- What current SIEM provider are you replacing (if applicable)? None
- If you are replacing a current SIEM system, can you please provide the amount of estimated data ingested? N/A - we are expecting our vendor to help determine
- Can a POV be used to properly size this environment if there isn't a SIEM system being replaced? - Possibly, we would consider this.
- Does VSC have an A5 License with Microsoft? A1/A3
- Is there a specific security event driving this acquisition? Not relevant
- Does VSC have any footprint in AWS, Azure or GCP? - We are just starting to engage with Azure
- Is VSC intending to ingest all endpoints, including staff, faculty and students? If yes, what is the number of endpoints? - No students or faculty expected at this time. Our focus will be on infrastructure, servers and IT applications
- How many team members are on VSC's security team? Not enough
- Would VSC entertain a 2-year term, if it can be shown to be of value to VSC? Yes
- How many events per second during your busy hours do you expect to be sending to the SIEM? Unknown we are expecting our vendor to help determine
- How do you plan on implementing the solution? - Cloud based is preferred
- What is the breakdown of your server functions, i.e., application vs email vs DNS vs domain controllers? Approximately 350 application servers 25 SQL Servers, 12 Webservers and 39 DCs.
- What is the required duration of data retention? We are using 30 days as the starting point. We realize some data will be less retention time and others more
- For on-site collectors, will they be at every site, and if so, do you have the capability to have them all VM or would hardware be required? We do not necessary have a preference. Depends on the solution.
- On how many endpoints/servers do you intend to do advanced analytics such as user behavior monitoring, registry change, and file integrity monitoring? Unknown at this time
- Can you provide an example of the expected workflow of a response playbook? Not at this time
- How many administrators would be logging in to manage the solution? 2-3

1. How much daily data ingest will you require from your various different data sources? Unknown - we are expecting our vendor to help determine
2. How long will you need to retain this data? We are using 30 days as the starting point. We realize some data will be less retention time and others more

1. Is this a FFP, T&M or Cost+ bid - This is an RFP - Please propose your solution, implementation and license cost and any annual costs.
2. Does VT only wish to see Rates for Solution proposed or also staff rates? - Only for the solution
3. Would you please consider an extension to the bid deadline?- No, only if we decide to change the requirements

- What is your total data ingest in LogRhythm today, calculated annually? Do you anticipate continued growth? If yes, by how much? (rough order of magnitude) - Unknown - we are expecting our vendor to help determine. We are not currently using any SIEM.
- Are you currently using LogRhythm for application performance and availability monitoring? - We are not a customer of Logrhythm
- What type of logs are you ingesting for non-security related platforms, and what are you using them for? - We currently do not have a SIEM
- How many SOC analysts do you currently have? Not relevant
- Do you conduct active threat hunting today? Vulnerability scanning
- What license for Office 365 do you currently have? A1/A3
- What threat intelligence feeds do you consume today? Only what it's included with the EDR and Nessus scanner. We also subscribe to some public domain sources such as MS-ISAC
- What is the driver for the log export in CSV format requirement? - There's not. We would accept any of the common formats, but it should at least produce a CSV file.
- Do you have a response template you would like submissions to use for the technical bullet points? No, but ensure you address the requirements clearly.
- Do you require any implementation services to be included in the initial bid? Separated line items.
- Is the initial bid intended to represent best and final pricing? We could end the RFP process at any time. Vendors are encouraged to lead with their best price since they may not an opportunity to adjust.

