Questions for RFP #251-26-186 S2 Security Management System

#	Reference	Vendor Question	Answers
1	Background - Page 5	We understand that Wake County Schools has 20,000 faculty. Is this an accurate number to use or is there a more accurate count available?	21,000 employees, however not all are faculty
2	Background - Page 5	We understand that there are 160,000 students within the district. Is this an accurate count or is there a more accurate count available?	165,077 10-day headcount for students
3	Organizational Background and Current Environment - Page 5	How many on-premises servers do you currently operate?	Information will be provided to the awarded vendor
4	Organizational Background and Current Environment - Page 5	We understand that Wake County Schools utilizes AWS for some infrastructure. Based on this fact, we have the following questions: ● How many compute instances (AWS EC2 instances, Azure VMs, etc.) are deployed? ● Do you use containers? If yes, how many containers are running concurrently on average? ● Do you make extensive use of serverless workloads? (Lambda, etc.) If yes, approximately how many functions run concurrently?	Wake County Public School System does leverage cloud infrastructure, including AWS, to support certain operational and instructional needs. However, for security reasons, we are unable to share detailed information on the number of compute instances, container deployments, or serverless workloads in a public forum. Vendors may assume a moderate-scale K-12 environment and propose solutions that can scale appropriately with district growth. Specific deployment details can be discussed with the awarded vendor under appropriate confidentiality agreements
5	Organizational Background and Current Environment - Page 5	How many Microsoft O365 users with mailboxes exist? ● Do all faculty/staff have an O365 mailbox? ● Do all students have an O365 mailbox?	See # 1 and #2
6	Organizational Background and Current Environment - Page 5	How many Google Workspaces users exist? Do all these users have mailboxes? ● Do all faculty/staff have Google Workspaces account? ● Do all students have a Google Workspaces account?	WCPSS uses Microsoft 365 for faculty, staff, and students, but mailbox counts aren't shared; vendors should assume a large mixed user base and show scalability
7	Technical Requirements - Page 6	What is your desired data retention period for the security log and telemetry we collect?	WCPSS requires data retention aligned with the state retention schedule, and industry standards, but specific retention periods are not shared;

			vendors should outline flexible retention options
8	Scope of Work - Page 5	How many internet egress points do you have (sites with direct internet access)?	WCPSS maintains multiple egress points for internet access, but exact numbers are not shared; vendors should assume a distributed environment and show how their SOC can support multi-site visibility
9	Scope of Work - Page 5	Is all internet-bound traffic from individual schools backhauled to a central datacenter/facility?	Vendors should demonstrate how their SOC services provide coverage for distributed traffic flows
10	Scope of Work - Page 5	Can you indicate how many of these sites have more than 3Gbps internet bandwidth and how many have less than 3Gbps internet bandwidth? If more than 3Gbps bandwidth, what is the average and maximum internet usage bandwidth at those sites?	WCPSS cannot provide specific bandwidth figures for sites. Vendors should assume a range of bandwidth capacities across locations and show how their SOC services scale to support both high- and low-bandwidth sites
11	Scope of Work - Page 5	Do all internet egress points have redundant firewalls in place? If not, how many are not redundant?	Egress points have redundant firewalls. Vendors should demonstrate how their SOC services can accommodate environments with varying network security configurations
12	1.1 Level 1: Monitoring and Escalation Only, Page 5	What is the total number of endpoints being monitored with CrowdStrike Falcon?	WCPSS uses CrowdStrike Falcon to monitor endpoints, currently 22.356 workstations, and 630 servers. Vendors should assume a sizable mixed environment and demonstrate how their SOC services scale to cover all endpoints
13	1.1 Level 1: Monitoring and Escalation Only, Page 5	What are the “other integrated sources” and count of them?	WCPSS integrates a variety of additional security and IT data sources, but specific types and counts are not shared. Vendors should propose solutions that can handle multiple source types and scale as needed
14	1.2 Level 2: Monitoring + Limited Response Support, Page 5	What are the sources and quantity of these sources for “Advanced Log Analysis”?	WCPSS uses a variety of sources for advanced log analysis, but specific types and counts are not shared. Vendors should demonstrate how their SOC

