PAIN POINT SOLVED: Securing the remote workforce (CMMC Level 1)

- **Simple** - Rubica's app Is easy to Install, Intuitive, and protects your mobile devices everywhere
- **Comprehensive -** All devices (iOS, Android, Windows, and Mac) get the same level of protection
- **Effective -** App catches 93% of malware that Is missed by antivirus. Their secure VPN tunnel & threat blocking tools protect your devices, connections, and online data
- **Affordable -** Enterprise-grade protection for a fraction of the cost for teams & remote workers. App does not require any hardware, servers, or IT support.
- **Private -** Browsing history will remain private while still keeping your devices secure

COMPANY OVERVIEW

Rubica is advanced cybersecurity built for ease-of-use and end-user privacy, extending enterprise-grade protection to mixed use devices, personal environments & remote workers. Our advanced threat detection and prevention covers all devices (phones, laptops, tablets) on any network or cell connection, no matter what the user is doing online. Set up is simple: Just download the app. No hardware, integration or IT support needed.

Our personal and work worlds are now blended. This requires a new approach to security which gives users convenience & privacy in their personal activities, but assures the company that there's advanced threat protection covering the device at all times, regardless of whether it's being used for work or personal. This is Rubica.

RUBICA'S PRICING MODEL

- Rubica's app is priced at $10/month per person for both Individuals and teams

Additional Information

- Website
- Enroll Now

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

REYNCON EDUCATIONAL SERVICES & TRAINING

Powered by mindset digital

SOLUTION: Build Awareness and Confidence… FAST

PROBLEM/PAIN POINT SOLVED: Cost Effective Training at Your Own Pace **(CMMC Level 1 and 4)**

- Need to launch a cybersecurity awareness training program right away.
- Want on-going reinforcement to keep secure behaviors top-of-mind.
- Have a distributed (or at home) workforce and need an easy way to send our courses.
- Want effective content—but need an economical solution.

COMPANY OVERVIEW

ReynCon was formed to create a sense of community by bringing together security practitioners and individuals who want to build their skills, whether new to our field, building skills for growth or a more cross-functional skill set.

Cyber Security Training and mentoring is a large part of helping organizations mature their teams and provide deeper knowledge from a business, risk-based approach to the technical details. We take pride for being agile and working closely with our clients, to provide meaningful training to help build their teams capabilities.

REYNCON PRICING MODEL

- Annual subscription $250 (Includes 15 seats)
- Additional seats are $18 per user / per year

ADDITIONAL INFORMATION

- Website
- Course Listing

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

RB ADVISORY

SOLUTION: Pre-Audit Certification, Remediation and Response Services

PROBLEM/PAIN POINT SOLVED: Provides a roadmap to compliance **(CMMC Levels 1-5)**

- Provide a GAP analysis of your processes and procedures and identify the areas that require attention with regard to CMMC requirement
- Remediation recommendations and assistance in the implementation of plans
- Pre-assessment testing and validation
- On-going Managed Security Compliance Services.

COMPANY OVERVIEW

This is not a “one-size fits all” approach. RB Advisory will discover where your business falls within the supply chain and the level of access necessary to Controlled Unclassified Information (CUI). CMMC Level 1 compliance represents "Basic Cyber Hygiene", Level 2 is "Intermediate”, and Level 3 begins to differentiate from the first two sets of controls with a "More Advanced Cyber Hygiene". The overall goal is to fully safeguard Federal Contract Information (FCI) by implementing and maintaining basic cyber essential processes and procedures and map them to the requirements of Federal Acquisition Regulation 52.204-21 (FAR) and NIST 800-171. Your Level 1 compliance will then have to be certified by a licensed, third-party assessor. Self-assessment is no longer valid.

Our services are designed to support your needs, establish readiness for compliance and maintain through your validation process!

RB ADVISORY PRICING MODEL

- The RB Advisory Review is implemented in tiers based on company size and CMMC scope, as an annual audit or over the duration of 36 months.
- IT Remediation and Implementation $225 an hour.

ADDITIONAL INFORMATION

- Website
- Education & Awareness Videos

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SOLUTION: Cybersecurity and IT Risk Management Services

PROBLEM/PAIN POINT SOLVED: Creating a more secure and resilient enterprise environment **(CMMC Levels 1-5)**

- **Virtual CISO -** Take on the role of a client's CISO to advise clients on governance, risk management, security testing, Incident response, 3rd party assurance and supplier audits
- **Cloud Security and Compliance Platform** - allows an organization to monitor their cloud accounts, manage Identity privilege across the cloud, and gain total compliance assurance
- **Cyber Insurance -** Partnered with Cysurance, LLC to provide affordable coverage underwritten by Chubb for risks that most Impact local and regional businesses
- **IT Risk Management and Compliance -** Provides clients with advice on Industry best practices, development, and Implementation of an Information Infrastructure to protect their Information
- **Career Development Training & Certification -** Provides clients with easy access towards training and certification in various standards

COMPANY OVERVIEW

Solvitur Systems is an innovative Information Technology consulting firm specializing in cybersecurity, information assurance, and cloud computing. Our team has experience working with a broad and diverse client base representing a wide range of industries, including Federal, State & Local Government Agencies, Non-Profit Organizations, Telecom & Media, Financial Services, and Information Technology.

