Colby Community College (CCC)   Cybersecurity XDR
RFP (Submission deadline is noon on 30 December 2023)

Overview and Background:

Colby Community College is located in the northwest corner of Kansas, approximately 50 miles from the Colorado and Nebraska borders. The college was established in 1964; it is a dynamic institution of more than 2,400 students. In addition to a main campus of approximately 60 acres, CCC operates a 60-acre farm for students to use as a hands-on laboratory and training facility.

Project Goals:

CCC is seeking competitive, sealed bids to purchase Cybersecurity XDR Protection solutions for the Campus computers.

General Information:

CCC is requesting Cybersecurity XDR Protection to provide against malicious attacks. This XDR solution needs to meet the following criteria:

The solution must identify and prevent malicious files from execution, including viruses, trojans, ransomware, spyware, cryptominers, and any other malware type.

The solution must identify malicious behavior of executed files\running processes\registry modifications\ memory access and terminate them at runtime or raise an alert (exploits, fileless, Macros, Powershell, WMI, etc.)

The solution must support the creation of rules to exclude specific addresses/IP ranges.

The solution must identify and block privilege escalation attacks.

The solution must identify and block reconnaissance attacks (scanning).
The solution must identify and block credential theft attempts from either memory (credential dump, brute force) or network traffic (ARP spoofing, DNS Responder).

The solution must identify and block/alert on lateral movement (SMB relay, pass the hash, etc.).

The solution must identify malicious user account behavior indicative of prior compromise.

The solution must support the isolation and mitigation of malicious presence and activity globally across the entire environment.

The solution must support response automation.

The solution must have flexible server deployment options to match various types of environments.

The solution must support rapid and seamless installation across all endpoints/servers in the environment.

The solution must support automated distribution on endpoints/servers that were joined to the environment following the initial installation.

The solution must have a light footprint for minimal impact on the endpoint/server performance.

The solution must provide encrypted communication between the management server and the agents on the endpoints/servers.

The solution must support all commonly used Operating Systems.

The solution must support connection to Active Directory.

The solution must co-exist with all commodity and proprietary software on the endpoints\servers.

The solution must provide full protection for endpoints and servers that are offline from the

The solution must collect endpoint, file, process, user activity, and network traffic in a fully self-sustained manner.

The solution must provide a central collection and processing of alerts in real-time.

The solution must provide a central distribution of updates without the need for user intervention and restarting the endpoint/server.

The solution must be able to specify a schedule for downloading updates, including disabling automatic updates. The solution must assign a risk score to all objects within the protected environment. The solution must support the logging of events, alerts, and updates. The solution must support integration with email infrastructure to notify security personnel in case of alerts.

The solution must support integration with common SIEM products. The solution must support standardized and customizable reports.

The RFP will b   https://www.colbycc.edu/about/vendors, and can be downloaded from there directly as of 5:00 p.m. on 8 December 2023.

Project Timeline:

The Cybersecurity XDR Protection solution bids proposed **MUST** include an ETA for delivery to CCC before 29 February 2024. If you are not able to meet or exceed this deadline, please provide a timeline that you are able to accommodate.

Submission of Proposals:

Respondents to this RFP must submit their sealed proposal   by hand or email   no later than 12:00 p.m. (CST) on 30 December 2023 to Sheri Knight, located in the Thomas Hall
                                                                at sheri.knight@colbycc.edu.

The Vice President of Business Affairs and the Accounting Administrative Assistant will open the proposals.

Anticipated Selection Schedule: