STATE OF OREGON
POSITION DESCRIPTION

Position Revised Date:
November 18th 2025

This position is:
☒ Classified
□ Unclassified
□ Executive Service
□ Mgmt Svc – Supervisory
□ Mgmt Svc – Managerial
□ Mgmt Svc - Confidential

Agency: The Department of Administrative Services

Division: Office of the State Chief Information Officer

□ New ☒ Revised

SECTION 1. POSITION INFORMATION

a.	Classification Title:	Information Systems Spec. 7	**b.**	Classification No:	
c.	Effective Date:		**d.**	Position No:	
e.	Working Title:	Security Analyst II – Threat Hunter	**f.**	Agency No:	
g.	Section Title:	Cyber Security Services	**h.**	Budget Auth No:	
i.	Employee Name:		**j.**	Repr. Code:	OAS

k. Work Location (City – County): Salem / Marion

l. Supervisor Name: Les DeFoor

m. Position: ☒ Permanent □ Seasonal □ Limited Duration □ Academic Year
☒ Full-Time □ Part-Time □ Intermittent □ Job Share

n. FLSA: □ Exempt ☒ Non-Exempt

If Exempt: □ Executive □ Professional □ Administrative

o. Eligible for Overtime: □ Yes ☒ No

SECTION 2. PROGRAM AND POSITION INFORMATION

a. Describe the program in which this position exists. Include program purpose, who's affected, size, and scope. Include relationship to agency mission.

The Department of Administrative Services ("DAS") is the central administrative agency that leads state government to implement the policy and budget decisions of the Governor and Oregon Legislature. Employing an enterprise-wide perspective, DAS serves state government by developing and upholding accountability standards to ensure productive and efficient use of state government's financial, human and information resources.

DAS provides a stable management infrastructure and essential business services including technology, financial, procurement, publishing/distribution, human resources and facility asset management. These services support and enable state and local government agencies to carry out their missions, benefiting all Oregonians.

The Office of the Oregon State CIO ("EIS") is a state government-wide information technology (IT) program led by Oregon's Chief Information Officer (CIO). The CIO is a statutory position appointed by the Governor and works closely with the COO and state leadership on adoption of statewide IT policies, standards and governance. EIS has independent statutory authority and is aligned with the DAS budget.

The office is funded by assessment and rates charged for the services provided.

EIS provides centralized oversight for enterprise-wide IT resource management, planning, policy, program development, project delivery and the setting of statewide IT standards. EIS provides training, and direction to ensure IT integrity, security and consistency across state agencies by working closely with elected officials, political subdivisions, state agencies and IT leadership. EIS team is built on collaboration and support. We work together to ensure our customer agencies receive the highest quality of service. We take pride in our work and look for ways to innovate. EIS is committed to hiring highly-skilled, diverse and dedicated employees who will bring a unique skill set to the team. The Office is comprised of the following sections: Data Center Services (DCS), Strategic IT Governance, Cyber Security Services (CSS), and Enterprise Shared Services.

The Cyber Security Services ("CSS") is an information security management section within EIS. It acts as a shared information security resource for the state of Oregon. CSS's mission: Leading Oregon Government to safeguard the State's information resources. CSS is comprised of the following units: Governance Risk and Compliance, Enterprise Security Architecture, Network Security, and Security Operations Center (SOC).

b. Describe the primary purpose of this position, and how it functions within this program. Complete this statement. The primary purpose of this position is to:

Continuously monitor Microsoft Sentinel and Defender XDR for security threats, perform initial triage to validate and assess alerts, and provide timely, actionable notification and escalation to support effective incident response and protect state agencies from cyber threats.

SECTION 3. DESCRIPTION OF DUTIES

List the major duties of the position. State the percentage of time for each duty. Mark "N" for new duties, "R" for revised duties or "NC" for no change in duties. Indicate whether the duty is an "Essential" (E) or "Non-Essential" (NE) function.

Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*

% of Time	N/R/NC	E/NE	DUTIES
10 %	R	E	**Customer Assistance (**Software 5 / Data 5): Mentor junior analysts by providing coaching on triage techniques, alert interpretation, escalation criteria, and behavioral analysis; delivering training on hunting tools, KQL/Sentinel queries, and Defender Advanced Hunting; reviewing investigations for accuracy and completeness; and developing reference materials, SOP guidance, and workshop content. Support agencies in understanding and interpreting threat-related data by assisting with exporting and analyzing security alert data, endpoint telemetry, authentication patterns, and network flows; explaining correlations and the relevance of suspicious patterns

			to MITRE ATT&CK techniques
50 %	R	E	**Operations** (Software 20 / Data 10)**:** Perform deep-dive investigations into escalated alerts, anomalies, and suspicious system behaviors by correlating endpoint, identity, cloud, and network telemetry across enterprise platforms such as Microsoft Sentinel, Defender, and EDR tools. Validate threat activity through behavioral analytics, anomaly detection methods, and MITRE ATT&CK mapping to identify attacker tradecraft, including credential abuse, privilege escalation, lateral movement, and command-and-control activity. Aggregate and analyze threat data across SIEM, EDR, firewall, identity, and email systems to identify coordinated attack patterns, correlating intelligence from multiple threat feeds, and detecting indicators not identified by automated tools. Conduct deep-dive investigations on escalated alerts using behavioral analytics and multi-source telemetry correlation. • Serve as authoritative decision-maker for incident validation, severity classification, and escalation. • Identify attacker techniques and behaviors aligned to MITRE ATT&CK, including credential abuse, privilege escalation, and lateral movement. • Develop and execute advanced hunting queries to uncover hidden or stealthy threat activity. • Correlate detection data across SIEM, EDR, identity, firewall, cloud, and email systems to identify coordinated threats. • Integrate and analyze threat intelligence from multiple feeds to enhance situational awareness and detection fidelity. • Monitor and validate SOC telemetry pipelines and log ingestion to ensure enterprise visibility and detection coverage. • Coordinate with engineering teams to remediate ingestion failures, detection gaps, or degraded analytics capabilities.
15 %	R	E	**Construction** (Software 10 / Data 5)**:** Develop and enhance enterprise threat hunting capabilities by creating new Sentinel analytics rules, advanced hunting queries, and behavior-based detections aligned with MITRE ATT&CK

			techniques. Make recommendations which helps tune existing detections to improve accuracy, reduce false positives, and maintain strong detection fidelity, and develop repeatable playbooks to identify emerging or persistent attacker TTPs. Collaborates with engineering and architecture teams to validate, test, and operationalize new SIEM and EDR capabilities, while contributing to SOC content engineering through enhancements to UEBA logic, SOAR playbooks, and detection libraries.
20 %	R	E	**Planning** (Software 10 / Data 10)**:** Develop and enhance enterprise detection capabilities by creating new Sentinel analytics rules, advanced hunting queries, and behavior-based detections aligned to MITRE ATT&CK, while tuning existing content to maintain high fidelity and reduce false positives. Build reusable hunting playbooks targeting recurring attacker behaviors and continuously evaluate emerging methodologies, detection models, automation improvements, and analytical techniques to advance the SOC's threat-hunting maturity. Integrate new telemetry sources, including identity, cloud, network, and email data, into hunting workflows and validates new SIEM/EDR features, ingestion pipelines, and analytics in collaboration with engineering and architecture teams. Assist with improving the SOC content such as UEBA models, SOAR playbooks, correlation rules, and detection libraries; producing technical documentation for detection logic; and testing new analytics in lab and production environments. Stay current on trending security issues.
5%	R	NE	Other duties as assigned
100%			

SECTION 4. WORKING CONDITIONS

Describe any on-going working conditions. Include any physical, sensory, and environmental demands. State the frequency of exposure to these conditions.

This position is suitable for remote hybrid work options.