SOLVITUR SYSTEMS PRICING MODEL

- Solvitur Systems' pricing starts at $150 per hour

ADDITIONAL INFORMATION

- Website
- Blog

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SOLUTION: Cloud Security Platform for End-to-End Protection

PROBLEM/PAIN POINT SOLVED: Overcoming data privacy, residency, security, and regulatory compliance risks (**CMMC Level 3**)

- **CipherCloud CASB+ -** offers complete visibility of organization's cloud usage, adaptive access control, zero-day threat protection, and regulation compliance
- **Secure Remote Workforce -** Continuously monitor user behavior, protect sensitive data through a DLP Interface and respond in real-time with centralized security controls
- **Cloud Security Posture Management -** reduce operational complexity of managing multiple clouds through a centralized security solution
- **Cloud Encryption Gateway -** seamless encryption/tokenization solution to meet any governance policies or compliance needs
- **Data Loss Prevention -** Cloud DLP allows you to Identify and classify data across all sanctioned cloud applications
- **Digital Rights Management -** applies data protection controls, encryption, and centralized control of sensitive data, even when shared externally

COMPANY OVERVIEW

CipherCloud, the leader in cloud information protection, enables organizations to securely adopt cloud applications by overcoming data privacy, residency, security, and regulatory compliance risks. CipherCloud delivers an open platform with comprehensive security controls, including AES 256-bit encryption, tokenization, data loss prevention, malware detection and visibility tools. CipherCloud's groundbreaking technology protects sensitive information in real time, before it is sent to the cloud, while preserving application usability and functionality.

CIPHERCLOUD PRICING MODEL

- CipherCloud's pricing starts at $25,000 (500 Employees / 2-3 CLoud Environments)

ADDITIONAL INFORMATION

- Website
- Whitepapers
- Request Free Trial
- Blog

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

DOBBS DEFENSE SOLUTIONS

SOLUTION: High-quality IT, Cybersecurity, and Data Analytics Solutions

PROBLEM/PAIN POINT SOLVED: Delivering mission-centric solutions for government and commercial clients (**CMMC Level 3**)

- **Cyber Solutions -** Threat Assessments/Management, Identity and Access Management, Endpoint Security Management, Incident Response, Penetration Testing, Vulnerability Assessment/Management, Assessment & Authorization, and Network Security
- **Business Intelligence -** Data Analytics & Visualization, AI & System Automation, Software Process Assessment, Machine Learning, Dashboard Reporting, AI Decision Management, Business Analytics Dashboard
- **Enterprise IT Services -** Infrastructure Modernization, Project/Program Management, Enterprise Mobility Management, Business Process Management, Enterprise Information Management, IT Helpdesk/CRM, Systems Integration, Customer Application Development, Enterprise Consulting, Digital Transformation

COMPANY OVERVIEW

Our executives and personnel have more than 35 years of proven experience in information technology (IT), cybersecurity, business intelligence (BI), and project/program management (PM). D2S focuses on delivering IT, BI, cyber, and PM capabilities by employing professional services with exceptional results.

We work with government and commercial customers who want to realign their enterprise IT, cyber, and data analytics solutions. We are committed to supporting our customers' missions by investing in an experienced workforce that delivers premier solutions to meet customers' business needs.

DOBBS DEFENSE PRICING MODEL

- Dobbs Defense's pricing starts at $250 per hour

ADDITIONAL INFORMATION

- Website
- Contract Vehicles

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

DEKKO SECURE

SOLUTION: Dekko Online Platform

PROBLEM/PAIN POINT SOLVED: Secure file sharing, document approval, and instant and comprehensive messaging (**CMMC Level 3**)

- **DekkoVAULT** - file sharing with collaboration, granular permissions, sharing expiry, and no size limits
- **DekkoSIGN** - document approval with watermarks, multiple approvers, and commentary and note options
- **DekkoCHAT** - instant group conversations, ability to chat while you work and see who's online. All exclusive to your business
- **DekkoMAIL** - comprehensive messaging with no attachment limit, read receipts, and the ability to revoke mistakenly sent emails.
- **DekkoHUBs** - for facilitating the isolation of teams and projects; setting user availability, eliminating misaddressing, and managing both internal and internal to external workflows
- **DekkoLYNX** - Live video conferencing

COMPANY OVERVIEW

Dekko is a flexible and secure web-based workflow application for documents that are critical and confidential. We believe that everyone has the right to robust and private communication tools. Our mission is to deliver collaborative solution that embody these principles by focusing on replacing high-risk electronic exchanges.

DEKKO SECURE PRICING MODEL

- Dekko Secure Licenses start at: $45 per user

ADDITIONAL INFORMATION

- Website
- Blog
- Dekko Secure launches new data sharing service

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SOLUTION: Comprehensive PAM at cloud scale and speed

PROBLEM/PAIN POINT SOLVED: Manage, Provision and Delegate Privileged Access to Accounts from a Dashboard **(CMMC Level 3)**

- **Secret Server** - Discover privileged accounts, vault credentials, govern service accounts, delegate access, monitor and record sessions
    - Easiest to use and fastest to deploy enterprise-grade privileged access management & governance for organizations of all sizes, with on premise or cloud deployment
- **Privilege Manager -** All-In-one solution for least privilege management, threat Intelligence, and application control.
    - Seamless adoption for security teams, help desk support, and business users
- **Cloud Access Controller -** Authentication, authorization, auditing for anytime, anywhere access to IaaS, SaaS Apps, Databases.
    - Easily grant and revoke access for remote workers and 3rd parties without clients, agents, MFA and session recording for IaaS platforms and SaaS applications.