			services support multiple log sources and scale as needed
15	2.2 Future Integration Flexibility with Other Endpoint Solutions (Microsoft Security Suite or Similar Platforms), Page 6	What is the total number of users and devices using the Microsoft suite?	WCPSS uses Microsoft 365 across faculty, staff, and students, but specific user and device counts are not shared. Vendors should assume a large, mixed environment and demonstrate how their SOC services scale accordingly
15	SCOPE OF WORK	What is the count of school district owned workstations and servers? Please do not include student devices in this count.	See Question #15
17	SCOPE OF WORK	Is the intention for 1 centralized MDR instance for all WCPSS? OR does each school within the district intend to have their own instance/license of MDR?	WCPSS plans for a centralized MDR approach across the district. Vendors should demonstrate how their services can support a centralized deployment while providing visibility into multiple locations
18	SCOPE OF WORK	Is it WCPSS' preference to expand currently installed/deployed solutions to provide additional security services as it pertains to this RFP?	WCPSS is open to expanding existing security solutions or integrating new services. Vendors should describe how their SOC offerings complement or enhance current deployments.
19		Is it possible to receive a mutual NDA? If not, is it possible to include edits?	At this stage, no NDA is in place. Vendors should proceed with non-sensitive questions only; NDA discussions or edits will be considered if we move forward with shortlisted vendors
20	RFP Section Scope of Services Required 4 Pricing	Please provide the number of devices shown in CrowdStrike Falcon with EDR deployed (workstations and servers included)	See Question #15
21	RFP Section Scope of Services Required 4 Pricing	Please provide the number of employee & student accounts in Microsoft 365	See Question #15
22	RFP Section Scope of Services Required 4 Pricing	Please provide the number of employee & student accounts in Google Workspace	See Question #15
23	RFP Section Scope of Services Required 4 Pricing	Please provide the number of resources in AWS (including Virtual Machines, databases, & storage accounts).	See Question #15
24	Section 1 – Scope of Work	What is the total count of your knowledge workers? ● How many SIEM detection rules are currently in production?	WCPSS cannot share exact counts of knowledge workers or SIEM rules at this stage. Vendors should assume a sizable user base and an actively managed SIEM

			environment, and describe how their SOC services scale accordingly
25	Section 1 – Scope of Work	Is there a requirement for service provider resources, OR their 24/7/365 SOC personnel, to be in a certain geographical area, such as USA or Europe? ● Are you comfortable with some service provider staff located in India? ● Will you require an interaction model involving personnel in multiple geographies/regions/countries because of your global footprint?	Preferred USA. Vendors should describe how their SOC resources can provide 24/7 coverage and support
26	Section 1 – Scope of Work	Based on Section 1 'Scope of Work', it would appear that vendor can meet all your stated requirements. Are you interested in all the below services, or just a subset? We can execute and advise on all of them within our response? ● Managed SIEM? - # of knowledge workers? ● Managed EDR? - # of endpoints? ● Managed Firewalls? - # of firewalls? ● Vulnerability management? - # of IP's for internal scanning? - # of IP's for external scanning? ● Manage Abusebox / anti-phishing - # Mailboxes? ● Threat Management, Deep/Dark/Surface Web monitoring - # of brands, # of executives, # of takedowns per year? ● Incident Response Retainer(IRR)?	WCPSS is interested in vendors providing services as described in the RFP. Exact quantities and counts are not shared at this stage. Vendors should propose solutions that can scale across all service areas listed and demonstrate flexibility to meet multiple requirements
27	Section 1 – Scope of Work	Do you use Falcon Complete?	No
28	Section 1 – Scope of Work	Do you expect the service provider to take over full management/monitoring of your existing SIEM or EDR, or should we propose a net new SIEM or EDR with a migration plan/schedule?	Vendors may propose either approach—supporting existing SIEM/EDR or deploying a new solution with a migration plan. Proposals should describe scalability and integration with current security operations
29	Section 1 – Scope of Work	For your current/in-scope SIEM platform. ● What is your current license in GB/day? ● What is your actual average SIEM ingest in GB/day?	WCPSS does not disclose specific SIEM ingest, license, retention, or rule counts at this stage. Vendors should assume a moderately scaled SIEM environment

