COMMUNITY COLLEGE OF VERMONT
VERMONT STATE UNIVERSITY

VERMONT
STATE COLLEGES SYSTEM

OFFICE OF THE CHANCELLOR
PO BOX 7
MONTPELIER, VT 05601
P (802) 224-3000

Vermont State Colleges
Request for Proposals

Security Information and Event Management Platform

April 15, 2024

Proposals due:
May 10, 2024
5:00 PM Eastern Time

1.0 Organizational History

1.1 General Information

The Vermont State Colleges (VSC) is comprised of two member institutions – Community College of Vermont (CCV) and Vermont State University (VTSU). The system educates over ten thousand Vermonters and non-Vermonters each year, employs over three thousand Vermonters, and in Spring 2020, graduated over eighteen hundred Vermonters and out-of-state students into the workforce with certificates and degrees.

1.2 Mission Statement

For the benefit of Vermont, the Vermont State Colleges system provides affordable, high quality, student-centered and accessible education, fully integrating professional, liberal, and career study.

This integrated education, in conjunction with applied learning experiences, assures that graduates of VSC programs will:

1. Demonstrate competence in communication, research, and critical thinking.
2. Practice creative problem-solving both individually and collaboratively.
3. Be engaged, effective, and responsible citizens.
4. Bring to the workplace appropriate skills and an appreciation of work quality and ethics.
5. Embrace the necessity and joy of lifelong learning.

The Vermont State Colleges system provides continuing educational opportunities for individuals to meet their specific goals.

2.0 Introduction

This RFP is to solicit proposals from qualified vendors for the procurement of a Security Information and Event Management (SIEM) solution for the Vermont State Colleges system.

The proposed solution will support the VSC computing ecosystem comprised of 2 Datacenters, 5 Campuses, and 16 academic centers/learning sites. The VSC provides connectivity for 15000 users and thousands of devices to support learning across many disciplines. Totaling more than 375 physical and virtual servers, 3000 endpoints, 25 routers and firewalls, and 200 switches, we are looking to provide better visibility into the event connections between our systems.

- In addition to providing the capabilities requested in Section 3.0, we also seek to understand the vendor's approach to working with clients, engagement and project management, high-level milestones, and resource needs and expectations.

3.0 Requirements

The following is a listing of the key functional requirements for the Security Information and Event Management RFP. VSC will measure individual submissions against these.

3.1 General requirements

3.1.1 Client / Clientless – describe any use cases for an endpoint agent.

3.1.2 Cloud-based and requires a minimal on-premises footprint for log collection

3.1.3 Provides role-based administration that allows configuration based on views including responder, manager, and administrator.

3.1.4 Requires no manual parsing, correlation, or detection engine configuration for most platforms out of the box

3.2 Integrations/Logging

3.2.1 Must integrate with the following platforms without any customization.

- SentinelOne Endpoint Detection and Response
- FortiGate Firewalls
- Aruba and Cisco managed network devices
- Microsoft Office 365 including Email, OneDrive, and Teams
- Fischer Identity – SAML based Identity and Access Management
- Microsoft Active Directory
- Workstation and server operating systems
- Rubrik

3.2.2 Must accept information from the following platforms and platform types. Where possible specific platforms have been identified.

- Ellucian Colleague
- Application servers (application logs)
- Middleware - ColdFusion
- Database servers (database logs) - mySQL
- Web servers
- Software as a service platforms - Canvas, UKG, Zoom, DUO
- Nessus Security Center
- Syslog

3.2.3 The sensor should be able to queue logs on-premises in the event of an internet outage and reestablish connectivity when internet service is restored

3.2.4 The solution's sensor can be easily deployed in a virtual environment

3.2.5 The solution should have a documented process for accepting custom logs

3.2.6 Can support different retention requirements for various data/event logs

3.2.7 Describe backup for disaster recovery purposes

3.3 Detection

3.3.1 Threat analysis must automatically match events with the most up-to-date threat information, automatically correlating threats with data without requiring any human interaction.

3.3.2 Threat analysis must be performed automatically using multiple threat intelligence feeds.

3.3.3 The solution continuously monitors for threats.

3.3.4 Includes pre-defined detection rules for all integrations.

3.3.5 Must correlate threat intelligence feeds automatically.

3.4 Alerting

3.4.1 Alerts must be configurable by individual users
3.4.2 Alerts can be delivered by email, phone call or SMS
3.4.3 Alerts can be configured by threat or risk level
3.4.4 Alerts provide a direct link to an actionable playbook for response
3.4.5 Evidence for a threat is stacked within a single ticket to minimize noise and alert fatigue
3.4.6 Alerts are prioritized by threat level helping the responder to identify what to respond to first based on severity

3.5 Response

3.5.1 Must have pre-built playbooks that are automatically correlated with the threat identified.
3.5.2 Provides response playbooks that provide education-based benefits to increasing security awareness through guided analysis and response.
3.5.3 The solution provides response playbooks that allow collaborative interaction between IT/Security users.