COMPANY OVERVIEW

Thycotic provides enterprise password management software to the SMB and Enterprise space globally. IT Infrastructure teams at more than 3,000 companies depend on Secret Server every day to manage their privileged passwords.

Secret Server is an encrypted web-based repository for storing privileged accounts like Windows local admin accounts, UNIX root accounts and service accounts. It integrates with Active Directory and can also change passwords automatically on the network. Secret Server is easy to install, manage and fits well into almost any Disaster Recovery plan.

THYCOTIC PRICING MODEL

- Secret Server Cloud Professional: $3,200 for 1 User License

ADDITIONAL INFORMATION

- Website
- Resources
- Interactive PAM Dictionary
- Free Trial

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

Elevate Security

SOLUTION: ANALYZING EMPLOYEE BEHAVIOR TO IMPROVE SECURITY HABITS

PROBLEM/PAIN POINT SOLVED: Preparing workforce to prevent security breaches **(CMMC Level 4 and 5)**

- Gaining insight by measuring, analyzing, and acting on employee's security behaviors w/personalized tools
- **Reflex** - create, run, and analyze phishing campaigns and track improvement over time
- **Pulse** - Personalized scorecards for employees
- **Hacker's Mind** - Motivating employees through gamified security training
- **Vision** - dashboard to see company's security posture at a glance

COMPANY OVERVIEW

Elevate Security has built a people-centric platform to improve employee security behavior and take security awareness to the next level. Elevate uses data analytics and behavioral science to determine what areas your company needs to Improve to be better prepared for security Incidents.

ELEVATE SECURITY PRICING MODEL

- 500 License Annual Subscription: $50,000

ADDITIONAL INFORMATION

- Website
- Innovation Sandbox Presentation
- Watch a Demo
- News

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SOLUTION: Network detection and response platform

PROBLEM/PAIN POINT SOLVED: Turbocharging Incident response to maximize ROI of security operations **(CMMC Level 4 and 5)**

- Gain visibility and understanding of security Incidents Instantly
- Accelerate security Investigations by making everyone on the team an expert analyst
- Capture and analyze entire network traffic and translate into content and behavior aware Intelligence
- Big data repository with scalable capacity to store months of complete Intelligence
- Improve Incident resolution time by empowering SOC and IR teams with efficient tools and workflows to resolve Incidents quickly and effectively

COMPANY OVERVIEW

WireX Systems is a network security company founded to deliver cutting-edge security systems for intelligence agencies globally. Today WireX serves leading enterprises as a key component in their security infrastructure to accelerate incident response, mitigate data theft, and enable everyone within the enterprise to respond to a security alert. Our mission is to deliver the best incident response capabilities so that each member can respond almost instantly.

WIREX PRICING MODEL

- Enterprise Grade Organization: $100,000 Per Year

ADDITIONAL INFORMATION

- Website
- Use Cases
- Request a Demo
- Resource Center

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SOLUTION: Continuously monitor third-party risks and correlate findings to Industry standards

PROBLEM/PAIN POINT SOLVED: Provide full visibility Into a vendor's cyber position **(CMMC Level 4 and 5)**

- 3D Vendor Risk @ Scale - high quality data platform that communicates risk using technical grade, compliance with open standards, and financial Impact (FAIR)
- Financial Impact Report - NormShield calculates the probable financial risk in the case of a cyber breach with the Open Fair standard Value at Risk model
- Compliance Report - NormShield correlates platform findings to Industry standards and best practices
- Self-Risk Assessments - see what hackers know about you by continuously collecting Information in a non-obtrusive way using data collectors, crawlers, honeypots, etc.

COMPANY OVERVIEW

NormShield provides comprehensive Security-as-a-Service solutions focused on cyber threat intelligence, vulnerability management and continuous perimeter monitoring. They harvest cyber threat data from multiple sources and provide actionable intelligence to their customers so they can take preventive measures.

NormShield Cyber Risk Scorecards provide the information necessary to protect business from cyber-attacks. The scorecards provide a letter grade and a drill down into the data for each risk category so that remediation of vulnerabilities can be prioritized.

NORMSHIELD PRICING MODEL

- $995.00 Per Vendor or Supplier Monitored

ADDITIONAL INFORMATION

- Website
- Videos
- Request a Demo
- Blog

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

GURUCUL
PREDICTIVE SECURITY ANALYTICS

SOLUTION: Unified Security and Risk Analytics

PROBLEM/PAIN POINT SOLVED: One Platform for All Cyber Risks: Security, Identity and Fraud (CMMC Level 4)

- **User and Entity Behavior Analytics (UEBA)** - uses big data analytics, AI, and machine learning to Identify unknown threats that would otherwise appear as "normal" activity to rules-based engines
- **Security Orchestration, Automation and Response (SOAR) -** enables risk prioritized automated response workflows to mitigate Identified threats
- **SIEM -** Automate Intelligent responses using risk-prioritized alerts based on a vast library of machine learning models and risk scoring algorithms to scale
- **Intelligent AI/ML Based Threat Hunting** - Wide-range of threat hunting use cases like Insider threat detection, data exfiltration, phishing, endpoint forensics, malicious processes, ransomware detection, and network threat analytics.
- **Log Aggregator -** collection, processing, Indexing and storage of massive datasets for analysis, Investigation, security, and compliance

COMPANY OVERVIEW

Gurucul is a global cybersecurity company that is changing the way organizations protect their most valuable assets, data, and information from insider threats and external cyberattacks, both on-premises and in the cloud. Gurucul's real-time Unified Security and Risk Analytics technology delivers one platform for all cyber risks: security, identity, and fraud. It leverages machine learning behavior profiling with predictive risk-scoring algorithms to predict, detect and prevent data breaches, fraud, and insider threats. It also reduces the attack surface for accounts and eliminates unnecessary access rights and privileges to increase data protection.