		● What is your SIEM log retention requirement? Is this for compliance or internal audit reasons? ● How many SIEM detection rules are currently in production?	and describe how their SOC services support log collection, analysis, and retention in compliance with industry standards
30	Section 1 – Scope of Work	What are the specific, primary/critical or high priority in-scope managed technologies? (e.g. SIEM? EDR? IPS/Firewall?) We can manage, optimize and monitor all the following: ● CrowdStrike NextGen SIEM? ● CrowdStrike EPP (Falcon)? ● CrowdStrike Fusion SOAR? ● CrowdStrike Identity Protection? ● CrowdStrike Falcon Cloud Security? ● Microsoft Sentinel SIEM ● Microsoft Defender for Endpoint (MDE)? ● Microsoft Defender for Identity? ● Microsoft Defender for Cloud?	WCPSS is seeking coverage across multiple key security technologies as outlined in the RFP. Vendors should propose scalable SOC services that support a range of SIEM, EDR, and cloud security tools without requiring disclosure of exact deployments or configurations
31	Section 1 – Scope of Work	Do you have an established Microsoft E5 license? ● If so, are multiple security solutions within the Microsoft security stack operational or being considered for deployment?	Not for all staff
32	Section 1 – Scope of Work	Who is your primary CSP (Cloud Services Provider)? AWS, GCP, Azure, Oracle, other, hybrid/multiple?	No vendor has been identified as primary
33	Section 1 – Scope of Work	Do you have a CSPM tool (Cloud Security Posture Management), such as Wiz, Palo Alto Prisma, Lacework, Microsoft Defender for Cloud, or Google Security Command Centre? Is this tool or your cloud security environment in general, in-scope for security monitoring?	WCPSS uses cloud security tools to support our environment, but specific products and configurations are not disclosed. Vendors should describe how their SOC services can monitor and integrate with cloud security platforms as part of a scalable solution
34	Section 1 – Scope of Work	Specific to vulnerability management and/or patch mgmt.: ● What tool are you currently using for vulnerability management and patch management (e.g. Tenable, Qualys, Tanium, Microsoft Defender for Vulnerability Mgmt.)? ● Is there an expectation that the awarded service provider will fully manage/administer these VMS tools? ● What is the total number of internal and external ip addresses in-scope for vulnerability scanning/management?	WCPSS uses vulnerability and patch management tools, but specific products and IP counts are not shared. Vendors should propose solutions that can support vulnerability management at scale and describe whether they can fully manage or integrate with existing tools