3.6 Search/Reporting/Dashboards

3.6.1 Provides global search functionality with pre-built reporting for common use cases
3.6.2 Provides an intuitive click-through wizard to generate new report
3.6.3 Provides the ability to schedule reports that are sent in a recurring frequency defined by the user
3.6.4 Has a filter functionality for search & reporting
3.6.5 Has customizable reporting that allows the user to define what data columns are presented
3.6.6 The solution must allow all logs to export using CSV
3.6.7 Must provide a responder dashboard for managing open threats;
3.6.8 Must provide a security dashboard that summarizes threats identified within the environment.

3.7 Support

3.7.1 Describe support options including general technical support and any managed services offerings the bidder feels relevant to this RFP. The intention of this RFP is to acquire a SIEM however, we would consider fully managed offerings. Please ensure that managed SIEM offerings are clearly identified and separated from the SIEM pricing.

4.0 Qualifications, References and Pricing

4.1 Qualifications and References

Provide a description of the qualifications and experience of your company. Include responses to the specific required items listed below:

Bidder Profile and Qualifications

- Name, mailing address, email address and telephone numbers of company.
- Number of years in business.
- Number of employees in Vermont and nationally.
- Number of colleges and universities in which the product is installed and maintained by the bidder.

- Please provide a complete HECVAT Light Version (https://www.ren-isac.net/public-resources/hecvat.html).

Bidder References

You must demonstrate experience and capability in installation and maintenance of the proposed solution by providing evidence of successfully completing projects of similar size and scope. Please provide at least three customer references, with the following information:

- Customer name and location
- Contact person(s): name, title and telephone number
- Your project manager for the engagement
- Product installation date
- Number of years you have maintained the system

By submitting your proposal, you understand and agree that the VSC may make any investigations it deems necessary to determine your ability to perform the work. You agree to furnish the VSC all such additional information and data for this purpose, as the VSC may request.

4.2 Pricing

Your proposal should include all of the charges, and it should clearly state the pricing structure along with the types of products and/or services accompanying each price. The VSC expects fully bundled pricing for each service offered and any tiered pricing or volume purchasing discounts/rebates that maybe available due to purchasing loads.

4.3 Terms

4.3.1 Please provide 36 & 60 month term options on all pricing, unless otherwise noted.

4.4 Taxes/Fees

4.4.1 Please note any and all proposed taxes, fees, or charges.

4.4.2 The VSC is exempt from sales and use taxes. Submitted proposals shall not include these taxes. The College's tax exempt number will be provided to the selected bidder. Please clearly note these exemptions in your proposal.

5.0 RFP Instructions, Requirements and Information

This section provides information on how to contact the VSC for questions, deadlines, the selection process, legal and insurance requirements, and other general business matters.

5.1 Questions about this RFP

Please submit your questions to the VSC on or before Friday May 3, 2024, at 5:00 PM Eastern Time. All questions will be posted on the VSC website, www.vsc.edu, and made available to all bidders. The contact information for questions:

Name	Tony Hashem
Title	Director of IT Security
Email address	siem.rfp@vsc.edu

5.2 Deadline and Delivery

The deadline for submitting responses is 5:00 PM Eastern Time, Friday May 10, 2024. Provide an electronic copy **only, via email,** to:

Name	Tony Hashem
Title	Director of IT Security
Email address	siem.rfp@vsc.edu

5.3 Selection Process

Method of Award

VSC will base the evaluation of each proposal to this RFP on its demonstrated competence, compliance, format, cost, and enterprise applicability. This includes, but is not limited to, product availability, quality, prices, service availability, timing, and delivery. This RFP is to identify vendors with the interest, capability, and financial strength to supply the VSC with a Security Information and Event Management platform. If the VSC does not identify a suitable bidder within the RFP process, the VSC is not obligated to award the project to any bidder.

The VSC, in its best interests, reserves the option to accept or reject any or all proposals, to accept or reject any item or combination of items therein, to waive any irregularities or informalities in any proposal or items therein, and/or to negotiate with bidders following the evaluation of proposals without right of recourse by other bidders. A top proposal would be assessed in the judgment of VSC as best complying with all considerations set forth in this RFP. When VSC has tentatively selected a successful proposal, VSC may engage in discussions with the bidder to formulate plans in greater detail, to clarify unclear items for either party, and to otherwise complete negotiations prior to formal selection.

Evaluation Criteria (no weighting is implied by order of listing):

1. The extent to which the bidder's solution matches the requirements of the VSC.
2. Engagement methodology.

3. Bidder's qualifications and references.
4. Cost and length of contract.

5.4 Bid Process

Date	Milestone
04/15/2024	RFP issue date
05/03/2024	Questions Due
05/10/2024	Bidder written proposal due date
05/24/2024	Finalists notified
06/03/2024	Finalist presentations to VSC – Entire Week
06/17/2024	Bidder(s) selected
**July 2024	Contract(s) made

** The VSC will make its best effort to meet these dates but will take the time necessary to make a well-informed decision and negotiate a good contract. Bidders participating in this RFP should expect this date to change. The VSC will be under no obligation to inform bidders of a change in this date. The VSC will inform bidders of a change in all other dates that are part of the bid process.