GURUCUL'S PRICING MODEL

- Risk Analytics Platform starts at: $56,000

ADDITIONAL INFORMATION

- Website
- Blog
- Request a Demo
- Whitepapers

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SOLUTION: Cloud-based AppGate Software Defined Perimeter (SDP) User Access

PROBLEM/PAIN POINT SOLVED: Access to valuable data for each user **(CMMC Level 4 and 5)**

- Three available SDP versions routinely updating with software subscriptions
- Version 4.1 Supported until 31 January 2020, 4.2 supported, 4.3 fully supported
- Agile, enhanced security, lower cost

Cyxtera's AppGate scans continuously for changes in context and adjusts user access. All monitoring occurs while creating comprehensive logs for compliance reporting. AppGate, like the cloud, is massively scalable, resilient, and distributed on a global level. This cloud-native design allows it to integrate with security features on AWS or Microsoft Azure which cover 69% of the cloud market. AppGate is the solution for any business looking for a simplified network across a changing hybrid environment

COMPANY OVERVIEW

Cyxtera provides datacenters focused on evolving with the needs of enterprise IT and infrastructure security through IT estates, enhanced at all levels through availability, agility, and scalability. AppGate is designed to allow IT departments clearly plan and execute support requirements unique to their organization. AppGate SDP offers various levels of support and enables seamless access to as many cloud regions as reasonably possible.

CYXTERA PRICING MODEL

- SAAS Licenses: $100 Per User Per Year.

ADDITIONAL INFORMATION

- Website
- AppGate

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

SOLUTION: Remediant SecureONE - Precision Privileged Access Management

PROBLEM/PAIN POINT SOLVED: Stopping ransomware by bringing zero trust to administrators **(CMMC Level 4 and 5)**

- **Agentless Deployment -** can be set up as a single virtual or physical appliance, and managed with one headcount
- **Continuous Discovery -** constantly scans for and discovers privileged access across the ecosystem
- **Just-In-Time Administration -** privileged access Is elevated Instantly upon request using the user's own credentials
- **Stop Ransomware -** remove users from administrator groups with a single click
- **State of Privileged Access Reporting -** continuously report on how privileged access risk has evolved over time across the enterprise
- **Real-time SOC Insights -** Integrates with SIEMs to ensure real-time visibility into all privilege escalations

COMPANY OVERVIEW

Remediant provides enterprises with Privileged Access Management (PAM) software to help them protect their accounts from misuse and abuse. It enables real-time monitoring, zero trust protection of privileged accounts and Just-In-Time Administration (JITA) across IT/Security ecosystems. Its product, SecureONE, a next-generation Privileged Access Management (PAM) solution that dynamically allocating privileged access across Windows, Linux, and Mac systems — without installing an agent.

REMEDIANT PRICING MODEL

- $45 Per Endpoint

ADDITIONAL INFORMATION

- Website
- CMMC Compliance
- Free Trial
- Blog

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

VIRESCIT TACTICAL SYSTEMS
A WHOLLY OWNED SUBSIDIARY OF WiSC ENTERPRISES

SOLUTION: SPECIALIZE IN FULL-SPECTRUM CYBERSECURITY

PROBLEM/PAIN POINT SOLVED: Customized Security Solutions Including Training & Certifications (**CMMC Level 4**)

- **Software Design & Testing -** extensive bench of capability to provide direct network and systems security architecture from the enterprise level down
- **NIST|Risk Management Framework (RMF) Training & Certification -** Self-paced online learning course for cybersecurity and IT professionals
- **Virtus 1 Program -** allows remote, real time access to strategic and tactical Information
- **SEPT Program -** Vulnerability & Threat Assessment, Soft Skills Training & Policy, Insider Threat Policy & Programs, APT Mitigation, Critical Risk / Vulnerability Management, Short to Long Term Programs
- **Managed Services -** provides compliance validation specialty teams in support of the customer's specific needs

COMPANY OVERVIEW

We provide unique offerings and enduring solutions that support the key categories of Information Technology and Systems. From Cyber Security and Mobile Connectivity, to Operational Engineering and Penetration Testing, we wear the hat you need for the mission you have…and the mission you'll have next!

In order to provide the absolute best cybersecurity capabilities, VTS employs only experts. Everyone at VTS has performed their jobs in the real world, many for more than twenty years. Our personnel are true "subject-matter experts", with very challenging and often unique experiences dealing with the most complex adversaries in the US and abroad.