35	Section 1 – Scope of Work	1. Is OT or IoT security monitoring in-scope? If in-scope: ● What tool are you using for OT security (e.g. Nozomi, Claroty, Microsoft Defender for IoT)? ● Is there an expectation that the awarded service provider will fully manage/administer this OT security tool in a co-managed context, or is the requirement 'monitor only'? ● Do you have full or partial coverage in terms of sensor distribution across all in-scope OT sites and locations? ● Is there an expectation that the awarded service provider will fully implement your OT security solution, or expand upon the current implementation?	OT and IoT security may be in-scope. Specific tools, coverage, and management expectations are not disclosed. Vendors should describe how their SOC services can monitor, co-manage, or scale OT/IoT security coverage across distributed environments
36	Section 1 – Scope of Work	Will you expect to perform a 3rd party audit or risk assessment on any aspect of the awarded service provider's company or practice? If so, any specific audit or assessment?	WCPSS may conduct third-party audits or assessments as part of due diligence, but specifics are not shared at this stage. Vendors should describe how they support audit and compliance activities
37	Section 1 – Scope of Work	Is there a requirement for the service provider to adhere to any specific 3rd party certification or accreditation?	There are no specific certification requirements at this stage. Vendors should describe any relevant certifications or accreditations their SOC services hold
38	Section 1 – Scope of Work	Do you expect the service provider to take over full management/monitoring of your existing SIEM or EDR, or should we propose a net new SIEM or EDR with a migration plan/schedule?	Vendors may propose supporting existing SIEM/EDR or deploying a new solution with a migration plan. Proposals should describe scalability and integration with current security operations
39	Section 1 – Scope of Work	For your current/in-scope SIEM platform. ● What is your current license in GB/day? ● What is your actual average SIEM ingest in GB/day? ● What is your SIEM log retention requirement? Is this for compliance or internal audit reasons? ● How many SIEM detection rules are currently in production?	WCPSS does not share specific SIEM ingest, license, retention, or rule counts at this stage. Vendors should assume a moderately scaled SIEM environment and describe how their SOC services support log collection, analysis, and retention in line with industry standards
40	Qualifications, pg. 6-7	Regarding the bulleted list of qualifications, is the reseller required to meet each of these, or is it acceptable for the OEM (for example, Sophos) to meet the requirements if the reseller does not? Specifically referring to bullets 2-4:	Vendors should demonstrate how the proposed team and/or OEM partner meet the qualifications. It is acceptable

		• No fewer than five years of experience in performing the required duties as outlined in this RFP will be accepted. • Demonstrated experience with SCADA/ICS, IoT devices, and UNIX-based environments. • At least one staff member must hold a certification such as: OSCP, GXPN, GPEN, or comparable industry certification.	for experience or certifications to be held by the OEM, provided the reseller clearly outlines roles and responsibilities in the proposal
41	Exhibit B, pg. 15	Do any of the "Other" types of insurance apply or are required for this RFP? If so, which specifically apply?	Commercial General Liability plus Cyber Liability. See specifics in Exhibit B
42	Page 5 Section Background	Per RFP, 20,000 staff in the district and 160,000 students. Can you please provide the specifics on how devices are broken out? This will affect licensing: • How many Laptops and desktops (with running Windows or MAC OS): • How many iPad and Chromebooks • How many Servers (Running ServerOS/Linux)	See Question #15
43	Page 5 Section Scope of Work	What is the specific level of licenses you currently have for Crowdstrike / name of licensing other than falcon (more detail pls)?	WCPSS uses CrowdStrike Falcon for endpoint protection, but specific license levels or add-on modules are not disclosed. Vendors should assume a standard deployment and describe how their SOC services scale to support endpoint security coverage
44	Page 5 Section Scope of Work	What is your MS Office 365 license type?	WCPSS uses Microsoft 365 across faculty, staff, and students, but specific license types are not shared. Vendors should assume a standard enterprise deployment and describe how their SOC services scale accordingly."
45	Page 6: 1.3 Level 3: Full Managed Detection & Response (MDR) 2. Technical Requirements:	Are you looking for hands on remediation past isolation for your response actions? What response actions are you looking for?	WCPSS expects the SOC to provide detection, isolation, and recommended response guidance. Vendors should describe the range of response actions their services support, without requiring disclosure of internal playbooks or workflows
46	Page 6: 4 Pricing and Commercials Pricing	Is this for a single-year pricing, with the option of multiyear including the multi-year discounting? What is your preference on term?	One year with the option to renew for four additional one-year terms
47	Page 6: 4 Pricing and Commercials Pricing	For Advisory Services - Section 4, What advisory services are mandatory to be included? Please specify in detail what should be included in advisory services?	Vendors should propose advisory services that complement SOC