4. If our company has recently completed the full version of the HECVAT questionnaire as opposed to the Light version, can we share this copy with VSC instead? - Yes
5. Can VSC please provide the log/data retention requirements mentioned in 3.2.6? - we are using 30 days as a starting point but are flexible
6. Does VSC have any compliance requirements for the SIEM cloud environment? If so, can you please list them? (Ex: PCI, FISMA, FedRAMP, etc.)? We are subject to HIPAA, GLBA, FERPA and PCI. We do not store or process any payment card information.
7. What is the expected ingestion rate for VSC? Please provide this answer in measurement units of GB/day. - Unknown - we are expecting our vendor to help determine
8. Can you please provide a breakdown of the following:
    - 25 routers and firewalls
        - How many of each? 3 External firewalls 22 internal
        - What is the Firewall throughput or events per second? ~1000
    - 375 physical and virtual servers
        - How many are linux? 75
        - How many are Windows? 300

How many events per second during your busy hours do you expect to be sending to the SIEM? - Unknown - we expect the vendor to help us determine this based on our equipment, footprint and what is considered relevant events

How do you plan on implementing the solution? - Cloud based is preferred

What is the breakdown of your server functions, ie application vs email vs DNS vs domain controllers? O365, 39 DCs, 350 app servers, 25 SQL, 12 webservers

What is the required duration of data retention? 30 days to start

For on-site collectors, will they be at every site and if so, do you have the capability to have them all VM or would hardware be required? Depending on the solution we could probably do either

How many endpoints/servers do you intend to do advanced analytics such as user behavior monitoring, registry change, and file integrity monitoring on? Unknown at this time. We would look to the vendor for guidance and best practices

Can you provide an example of the expected workflow of a response playbook? No

How many administrators would be logging in to manage the solution? 2-3

1. We are considering using Tenable Nessus for threat analysis in your environment. This tool is known for its robust vulnerability scanning capabilities and its ability to integrate with multiple threat intelligence feeds, such as ThreatGRID. Would you be open to us using Tenable Nessus for this purpose? If you have any specific requirements or concerns about this tool, could you please share them with us? – This RFP is for a SIEM not a vulnerability scanner.
2. In addition to Tenable Nessus, are there any other threat analysis tools you have used in the past or would prefer us to use? If so, could you please provide some details about these tools and why you prefer them? This will help us better understand your preferences and tailor our approach to meet your needs. Not Relevant

3.2.2 Is it Ellucian Colleague ERP or SIEM? What logging is possible (syslog/API)? Ellucian ERP - Unsure of logging

3.2.2 What is the log format of the application logs from the application servers? Standard windows security logs

3.2.1 Is it possible to export logs from Fischer SAML in custom or generic log formats or via API? Will the University considering switching to a more well-known SAML IAM? Yes, we would need to know what is needed. No plans to switch at this time, but it's a possibility.

3.1 Is the University comfortable with virtual agent / agentless integrations for cloud/virtual infrastructure and 1 on premise security sensor for each datacenter for physical network infrastructure monitoring? (SPAN/TAP) Yes

3.2.2 What webservers does the University use? (Apache, nginx, etc) Apache, WordPress

3.2.2 Is it possible to export logs from the listed SaaS platforms via API? Probably

1 What is the average daily data ingestion rate? Unknown - We are expecting the vendor to help us determine this based on our size and equipment footprint and what's relevant
2 Are there SOAR playbooks built - No
3 Do you have automation in place for common response actions - No
4 Does the University currently use a SIEM its looking to replace/integrate? No
5 Is there an incumbent or is this a new requirement? If there is an incumbent, who is it? New
6 What is the expected budget for this contract? Not Relevant
7 What was the incumbent contract value? Not applicable

1) Do you have any compliance requirements? - We fall under HIPAA, FERPA, GLBA and PCI. We do not store or process any PCI data
2) Total number of servers - include physical and virtual – See RFP
3) Total numbers of laptops and desktops – See RFP
4) How many Sentinel One Licenses are deployed? What version of Sentinel One are you using? (S1 Core, Control, Complete) If using different versions of S1, what is the license breakdown? For example how many core vs complete? Not relevant
5) If you move forward with a managed service do want your managed SIEM vendor only ingesting logs from sentinel one for monitoring and alerting purposes or would you also like the vendor to fully manage your sentinel one instance/console, helping with policy, blocklist, exclusion configurations and taking all necessary response actions that the tool allows should there be an incident? We are not sure. The RFP is for SIEM, but are willing to consider a managed option.
6) Total number of Fortinet Firewalls? - 25
7) Are the firewalls paired as HA? yes
8) Who is your email vendor? Microsoft 365, Google, Exchange on premise etc.. - O365
9) Any other preferred Software & Applications to be monitored outside of what's listed in section 3.2.1 of the RFP? Not at this time
10) Any hosted infrastructure in the cloud? This includes servers, containers, and hosted applications. - Minimal, but we do use some SaaS
11) Are you currently using a SIEM? If so, what is your log ingestion per day in either EPS or GB/Day? No
12) Could you provide a Network or Server topology diagram? No