VTS CYBER PRICING MODEL

- VTS Risk Management Framework Training Courses: $2,995.00

ADDITIONAL INFORMATION

- Website

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

WHITEHAWK

SOLUTION: Cyber Risk Radar – Automated Path to CMMC for Vendors/Suppliers

PROBLEM/PAIN POINT SOLVED: Monitoring, Prioritization & Mitigation of Supply Chain/Vendor Cyber & Business Risks (CMMC Level 3)

- Supply chain business and cyber risk discovery and prioritization in near real-time
- Enables large and small SCRM, CIO, CMMC and capture teams to track all risks, vendor engagement and risk mitigation and documentation, enabling comprehensive compliance
- Provides actionable, sourced, & prioritized risk indicators mapped to your priorities
- Delivers scorecards and action plans, establishing risk baselines & documenting progress

The WhiteHawk Cyber Risk Radar automates supply chain risk discovery, prioritization and smart action, via the integration of state-of-the-art Software as a Service (SaaS) platforms, efficiently and effectively meeting all regulatory regimes and enabling to all business lines as appropriate, via one interactive, access controlled Executive VRM dashboard.

COMPANY OVERVIEW

WhiteHawk, Inc., is the first product agnostic, online Cybersecurity Exchange, based on a platform architecture that leverages publicly available data sets and Artificial Intelligence (AI)-based analytics, with a focus on identifying, prioritizing, and mitigating cyber risks - for businesses and organizations of all sizes, with demonstrated cost and time savings.

WHITEHAWK PRICING MODEL

- Customizable solution with three levels of service depending on criticality of suppliers and enterprise SCRM and CMMC needs.
- Cyber Risk Radar starts at $375 per supplier/vendor for an annual subscription.

ADDITIONAL INFORMATION

- Website
- Watch a Demo
- Cyber Risk Radar White Paper
- WhiteHawk TVWorldwide Interview

CONTACT

For questions or additional Information, contact WhiteHawk at: consultingservices@whitehawk.com or via phone at 833-942-9237

Schedule an appointment.

WHITEHAWK

Cybersecurity Maturity Model Certification (CMMC) Key

LEVEL 1 CONTROLS

Access Control

AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
AC.1.003	Verify and control/limit connections to and use of external information systems.
AC.1.004	Control information posted or processed on publicly accessible information systems.

Identification and Authentication

IA.1.076	Identify information system users, processes acting on behalf of users, or devices.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Media Protection

MP.1.118	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

Physical Protection

PE.1.131	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
PE.1.132	Escort visitors and monitor visitor activity.
PE.1.133	Maintain audit logs of physical access.
PE.1.134	Control and manage physical access devices.

System and Communications Protection

SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

System and Information Integrity

SI.1.210	Identify, report, and correct information and information system flaws in a timely manner
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.
SI.1.212	Update malicious code protection mechanisms when new releases are available
SI.1.213	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

LEVEL 2 CONTROLS

Access Control

AC.2.005	Having log on screen display notices upon initial login, display the system use information before granting access, referencing monitoring, recording, or auditing consistent with privacy accommodation.
AC.2.006	Placing restrictions on the use of portable storage devices such as thumb drives, imposing restrictions on authorized individuals regarding the use of company controlled removable media on external systems.
AC.2.007	Only granting enough privileges to users to allow them to do their jobs. Restricting access to privileged functions and security information to authorized employees.
AC.2.008	Having users with multiple account log on with the least privileged account when not performing privileged functions, making sure that this can be described or demonstrated.
AC.2.009	Lock the computer or account after a certain number of failed log-on attempts.
AC.2.010	Configuring the system to lock sessions after a predetermined period of inactivity, using pattern hiding displays when sessions are locked, giving users the option to lock sessions for temporary absence.
AC.2.011	Approving the use of wireless technologies by company management, having established guidelines for the use of wireless technologies, and monitoring wireless access to the system.
AC.2.013	Running network and system monitoring applications to monitor remote system access and log, accordingly, controlling remote access by running only necessary applications, using firewalls and end-to-end encryption.
AC.2.015	Allowing remote access only by authorized methods, maintained by one department, and route all remote access through a limited number of managed access control points.
AC.2.016	Having solutions to control the flow of system data, as well as documenting information flow control. This can include implementing firewalls and encryption to block outside traffic and restrict web requests to the internet that are not from the internal web proxy server.

Audit and Accountability

AU.2.041	Keeping track of network activity to individual users and being able to trace accountable users for unauthorized actions to protect against a user denying having performed an action.
AU.2.042	Having system provide alert functions and performing audit analysis/review through mechanisms in place. Retaining information audit records between 30 days to 1 year depending on data.
AU.2.043	Make the system use internal system clocks to generate time stamps for audit records. Having those time stamps be mapped to Coordinated Universal Time (UTC) and compare system clocks with Network Time Protocol (NTP) servers that synchronizes the clocks on a defined frequency.
AU.2.044	Review system and audit logs to keep track of what users have performed activities.

Awareness and Training

AT.2.056	Having employees complete annual training about their roles and responsibilities pertaining to information security and procedures related to the security of the system, as well completing security awareness training.
AT.2.057	Same as above, but with an emphasis for employees with security specific roles and more technical training such as identifying suspicious email or web communications.