			operations, such as risk assessments, threat intelligence guidance, and security best practices. Specific mandatory items or internal details are not disclosed at this stage
48	Page 6: 2.2 Future Integration Flexibility with Other Endpoint Solutions (Microsoft Security Suite or Similar Platforms**)**	Do you want your SOC / MDR to have integration / monitor and correlate logs from: firewall, backup (rubrik / veeam), Cloud environment, email?	Yes, the SOC/MDR should support integration, monitoring, and correlation across multiple sources, including firewalls, backup systems, cloud environments, and email. Vendors should describe how their services handle multi-source visibility and correlation at scale
49	Page 6: 2. Technical Requirements	Are you looking for Network Detection Response (NDR) to be included?	No, not at this time
50	Page 6: 2. Technical Requirements	Are you looking to include Managed Vulnerability Scanning?	No, not at this time
51	Page 5 Section Background	Per RFP, 20,000 staff in the district and 160,000 students. Can you please provide the specifics on how devices are broken out? This will affect licensing: a. How many Laptops and desktops (with running Windows or MAC OS): b. How many iPad and Chromebooks: c. How many Servers (Running ServerOS / Linux):	See Question #15
52	Page 5 Section Scope of Work	What is the specific level of licenses you currently have for Crowdstrike / name of licensing other than falcon (more detail pls)?	See Question #43
53	Page 5 Section Scope of Work	What is your MS Office 365 license type?	See Question #44
54	Page 6: 1.3 Level 3: Full Managed Detection & Response (MDR)	Technical Requirements: Are you looking for hands on remediation past isolation for your response actions? What response actions are you looking for?	See Question #45
55	Page 6: 4 Pricing and Commercials Pricing	Is this for a single-year pricing, with the option of multiyear including the multi-year discounting? What is your preference on term?	See Question #46
56	Page 6: 4 Pricing and Commercials Pricing	For Advisory Services - Section 4, What advisory services are mandatory to be included? Please specify in detail what should be included in advisory services?	See Question #47
57	Page 6: 2.2 Future Integration Flexibility with Other Endpoint Solutions (Microsoft Security Suite or Similar Platforms)	Do you want your SOC / MDR to have integration / monitor and correlate logs from: firewall, backup (rubrik / veeam), Cloud environment, email?	See Question #48

58	Page 6: 2. Technical Requirements	Are you looking for Network Detection Response (NDR) to be included?	See Question #39
59	Page 6: 2. Technical Requirements	Are you looking to include Managed Vulnerability Scanning?	See Question #50
60	RFP Section 2.1, Page 6	How many endpoints are being monitored with Crowdstrike Falcon?	See Question #15
61	RFP Section "QUALIFICATIONS", Page 6	Does Wake have ICS/SCADA networks requiring monitoring in the initial phase of deployment ["ICS/SCADA IoT" is mentioned as a desired skill but is never mentioned elsewhere] ○ If so, can any details be provided (# of IPs monitored, device types, any security tools deployed)	See above
62	RFP Section 1.2, Page 5	For the proposed level 2 monitoring and "Advanced Log Analysis", does Wake County have tools other than CrowdStrike Falcon they want monitored? ○ If so, can those be listed?	See Question #15
63	Reference: Organizational Background and Current Environment, Page 5	How many endpoints are being monitored with CrowdStrike Falcon	See Question #15
64	Qualifications, Page 6	Does Wake have ICS/SCADA networks requiring monitoring in the initial phase of deployment [They mention "ICS/SCADA IoT" as a desired skill but never mention it elsewhere] ○ If so, can any details be provided (# of IPs monitored, device types, any security tools deployed)	See above
65	1.2 Level 2: Monitoring + Limited Response Support, Page 5	For the proposed level 2 monitoring and "Advanced Log Analysis", does Wake County have tools other than CrowdStrike Falcon they want monitored? ○ If so, can those be listed?	See Question #15
66		**Current Environment & Integration** ● Can you provide more detail on your current CrowdStrike Falcon deployment (number of endpoints, OS types, integration points)? ● What other security solutions or SIEM platforms are currently in use (e.g., Splunk, Sentinel, others)? ● Are there existing integrations between CrowdStrike Falcon and other platforms (e.g., Microsoft Security Suite)? If so, which ones? ● What is the anticipated timeline for possible migration or integration with Microsoft Security Suite or other platforms?	WCPSS uses CrowdStrike Falcon and other security solutions, but specific endpoint counts, OS types, and integrations are not shared. Vendors should assume a hybrid environment and describe how their SOC services support scalable monitoring and integration across multiple security platforms _____ No specific timeline is shared at this stage. Vendors should describe how their SOC services can support migration or integration with Microsoft Security