5.5 Confidentiality

The Vermont State Colleges comply with the Vermont Public Records Act, 1 VSA § 315 *et seq*. which requires public agencies to allow any person to inspect or copy any public record upon request. Accordingly, bidders are hereby advised that any communications, data or other information received by the Vermont State Colleges during the RFP process could be subject to a public records request. However, certain public records are exempt from public inspection and copying, as set forth in 1 VSA § 317(c), including, for example, those portions of a record which meet the statutory definition of a trade secret. Accordingly, bidders should submit a second copy of their proposal, from which any portion of the proposal that the bidder reasonably believes to be exempt from disclosure under the Public Records Act has been redacted.

By submitting a proposal, you indicate that you understand the requirements of this subsection (5.5) and the potential applicability of Vermont's Public Records Act to your proposal.

5.6 Indemnification

The bidder shall indemnify and hold VSC, its officers, agents and employees free and harmless from any and all claims, liabilities, losses, actions, proceedings, suits, damages and expenses, including out-of-pocket litigation costs and reasonable legal fees, arising from or relating to the bidder's performance in response to this RFP and under any contract entered into with the successful bidder.

By submitting a proposal, and in exchange for VSC's consideration of same, you agree on behalf of yourself, your shareholders and your officers to be bound by the indemnification provisions of this subsection (5.6).

5.7 Rights of the VSC

VSC reserves the right, at its discretion, to pursue actions that include but are not limited to the following:

- Request additional information
- Request clarification of any sections or questions in the bidder's response to this RFP
- Reject, for any reason, any or all of the proposals submitted to VSC
- Issue subsequent RFP or RFP invitations to bid as a result of changes and/or refinements to the proposed project

This RFP does not obligate the VSC to accept any proposal, negotiate with any bidder, award a contract or proceed with the project as it is outlined in this RFP.

5.8 Assignment

The bidder may not assign or transfer its rights or obligations under this RFP without the prior written consent of VSC, which consent shall not be unreasonably withheld. Any assignment of the RFP agreement by the bidder without the prior written consent of VSC shall void the RFP response from the bidder.

5.9 Insurance

You shall provide with your proposal, proof of insurance as stated below. In the event you do not carry the maximums requested, you must provide written proof that you will be able to provide the maximums if awarded the contract. You shall secure, pay for, and maintain in effect the following insurance during the contract period:

- Commercial General Liability Insurance: Including Bodily Injury and Property Damage Liability, Independent Contractor's Liability, Contractual Liability, Product Liability and Completed Operations Liability in an amount not less than $1,000,000 combined single limit, per occurrence, and $3,000,000 annual aggregate.
- Workers Compensation and Employers Liability Insurance: For any bidders with employees, standard workers' compensation as required by Vermont State statute and employer's liability insurance in an amount not less than $100,000 per accident, $500,000 annual aggregate.
- Automobile Liability: For bidders who will drive on VSC's premises, Automobile Liability in an amount not less than $1,000,000 per occurrence for bodily injury and property damage, including owned, hired, and non-owned vehicle coverage.
- Professional Liability: $1,000,000 each claim, when applicable.
- Cyber Liability: $1,000,000 each event for Breach Response

If selected as the successful bidder, you agree to name the VSC as additional insured on your liability policies and shall provide a 30-day notice of cancellation or non-renewal of coverage to the VSC. The VSC does not need to be named as an additional insured on the workers compensation policy.

If selected as the successful bidder, you agree to submit a copy of the Certificate of Insurance verifying the above coverage levels to the VSC twenty (20) days prior to selling or distributing products and

services at VSC or otherwise performing under the contract. Any liability coverage on a “claims made” basis shall be designated as such on the certificate.

Failure of the bidder to take out and/or maintain any required insurance shall not relieve the bidder from any liability under the contract, nor shall the insurance requirements be construed to conflict with or otherwise limit the obligation of the bidder concerning indemnification. The bidder’s policies shall be considered primary insurance and exclusive of any insurance carried by VSC.

5.10 Intent to Bid

The undersigned (“You”) agrees to all provisions required in the Security Information and Event Management RFP dated April 15, 2024, and all applicable addenda, with the exception of those listed below. Any exemptions listed may affect the viability of your proposal.

In addition, the undersigned (“You”) agrees to provide all equipment, material and personnel associated with these services as described in the Security Information and Event Management RFP dated April 15, 2024, and all applicable addenda.

Exceptions:

Section Reference Number	Reason for exception

_____
Company Name

_____
Signature of Authorized Representative

_____
Print Name of Authorized Representative

_____
Print Title of Authorized Representative