What is the license scope of the project? The detail provided in the RFP Introduction section is helpful but it doesn't specify desired ingestion rate. - We are uncertain what our ingestion rate since we are not sure what should be ingested. We are looking for the vendors to assist us in determining this.

- Quantity of Firewalls: We have 3 external firewalls and several internal location specific ones for internal traffic

- Quantity of Domain Controllers: 39
- Number of Students: Approx. 10000 student
- Number of Faculty: Faculty and Staff 2900
- How are the students segmented: Via role at the network access level. (likely not relevant)
- Quantity of application servers? 350
- Quantity of SQL Servers? 25
- Quantity of Webservers? 12
- Do you have a radius server? Yes (CPPM)
- Do you utilize Aruba ClearPass Policy Manager (CPPM)? Yes
- Estimated budget for the Security Information and Event Management Platform RFP? Not Relevant
- Any other Security products missing? Unclear
- Does Vermont State Colleges have a current cyber security partner? Not relevant
- Does the selected vendor need a State of Vermont business license? Unlikely, but we will verify.

1. Do you have an exact breakout of the operating systems for the 3,000 endpoints? (for example, how many Windows and MACs) - We are about 95% Windows
2. Does VSC need to be PCI compliant or have to adhere by any additional compliances? - We fall under the following regulatory guidelines – PCI, HIPAA, GLBA, FERPA. We do not store any PCI data, we only serve as a pass through to our card processing vendor.

1. What specific security data is to be gathered from the application server logs? - Security event data such as logins, access changes, failed login etc
2. If Fischer Identity is not initially supported, but other MFA is supported, will the submission be rejected? Not Rejected
3. If log retentions are not customizable outside of existing retention standards, is that a deal breaker? No
4. Is a documented incident response plan in place? Not relevant
5. Is a documented disaster recovery plan in place? Not relevant
6. Does a CISO or ISO role exist within the organization? - Yes
7. Is there a current SIEM solution in place? - No
8. Complete list of assets and # of assets to be monitored….Firewalls – make and models, Web Application Firewalls, DNS Server (MS, BIND, etc..), any NetFlow capabilities, Number of Infrastructure devices (routers, switches, etc.) make and models, Number of Servers make and models, Number of Active Directory or Ldap Servers. - SEE RFP
9. Complete list of all cloud instances. - SaaS Applications, Very limited Azure, Some Wordpress sites
10. Current list of security tools being used i.e….SIEM, Endpoint security/management, Vulnerability Identification, Intrusion Detection, CMBD solution, etc.. - SentinelOne, Fortinet, Microsoft, Nessus Scanner, SOPHOS
11. # of Full Time Employees – Apprx 2900
12. For a cloud based SIEM/XDR solution does the solution need to be FedRAMP certified. Or GovCloud? If CJIS compliance required, it is assumed that GovCloud? - No
13. Who is the project sponsor? - Not Relevant
14. Is there budget allocated for this project? Not Relevant
15. What is the expected timeline for delivery of said services? - July / August 2024
16. Will end user contract with just one vendor or more? - One
17. Was this RFP created internally or was a 3rd party resource used to help create the RFP? If so, will that 3rd party be allowed to participate in bidding on the RFP? - Internally
18. Please confirm that current RFP Scope is for Manage, Detect and Respond (MDR) services at a 24x7x365 pace. - See RFP

19. What is the current Log Collection & Storage requirements. Is 7 days hot/90 days warm/365 days cold (some level of collection/storage will be required to support Analysis & Response). We are using 30 available days as a baseline but may vary depending on data
20. Are there specific Compliance reporting requirements? - Not at this time
21. What is current storage solution being utilized? - Not relevant
22. What is current backup solution being utilized? - Rubrik
23. What phone system is being utilized? - Not relevant
24. Do you have SOAR solutions you would like implemented as part of the solution. - Not relevant
25. Do you know your current EPS – Events Per Second for in-scope networks? Unknown, we are expecting the vendor to assist in determining what is relevant and what isn't.