			Suite or other platforms in a flexible and scalable manner
67		**Scope of Services & Responsibilities** ● For Level 2 and Level 3 SOC services, what are the expected volumes of security events/logs per day or month? ● Is vendor expected to provide Level 1 services, or just supplement/replace with Level 2 and 3? ● Will vendor have direct access to incident response tools, or will all actions be coordinated with WCPSS staff? ● Are forensic investigations to be performed remotely, onsite, or both? ● What is the expected frequency of proactive threat hunting and forensic investigations?	Specific volumes, access details, and frequencies are not shared. Vendors should describe how their SOC services support Level 1–3 coverage, remote or onsite forensic investigations, and proactive threat hunting in a scalable and coordinated manner
68		**3. Technical & Operational Requirements** ● What is the preferred method for communication and escalation (ticketing system, email, phone, SMS)? Are there systems already in use? ● Are there requirements for data residency, local storage, or specific regulatory compliance (beyond FERPA)? ● Are there any limitations or restrictions on remote access for incident response and management? ● Will vendor be responsible for the development and maintenance of incident response playbooks? If so, how many playbooks are currently in use?	Specific tools, compliance, access restrictions, and playbook counts are not shared. Vendors should describe how their SOC services support scalable communication, escalation, regulatory alignment, and playbook development or integration
69		**4. Reporting & SLAs** ● What are the required or expected SLAs for response times, containment, and remediation? ● What reporting cadence and format is preferred (daily, weekly, monthly, custom dashboards)? ● Are there specific metrics or KPIs WCPSS wants tracked and reported?	Specific SLA targets, reporting cadence, and KPIs are not shared at this stage. Vendors should describe how their SOC services provide flexible reporting, metrics, and SLA options to meet a variety of operational needs
70		**5. Personnel & Background Checks** ● For staff background checks, are there specific forms or procedures we must follow beyond the Lunsford Act requirements? ● Will any vendor staff need onsite presence, or is remote support sufficient for all SOC services?	Specific background check forms or procedures beyond statutory requirements are not shared. Vendors should describe how their SOC staff provide support remotely and, if applicable, onsite, in a scalable and compliant manner
71		**6. Pricing & Commercials** ● Does WCPSS prefer pricing by endpoint, log volume, fixed fee, or another structure? ● Should professional services (forensics, playbook development, advisory) be priced separately or included in base fees? ● Are there anticipated multi-year commitments or preferences for contract duration?	**6. Pricing & Commercials** "Preferred pricing structures and contract durations are not specified. Vendors should describe flexible pricing

		7. References & Qualifications ● Are references from private sector clients acceptable, or must all references be public-sector/education? ● Is experience with SCADA/ICS and IoT devices mandatory for all SOC staff, or only for select engagements? ● Are specific certifications required for all staff or only key personnel (e.g., OSCP, GXPN, GPEN)?	models, including endpoint, log volume, fixed fee, or professional services options." **7. References & Qualifications** "References may include public- or private-sector clients. Vendors should describe experience relevant to education, SCADA/ICS, IoT, and indicate which staff hold key certifications."
72		**8. Other Clarifications** ● Are there anticipated periods of increased activity (e.g., school start/end, holidays) that would require enhanced monitoring? ● Are there any known limitations with the current environment that could impact integration or service delivery? ● Is WCPSS open to pilot or proof-of-concept prior to full contract execution?	**8. Other Clarifications** ● "Vendors should assume variable activity periods and demonstrate how their SOC services scale to meet potential peaks." ● "Specific environment limitations are not shared. Vendors should describe how their solutions accommodate integration with diverse or distributed systems." ● "WCPSS is open to pilots or proof-of-concept arrangements. Vendors should outline how such engagements can demonstrate capability prior to full contract execution."