Configuration Management

CM.2.061	Having baseline configurations documented and maintained for each information system type, as well as updating these as needed to accommodate security risks or software changes and having it approved by a CISO or equivalent. Using a system development lifecycle methodology that includes security considerations.
CM.2.062	Configuring system to exclude any function not needed in the operational environment and having system employ processing components that have minimal data storage such as diskless nodes. In certain systems, having it deliver one function when practical.
CM.2.063	Placing user controls to prohibit the installation of unauthorized software, ensuring all software use on the system is approved, and having user-installed software operated with limited privileges.
CM.2.064	Having security baseline configurations that reflect the most restrictive appropriate settings and documenting any changes or deviations.
CM.2.065	Documenting changes to the system that are authorized by company management, auditing these changes, and tracking changes through an IT service management system or equivalent tracking service.
CM.2.066	Testing changes that affect the system security requirements prior to the implementation, the effectiveness of the changes, and ensuring that these changes are compliance- approved and documented.

Identification and Authentication

IA.2.078	Require employees to have at least 12 characters in their passwords and include numbers, upper/lowercase, and special characters.
IA.2.079	Do not let employees re-use previous passwords.
IA.2.080	Requiring employees to create a new password during the hiring process from their initial generated passwords. Ensuring that temporary password activation links are sent to employees when a password change is required and only used for a password reset.
IA.2.081	Having passwords that cannot be reverse encrypted, using hashes and salts, and making sure passwords are encrypted in storage and in transmission.
IA.2.082	When a user types authentication information such as a password, it should show up as dots on the computer screen. Also, if a user inputs a wrong field of information. It should not specify that it was “Wrong password”, or “Wrong username.”

Incident Response

IR.2.092	Establishing an incident response policy that specifically outlines requirements for handling incidents involving CUI that include preparation, detection, analysis, containment, eradication, and recovery.
IR.2.093	Have a system set in place such as an Intrusion Detection system to detect and report suspicious activity.
IR.2.094	Have a plan set in place to categorize and prioritize events and handle them as appropriate.
IR.2.096	Write procedures ahead of time when responding to incidents depending on the type of incident. Responses should prevent or contain the impact of an incident

	while it is occurring or shortly after.
IR.2.097	Examining the causes of the event or incident and how your organization responded to it by looking at administrative, technical, and physical control weaknesses that may have allowed the incident to occur. Making improvements after examining by updating plans.
Maintenance	
MA.2.111	Managing IT system maintenance tools such as diagnostics and patching tools and supporting systems and devices per manufacturer recommendations. Maintenance should be performed on the system and has to be approved by management.
MA.2.112	Placing controls that limit the tools, and resources that employees use to maintain the system and devices. This may include authorized tools, employees, or techniques and settings.
MA.2.113	Requiring multifactor authentication for remote access to a system and ensuring that the connections are terminated when the session is completed.
MA.2.114	Ensuring all activities of maintenance personnel are monitored and that the company has defined methods for supervision.
MA.2.119	
Media Protection	
MP.2.119	Having responsible parties for the data in the systems document and ensure proper authorization controls for data in media and print, securely storing system media in protected areas, making sure only approved individuals have access to media from CUI systems, and removing the audit log of any media from these systems.
MP.2.120	Managing all CUI systems under least access rules and limiting CUI media access to authorized users.
MP.2.121	Restricting the use of writable and removable media on the system.
Physical Security	
PS.2.127	Ensuring that individuals are screened before granting them access to any systems that contain CUI.
PS.2.128	Disabling information system access prior to employee termination, retrieving all company information and property from terminated or transferred employee, reviewing electronic and physical access permissions when employees are reassigned or transferred.
Physical Protection	
PE.2.135	Having the facility manager review the location and type of physical security in use such as locks, card readers, etc., and evaluating the suitability for the company's needs.
Recovery	
RE.2.137	Back up organizational data often. Test these backups by verifying that the operating system, application, and data are intact and functional.
RE.2.138	Encrypting data backups on media before removal from a secured facility, protecting the confidentiality and integrity of backup information at the storage location, and having cryptographic mechanisms that comply with FIPS 140-2 (Security Requirements for Cryptographic Modules.)
Risk Management	
RM.2.141	Establishing a risk management policy, conducting initial and periodic risk assessments, documenting and assessing changes in use or infrastructure.

RM.2.142	Performing vulnerability scanning periodically for common and new vulnerabilities. Creating reports regarding the scans for company management and keeping documentation.
RM.2.143	Creating an action plan for remediation, acceptance or avoidance upon recognition of any vulnerability. Prioritizing high vulnerabilities and including a reasonable time frame for implementation.

Security Assessment

CA.2.157	Ensuring that security plans are consistent with the company's enterprise architecture, authorization boundaries, operational context, operational environment, and security requirements.
CA.2.158	Conducting periodic security assessments to ensure that security controls are implemented correctly and meet security requirements. This includes vulnerability scanning, pen testing, log reviews, and speaking with company employees.
CA.2.159	Developing an action plan to remediate identified weaknesses or deficiencies that designates remediation dates for each item.

System and Communications Protection

SC.2.178	Configuring collaborative computing devices so they cannot be remotely activated, having users notified when collaborative computing devices are in use.
SC.2.179	When accessing devices over the network, you should use a secure encryption method such as Secure Shell (SSH).

System and Information Integrity

SI.2.214	Having the company receive security alerts, advisories, and directives from reputable external organizations, responding to alerts in a timely manner, and generating internal security alerts.
SI.2.216	Monitor system to detect attacks as well as unauthorized local, network, and remote connections. Deploy monitoring devices to collect information and monitor inbound and outbound communications for unusual activity.
SI.2.217	Monitoring the system to identify unauthorized access and use and log monitoring.

LEVEL 3 CONTROLS

Access Control

AC.3.012	Require passwords before allowing access to wireless networks.
AC.3.014	Enable employees to establish configurations to protect the confidential needs of work done remotely.
AC.3.017	Divide responsibilities among individuals.
AC.3.018	Only let those with authorized access perform privileged functions with classified and sensitive information.
AC.3.019	Have a reaction to end a user's session when a condition set in place is triggered.
AC.3.020	Only allow authorized mobile devices to connect to wireless networks.
AC.3.021	Restrict those who have privileged access, including when they can access and from where.
AC.3.022	Ensure CUI is disguised on mobile platforms.

Asset Management

AM.3.036

Audit and Accountability

AU.3.045	Keep events updated and frequently review and verify them.
AU.3.046	Report any failures in logging the audit process.
AU.3.048	
AU.3.049	Have secure backups in place to protect information from being manipulated or removed.
AU.3.050	Limit access to audit logging functionality to authorized users.
AU.3.051	Have an established reviewing and reporting process for incident response and suspicious activity.
AU.3.052	Implement a SIEM with built-in AI or rules that will be able to filter your audit logs into meaningful reports.

Awareness and Training

AT.3.058	Enable entire employee base to report and recognize insider threats through routine security awareness training.

Configuration Management

CM.3.067	Have a policy in place that defines restrictions and requirements for logical access and update it regularly.
CM.3.068	Restrict programs to only those essential to the desired functions; to minimize outside threats.
CM.3.069	Explicitly deny all but authorized users to access certain software.

Identification and Authentication

IA.3.083	Enable multifactor authentication across all authorized users before granting network access.
IA.3.084	Promote policies such as Transport Layer Security (TLS) before providing network access to any accounts.
IA.3.085	Change passwords or user identifications frequently to prevent them from being compromised.
IA.3.086	Remove access from unused identifiers.

Incident Response

IR.3.098	Identify, record, and report all incidents to any authorized authorities in house and if necessary, legal authorities.
IR.3.099	Send tests such as fake phishing attempts to evaluate the quality of incident response.

Maintenance

MA.3.115	Adopt a clean desk policy.
MA.3.116	Verify devices on a separate system before allowing media to be run on organizational systems.

Physical Protection

PE.3.136	Ensure safeguarding standards are established and enforced across all work locations.

Recovery

RE.3.139	Back up organizational data often. Test these backups by verifying that the Operating system, application, and data are intact and functional.

Risk Management

RM.3.144	Develop an action plan to remediate identified weaknesses or deficiencies that designates remediation dates for each item.

RM.3.146	Have a policy in place that enables your business to prioritize, identify, and mitigate risk.
RM.3.147	Keep products not supported by your supply chain separate and restrict access to minimize risk.

Security Assessment

CA.3.161	Run network and system monitoring applications to monitor remote system access and log, accordingly. Control remote access by running only necessary applications and use firewalls and end-to-end encryption.
CA.3.162	Conduct periodic security assessments to ensure security controls are implemented correctly and meet security requirements. Include vulnerability scanning, pen testing, log reviews, and speaking with company employees during these assessments.

Situational Awareness

SA.3.169	Have an incident response plan established and train necessary personnel.

System and Communication Protection

SC.3.177	Ensure any hardware or software cryptographic module implements algorithms from an approved FIPS list.
SC.3.180	Build all software and technical innovations with security included in the planning.
SC.3.181	Divide responsibilities among individuals dependent on functionality.
SC.3.182	Establish gateways and restrictions for information transfer and establish secure teams within the online workspace.
SC.3.183	Explicitly deny all but authorized users which fill an established criterion to access certain software.
SC.3.184	Ensure a valid Business Associate Agreement (BAA), which requires the third parties to verify the remote workstations are protected. Internal employees and contractors should have an established Acceptable Use Policy (AUP) that outlines the acceptable use of equipment.
SC.3.185	Enable two-factor authentication, firewalls, or other virtual safeguards, if media is not already physically contained.
SC.3.186	Remove access from unused identifiers
SC.3.187	When accessing devices over the network, you should use a secure encryption method such as SSH.
SC.3.188	Only use mobile code on trusted sites in line with company policy.
SC.3.189	Only use VoIP technology on trusted sites in line with company policy.
SC.3.190	Ensure all parties in communication sessions are authorized and are who they say they are.
SC.3.191	Ensure classified information is stored in a safe location.
SC.3.192	Use the DNS to block malicious websites and filter out harmful or inappropriate content. Ensure company data remains secure and controls what employees can access on company-managed networks.
SC.3.193	Have clear policy guidelines forbidding the use of anything labeled as CUI to be posted on any websites not owned by the company.

System and Information Integrity

SI.3.218	Employ spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.

SI.3.219	Use different engines, protocols, and software, such as anti-spam, anti-virus, SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) and DMARC (Domain-based Message Authentication Reporting & Conformance) to protect from forgery.
SI.3.220	Use an email protection software like Barracuda to filter spam or malicious emails.

