Cybersecurity Capabilities

Back to Cybersecurity Grants

Introduction

The following list identifies the prioritized cybersecurity capabilities available under the State Term Contract (STC) No. 43230000-24-STC, Digital Security Solutions. These offerings are designed to support a range of cybersecurity needs. Review the list to identify which capabilities align with your current priorities.

1. External-Facing Asset Discovery
2. Endpoint-Based Asset Discovery
3. Network-Based Asset Discovery
4. Endpoint Detection & Response (EDR)
5. Content Delivery Network
6. Security Operations Platform
7. Email Security
8. Identity Access Management (IAM)
9. Secure Access Service Edge (SASE)
10. Vulnerability Assessment and Management (VAM)
11. Data Security
12. Secure Information Sharing Platform

1. External-Facing Asset Discovery:

Description: An internet-facing attack surface discovery tool which provides a continuously updated inventory and vulnerability scanning of all global internet-facing assets to detect on-premises and cloud systems.

Solution Providers:

- Axonius Cybersecurity Asset Management
- BlueVoyant Standard Vulnerability Scanning
- Check Point - Infinity External Attack Surface Management
- CrowdStrike
- DarkTrace/Attack Surface Management
- Divergent External Facing Asset Discovery
- External-Facing Asset Discovery Services and Technology
- ExtraHop RevealX 360
- Fortinet FortiRECON
- Google Mandiant Advantage Attack Surface Management
- Invicti Enterprise
- Ivanti Neurons for External Attack Surface Mgmt
- Lumen Managed External Attack Surface Management
- NetWatch.Ai
- Palo Alto Networks - Cortex Xpanse
- Recorded Future
- Shodan Corporate
- Tenable.ASM (Attack Surface Management)
- Tenable.IO - Vulnerability Management
- Trend Micro Vision One Attack Surface Risk Management (ASRM)
- Wiz Advanced

2. Endpoint-Based Asset Discovery:

Description: A solution focused on infrastructure which discovers network connected devices and provides a comprehensive inventory of hardware and software assets across your enterprise. Agents are typically deployed to all laptop, desktop, and server devices.

Solution Providers:

- Axonius Cybersecurity Asset Management
- BlueVoyant Platform Bundle MDR, SIEM and Vulnerability Scanning
- CrowdStrike Falcon Discover
- Divergent Endpoint Asset Discovery
- Elastic
- Skyline Endpoint-Based Asset Discovery Services and Technology
- Forescout Technologies Inc.
- Fortinet FortiClient/EMS FortiNAC
- Heimdal Advanced Vulnerability Management Solution
- Ivanti
- LevelBlue USM
- Lumen Manage Cybersecurity Asset Management
- N-able N-central Remote Monitoring and Management (RMM)
- Netwatch.ai
- Omnissa Workspace ONE
- Open Text, Corp.
- SentinelOne - Singularity Vulnerability Management
- SEPIO
- Tanium
- Tenable.IO - Vulnerability Management
- ServiceNow Discovery, SecOps, ITAM, and ITOM
- Trend Micro Vision One Attack Surface Risk Management (ASRM)

Go Back to Top

3. Network-Based Asset Discovery:

Description: A solution providing enterprise visibility into managed, unmanaged and Internet of Things (IoT) devices discovered via network traffic.

Solution Providers:

- Akamai Technologies
- Armis Centrix
- Axonius Cybersecurity Asset Management
- BlueVoyant Standard Vulnerability Scanning
- Check Point Infinity Network Detection and Response (NDR)
- Cisco Identity Services Engine (ISE)
- Darktrace/NETWORK
- Divergent Network-Based Asset Discovery
- ExtraHop RevealX 360
- Forescout Technologies, Inc.
- Fortinet FortiNAC
- Infoblox
- ServiceNow Discovery and SecOps
- Ivanti Neurons
- LevelBlue USM
- Lumen Managed Network Based Asset Discovery
- NetSkope One
- NetWatch.Ai
- Palo Alto Networks - NGFW IoT Cloud Delivered Security Service
- Solarwinds
- Tanium Inc. Core Platform
- Tenable Vulnerability Management
- Zscaler Zero Trust Network Segmentation

4. Endpoint Detection & Response (EDR):

Description: An agent deployed to each endpoint (including desktops, laptops, and servers), runs autonomously on each device and monitors all processes in real-time to provide enterprise visibility, analytics, malware defense, and automated response.

