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 identify malicious interactions with data files.

The solution must identify data exfiltration via legitimate protocols (DNS tunneling, ICMP tunneling).

The solution must identify and block the usage of common attack tools (Metasploit, Empire, Cobalt, etc.).

The solution must have an internal protection mechanism against access and manipulation of unauthorized users.

The solution must support File Integrity Monitoring (FIM).

The solution must have built-in vulnerability assessment.

The solution must provide the means to conduct Inventory Management.

The solution must provide log collection and retention.

The solution must include threat hunting.

The solution must support the discovery of unattended attack surfaces.

The solution must continuously collect data on all the entities and their activities within the environment.

The solution must support the display of entity and activity data.

The solution must support dynamic analysis (i.e., sandbox).

The solution must support cross-organization queries.

The solution must support the means to execute forensic investigation.

The solution must support isolation and mitigation of malicious presence and activity locally on the endpoint.

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 organization’s network.

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 be posted on CCC's website, 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 Administration Office (CCC's Main Campus), or via email at sheri.knight@colbycc.edu.

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

Anticipated Selection Schedule:

All submitted proposals will be reviewed and evaluated, and then CCC will recommend to the Board of Trustees (BOT) for a decision; the BOT meeting will be held on 15 January 2024. The selected vendor will be notified within 24 hours after the BOT has approved a recommendation.

Elements of Proposal:

A submission should, at a minimum, include the following elements:

1. Manufacturer product and or model of units being proposed.
2. All additional options or implementation fees.
3. Please disclose the Manufacturer's Suggested Retail Price (MSRP).
4. Specific warranty details for each unit proposed.
5. Document any related fees or processing fees.
6. Document any delivery fees to have the items delivered to CCC.
7. Timeframe to secure and deliver items.

Mandatory Disclosures

Tax Exempt:

Colby Community College (CCC) is a tax-exempt entity. All bids should reflect that no sales tax is included in the final submission.

Exclusions:

If any exclusions exist as a part of this proposal, vendors must clearly define them in a section labeled *exclusions*.

Sub-Contracted Work (if applicable):

If any of the scope of the project will be outsourced to a third party, the vendor name and work to be completed must be included in the proposal. CCC reserves the right to request a different subcontracted company.

RFP Questions (if applicable):

Vendors should only direct inquiries and questions to the following individual(s) at CCC. Any communication received by anyone else at CCC should not be included in the proposal.

Point(s) of Contact:

Sheri Knight, sheri.knight@colbycc.edu, or at (785/460-5407

Statement of Disclosure:

The board reserves the right to reject any or all bids, to accept that bid which appears to be in the best interest of the college, to waive any informalities in any part of any bid, and to reject any or all bids received after the date and time specified. Any bid may be withdrawn prior to the scheduled time for the opening of bids. The bidder to whom the award is made may be required to enter into a written contract with the college and provide a performance or public works bond as required by law or the Board of Trustees (where applicable).