Media Protection

MP.3.122	Ensure CUI is distinguished, clearly marked, and only distributed to necessary audiences.
MP.3.123	Ensure all storage devices and flash drives are identified and assigned to an authorized owner.
MP.3.124	Know who has access to CUI media and who is responsible for keeping access secured in and outside of controlled areas.
MP.3.125	Enable two-factor authentication, firewalls, or other virtual safeguards if media is not already physically contained.

LEVEL 4 CONTROLS

Access Control

AC.4.023	Implement network segmentation specific to data classification zones. Set user permissions on files containing CUI.
AC.4.025	Have a schedule in place to review the current CUI program and if necessary, change who has access to CUI program.
AC.4.032	Only granting authorized individuals' external access, placing guidelines on the use of personally owned or external system access, and limiting the number of access points to the system to better monitor network traffic.

Asset Management

AM.4.226	Having a capability in place that can identify attributes of a specific system's components such as OS information and firmware.

Audit and Accountability

AU.4.053	Automate the process of scanning audit logs for tactics, techniques, and procedures and identify and prioritize any suspicious activity.
AU.4.054	Review all audit information at a broad and specific level to get a holistic view of activity.

Awareness and Training

AT.4.059	Ensure awareness training is focused on recognizing and responding to persistent adversaries and social engineering threat vectors such as phishing. Review and update training annually.
AT.4.060	Design and practice realistic cyber threat scenarios to provide individuals with real hands-on experience.

Configuration Management

CM.4.073	Ensure you have an application review process in place before allowing the installation of software on company-owned assets.

Incident Response

IR.4.100	Apply realistic attack methodologies and concepts when updating or executing the procedures of incident response.
IR.4.101	Ensure that your organization has a 24/7 security operations center in place to respond to incidents promptly.

Risk Management

RM.4.148	Ensure that there is a documented plan for managing and mitigating supply chain risk that Is reviewing on an annual basis.
RM.4.149	Keep records of tactics, techniques, and practices of threat actors updated.
RM.4.150	Utilize information about cyber threat actors to keep the system and security structure up to date and apply that Information to Increase Information security maturity.
RM.4.151	Have a plan to perform vulnerability scans over the network environment, from outside and inside perspectives, on a regular scheduled basis.

Security Assessment

CA.4.163	Updating information system protection mechanisms within five days of new releases and completing these updates with configuration management policy and procedures.
CA.4.164	Performing periodic penetration testing of the system for malware and other vulnerabilities as defined in company policy, performing real-time scans of files from external sources, and disinfecting or quarantining infected files.
CA.4.227	Perform scheduled red team assessments of your organizational assets to understand the strength of its defense against threat actors

Situational Awareness

SA.4.171	Have a method or program in place to identify, prioritize, and mitigate cyber threats that have evaded controls from level 3.
SA.4.173	Create centralized system capabilities to be able to share and integrate IoC's

System and Communications Protection

SC.4.197	Separate assets within the system to ensure that users can control which users can access, view, or modify policies and resource
SC.4.199	Only allow access to secure domains by restricting requests from known malicious domains or any server that is not "HTTPS."
SC.4.202	Use a testing environment in a virtual machine, for example, to isolate any code changes that have not yet been tested in a way that is risk-free from compromising any systems
SC.4.228	Keep access to high-value information within the network and available to authorized personnel only
SC.4.229	Create a blacklist of unauthorized websites that you could restrict access to when connected to the network.

System and Information Integrity

SI.4.221	Utilize information about cyber threat actors to keep the system and security structure up to date with means to effectively secure yourself from adversaries with techniques and mitigations from other organizations.

LEVEL 5 CONTROLS

Access Control

AC.5.024	Record all authorized devices connected to the network and identify any unauthorized connections

Audit and Accountability

AU.5.055	Ensure all assets have a security-relevant record, a source for those records, and the sequence of activities involved recorded. Identify any assets not following that procedure and make corrections

Configuration Management

CM.5.074	Read the terms of agreement for all software essential to the organization or its security and verify that the inner mechanisms can be trusted to use.
Incident Response	
IR.5.102	Combine human and machine capabilities to ensure a timely and effective response to incidents.
IR.5.106	Collect data in a way that can protect authorized users and identify where, on what device, and who was responsible for any cyber incidents that may have occurred.
IR.5.108	Place personnel in charge of responding and investigating cyber incidents both in-person and remote within 24 hours of its occurrence
IR.5.110	Perform drills to test personnel knowledge and effectiveness in following procedures.
Recovery	
RE.5.140	Use facilities that can be trusted and secure under the definition of the organization's requirements.
Risk Management	
RM.5.152	For software not on the whitelist, have a procedure in place that minimizes defined risk.
RM.5.155	Routinely test security solutions with anticipated risk scenarios to measure its effectiveness in incident response.
System and Communications Protection	
SC.5.198	Setup boundaries within the network to record packets as they pass through from checkpoint to checkpoint and monitor for consistency.
SC.5.208	Have in and out of house protections in place to enhance security capabilities and protections.
SC.5.230	Enforce protocol compliance by properly configuring your IDS/IPS and develop a policy that outlines the tools used.
System and Information Integrity	
SI.5.222	Implement Endpoint detection and response software. These tools continuously monitor the system for any scripts or code that could lead to malicious actions.
SI.5.223	Implement a User and Entity Behavior Analytics service that continuously monitors individuals and systems for any unusual behavior that may be indicative of malicious behavior.