Solution Providers:

- Barracuda XDR Managed Endpoint Security
- BlueAlly Managed XDR
- BlueVoyant XDR Bundle (MDR+SIEM)
- Broadcom - Symantec Endpoint Security (SES)
- Carbon Black EDR by Broadcom
- SecOps, TISC, Orchestration, 3rd-party EDR tool
- Check Point Harmony Endpoint
- Cisco Secure Endpoint
- CrowdStrike Falcon Complete for Endpoint Detection and Response
- CyberArk Endpoint Privilege Manager (EPM)
- Cylance Endpoint Security
- Darktrace/ENDPOINT
- Dell MDR
- Elastic
- Fortinet FortiEDR
- Halcyon Tech
- Heimdal Unified Endpoint Detection & Response Solution
- HighWire EDR Managed Service
- Managed Endpoint Detection and Response (MEDR) - Qualys Multi Vector
- Microsoft, Azure, MS Defender/SentinelOne
- MixMode Endpoint Detection and Response
- N-able Endpoint Detection and Response (EDR)
- Palo Alto Networks - Cortex XDR
- Proofpoint - Identity Threat Detection and Response
- Secureworks, inc. (Secureworks) – XDR
- SentinelOne - Singularity Complete, Vulnerability Management, and Vigilance
- Sophos - Intercept X Advanced with XDR
- Tanium Inc. Core Platform
- ThreatSpike
- Trellix TRX/MV6
- Trend Micro Vision One Endpoint Security

Go Back to Top

5. Content Delivery Network:

Description: Software, including web application firewall, to manage and secure enterprise websites and APIs against DDoS and targeted web app attacks while fending off adversarial bots and detecting client-side script attacks.

Solution Providers:

- Akamai Technologies
- Cloudflare CDN
- F5 Distributed Cloud (XC)
- Fortinet FortiADC
- Fortinet FortiWEB Cloud

6. Security Operations Platform:

Description: Providing 24/7/365 monitoring and initial incident investigations to augment your security team.

Solution Providers:

- Arctic Wolf Managed Detection and Response
- Avertium (MXDR Services for Existing Microsoft users)
- Barracuda XDR
- BlueAlly Managed Security Operations Platform
- BlueVoyant XDR Bundle (MDR + SIEM)
- Check Point Infinity MDR
- Cisco XDR
- Cloudflare Dashboard
- Critical Start - Cyber Operations Risk and Response Platform
- CrowdStrike Falcon for Security Operations Platform

Darktrace

- Dell MDR
- Dynatrace
- Elastic
- ExtraHop Networks RevealX
- Forescout Technologies, Inc.
- Fortinet FortiAnalyzer, FortiSIEM, FortiSOC
- Google Mandiant
- Google Security Operations (SecOps)
- Heimdal Security Operations Platform Solution
- HighWire Networks SOC Managed Service
- Hosted FortiSIEM
- Infoblox
- Legato Security (Legato) - Security Operations Center as a Services (SOCaaS)
- LevelBlue USM
- Presidio Managed Detection and Response
- MixMode Security Operations Platform (SOP)
- NetWatch.Ai
- Palo Alto Networks - Cortex XSIAM
- Proofpoint Identity Threat Detection and Response
- ReliaQuest GreyMatter
- RSM Defense
- Secureworks, inc. (Secureworks) - Taegis XDR
- Semperis Directory Services Protector & Active Directory Forest Recovery
- Snowflake - Security Operations Platform
- Sophos MDR
- Splunk - Security Operations Platform
- Tanium - Secuirty Operations Platform
- Tenable.ONE
- ThreatBoard - Security Operations Platform (SOP) SaaS
- Trellix XDR/Helix
- Trend Micro Vision One

Go Back to Top

7. Email Security:

Description: Protects your email accounts from threats such as phishing attacks and malware.

Solution Providers:

- Abnormal Security
- Barracuda Email Protection
- BlueVoyant Microsoft Content Delivery
- Check Point - Harmony Email and Collaboration (HEC)
- Cisco Secure Email
- Cloudflare Email Security
- Darktrace/EMAIL
- NWN Enterprise Email Security
- Forcepoint Email Security
- Fortinet - FortiMail and FortiSandbox
- Heimdal Advanced Email Security Solution
- IRONSCALES
- Lumen Managed Email Security
- Microsoft Defender for Office 365
- Mimecast Email Security - Cloud Gateway
- Omnissa Workspace ONE
- OpenText
- Proofpoint - Email Security Protection (Proofpoint on Demand)
- Proofpoint - Tessian Adapative Email Security
- Sophos Email Advance
- Trellix ETP/Email Security
- Trend Micro Vision One Email & Collaboration Security
- XQ Msg

8. Identity Access Management (IAM):

Description: Products or services responsible for providing centralized management for digital identities and control access to systems and data based on organizational policies.