1. Threat Intelligence - Does it exist at VSC now? OR, is the expectation that it will be included. If it exists, what are the specific sources, are they paid or free, and how long do the contracts last. - We get some threat intelligence via our EDR and vulnerability solutions. We also receive some free threat sources but we have no integration. MSISAC and through our firewall vendor
2. Do you expect Playbooks to be in place or do you expect it to be built (requiring services). - We expect there to be some build in capability. Over time, we would develop our own.
3. Do you have a list of target use cases for automation playbooks? No
4. We will need to have a discussion around ***sizing and log volumes***. Does VSC have specific information about the volume of logs from non-endpoint sources and thoughts on retention timeframes? - We are looking to the vendor to help us figure that out.
5. Analytics - Is the expectation that there are native (built-in) analytics that baseline normal behavior and detect anomalies in network, endpoint, or identity activity or is it expected that services will be required to build custom analytics. - We expect there to be some built in analytics and baselines. We understand we will need to establish our own as well.
6. Do you have a list of analytics or Machine Learning models that you would want to see in the solution? - N/A
7. Is there openness to other endpoints instead of / in place of SentinelOne? - No
8. When does the SentinelOne contract expire? - Not relevant
9. If the solution can provide greatly increased insights and capability with a different endpoint, is VSC open to running this endpoint in monitor-only mode (in addition to running S1)? - We are not open at this time to considering different endpoint products.
10. Will there be a local SOC team or a MSSP / MDR partner involved in monitoring the solution and providing incident triage and response capabilities? Initially, we plan to manage internally but will consider managed options as add on to this RFP.
11. Does the proposed solution need bi-directional integrations, which can also take action in the event of an incident (e.g. block a malicious IP, isolate a host, or reset a user's password)? No, but we would see this as a differentiator
12. Should the solution intelligently group alerts (into an incident or a case) to improve analyst workflow? - Yes, we assumed this was tables takes. We will be looking for this functionality.

Would like more elaboration on how VSC views the importance of:

1. Automation Playbooks - how much will VSC try to employ automation to the triage and incident response process? Has there been discussion of which tasks lend themselves

to automation? - We have not gone this path yet. However, given our resource constraints this would benefit us.

2. Case Management capabilities - is there a desire or expectation for built in (out of the box) case management? - Yes – We assumed there would be something built in we could evaluate
3. Built-in collaboration tools - is there an expectation for built in collaboration tools within the core solution? - This would be a differentiator
4. Analytics - Are you thinking of these as basic saved searches & queries or is VSC looking for a more comprehensive solution that includes Machine Learning models and the application of AI in the future. - We would expect to have saved and canned searches but for the planform to have the ability to integrate machine learning.
5. Ability to executive response actions natively from within the tool - should the solution provide the ability to respond to alerts / remediate problems directly from within the tool? - This would be a differentiator
6. Threat Intel - should this be automatically applied to discovered alerts and incidents? Do you want basic querying capabilities or a Threat Intel Management system? - Yes, but we do not need a threat management intelligent system. Having threat intel built into the platform would be a differentiator amongst vendors.
7. Do you expect automatic correlation and aggregation of alerts from disparate sources into a single larger incident. Has VSC given thought about how this will happen? Do you expect to contract services to build this or do you expect this to be part of the purchase solution? - Yes, we expect there to be some built in capabilities but eventually design our own custom.
8. Does VSC place value on the ability to align discovered alerts to the Mitre Att&ck framework? - This would be a differentiator