Solution Providers:

- Akamai Technologies
- Avertium : IAM services for existing Microsoft Users
- Beyond Identity
- Cisco Identity Services Engine
- CrowdStrike Identity Threat Detection and Response
- CyberArk Identity
- Fortinet FortiAUTHENTICATOR
- IBM, Inc. Verify
- Microsoft Entra ID
- Okta Identity and Access Management (IAM) and Privileged Access Management (PAM) - Workforce Identity Cloud
- Omnissa Workspace ONE
- One Identity Safeguard and OneLogin
- Proofpoint Identity Threat Detection and Response
- RSA
- SailPoint Identity Security
- Stellar IT Solutions: SAML, OpenID, Oracle

Go Back to Top

9. Secure Access Service Edge (SASE):

Description: Products or services responsible for combining networking and security services, and delivering both through a cloud-based framework that supports remote users, branch offices, and cloud applications.

Solution Providers:

- Akamai Technologies
- Barracuda SecureEdge
- Broadcom - Symantec Secure Access Service Edge
- Check Point Harmony Connect (SASE)
- Cisco Secure Access
- Cloudflare One
- Dell Services: Zscaler with Zero Trust Services – Security, Software, Design and Configuration
- Forcepoint
- Fortinet FortiGate, FortiSASE, FortiClient
- HighWire Networks SASE Managed Service
- Island Enterprise Browser, Island Technologies
- Lumen Managed SASE (Fortinet)
- Lumen Managed SASE (Versa)
- Netskope One
- Palo Alto Networks Prisma Access
- Skyhigh Security Service Edge
- Versa Networks SDWAN and Verson Networks SSE
- Zscaler Zero Trust Exchange

10. Vulnerability Assessment and Management (VAM):

Description: Products or services responsible for enabling organizations to continuously scan their IT assets for security vulnerabilities, to evaluate the risks associated with these vulnerabilities, and to prioritize remediation efforts.

Solution Providers:

- Armis VIPR Pro
- Axonius Cybersecurity Asset Management
- BlueAlly Managed Vulnerability Assessment and Management
- Check Point Infinity Vulnerability Management

- Cortex XSIAM
- Critical Start Vulnerability Management Services
- CrowdStrike Falcon Spotlight
- Dell MDR Vulnerability Management
- Directory Services Protector & Active Directory Forest Recovery
- Divergent Vulnerability Assessment and Management
- Dynatrace
- Darktrace/Attack Surface Management, Darktrace/Proactive Exposure Management
- Forescout Technologies, Inc.
- Foresite Managed Autonomous Testing
- FortifyData Enterprise
- Fortinet FortiScanner Cloud, FortiClient EMS
- Heimdal Advanced Vulnerability Management Solution
- HighWire Networks Vulnerability Management Managed Service
- IBM - Gaurdium Vulnerability Assessment
- InsightVM
- Invicti Enterprise
- Ivanti Neurons for Patch Management
- Nessus
- Omnissa Workspace One
- Palo Alto Networks Cortex XSIAM
- Rapid7 InsightVM
- Recorded Future
- Ret Hat, Inc. Insights
- SecPod Technologies, SanerNow
- Secureworks, Inc. (Secureworks) – VDR
- Semperis Directory Services Protector & Active Directory Forest Recovery
- Tanium Vulnerability Assessment and Management
- Tenable Vulnerability Management
- ThreatBoard - Vulnerability Assessment and Management (VAM) Saas
- Trend Micro Vision One Attack Surface Risk Management (ASRM)
- Vulnerability Assessment and Management

- Wiz Advanced
- Zscaler Unified Vulnerability Management

Go Back to Top

11. Data Security:

Description: Products or services responsible for protecting sensitive information from unauthorized access, loss, or exfiltration.

Solution Providers:

- Antivirus for Amazon S3 (AVS3)
- Assured Rubrik Data Security Solution
- BigID for Data Security, Compliance, Privacy, and AI
- Broadcom - Symantec DLP
- Cisco User Protection Suite
- Cohesity
- Commvault Cloud, Powered by Metallic AI
- Cribl Edge, Lake, Stream and Search
- CrowdStrike Data Protection
- Data Loss Prevention, Data Security Posture Management, ForcepointOne SSE
- Fortinet FortiDLP
- IBM Guardium
- Island Enterprise Browser, Island Technologies
- Stellar IT Solutions: Microsoft Purview Informatica
- NetSkope One
- NVISIONx
- OpenText
- Palo Alto Networks Prisma SASE / Strata Data Loss Prevention / Cortex
- Privacera
- Proofpoint Adaptive Email DLP

Proofpoint Information Protection

- Rubrik Security Cloud and Data Security Posture Management
- Snowflake
- Trellix DLP
- Varonis Data Security Platform
- Wiz Advanced
- Zscaler Data Protection

12. Secure Information Sharing Platform

Description: A structured cloud solution for securely routing, tracking, and fulfilling intelligence requests to streamline multi-agency operations and provide real-time visibility.

Solution Providers:

- IRIS Intel

Go Back to Top