This position will spend large amounts of time utilizing computer equipment, computer monitors, typing and viewing data on electronic screens.

This position can spend large amounts of time sitting or standing in one place while performing tasks.

This position works in a very distractive environment and requires the ability to shift tasks and focus often.

Duties are performed in an office environment working at a computer terminal for long periods of time, working in or around noisy machinery.

Business needs may require working irregular hours or shift work (24/7, weekends, evenings, holidays, and travel for job related purposes) in order to do work or make changes or maintenance that are not approved to be done during the hours of 6am – 6pm.

Business needs may require re-assignment to one of three shifts (days, swing or graveyard) and with short notice.

Driver's license is required or satisfactory means of transportation.

SECTION 5. GUIDELINES

a. List any established guidelines used in this position, such as state or federal laws or regulations, policies, manuals, or desk procedures.

This position is designated as an "Essential Position" (State Policy #60.015.01) in all cases of official state office closures. The incumbent in this position is required to report to work in all cases of official notification of state office closures.

Exceptions: previously approved vacation and absences. This position may be assigned tasks outside the normal position duties to respond to the special conditions of the closures. If reporting to your normal work location is deemed too dangerous, then you must contact your supervisor to be reassigned to an alternate and/or remote location.

Oregon Revised Statutes

- Oregon Administrative Rules
- Department of Administrative Services Policies and Procedures
- Enterprise Information Security Strategy
- EIS Strategic and Section Plans
- Statewide Information Security Plan & Standards
- NIST SP 800-53 R5 Security and Privacy Controls
- NIST SP 800-30 Risk Management Guide for Information Technology Systems
- NIST SP 800-37 Guide for Applying the Risk Management Framework
- All Other Applicable Statewide, DAS, and EIS Policies, Procedures and Standards
- Federal and State government regulations including:
  - Criminal Justice Information Services (CJIS)
  - Federal Information System Management Requirements (FISMA)
  - IRS Publication 1075
  - HIPAA Security and Privacy Rules
  - Oregon Consumer Information Protection Act

Other Best Practices Resources, such as ISO 27000 series, Common Criteria, National Institute for Standards and Technology (NIST SP-800 series), CIS Controls, etc...

b. How are these guidelines used?

The above guidelines provide general guidance and policy directions, and a framework that should be applied as necessary for each application. This includes decisions concerning the appropriate application and interpretation of policies and procedures that relate to highly sensitive confidential information.

They are used to determine correct operational procedures necessary for efficient and secure operation of statewide computer systems including work processes and procedures that ensure consistent quality of services.

SECTION 6. WORK CONTACTS

With whom, outside of co-workers in this work unit, must the employee in this position regularly come in contact?

Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*

Who Contacted	How	Purpose	How Often?
Agency Customers	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily
Managers/co-workers	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily
Vendors	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries, coordination	Daily
Other State Employees	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily

SECTION 7. POSITION RELATED DECISION MAKING

Describe the typical decisions of this position. Explain the direct effect of these decisions.

This position must exercise discretion and independent judgement in making decisions and resolving cyber threat findings or vulnerabilities within the state security operations center.

This position must know when to escalate cyber threat findings with agencies following policies and procedures within the State and Cyber Security Services.

This position will make decisions based on system reporting to assist agencies in deciding priorities within the scope of vulnerabilities.

This position may act independently but will consult with management before any final actions are taken.

Decisions and directions by this position will directly affect major functions within agencies and the enterprise cyber security program which could result in serious effects on over all agency technology utilization.

SECTION 8. REVIEW OF WORK

Who reviews the work of the position?

Classification Title	Position Number	How	How Often	Purpose of Review
IT Cyber Security Manager 2	1970060	In person, phone, email, by letter or electronic means	Daily/Weekly	To determine if corrective actions or directions are needed. To stay informed of active threats.
IT Cyber Security Manager 2	1970060	In person, phone, email, by letter or electronic means	Quarterly	Performance Accountability Feedback

SECTION 9. OVERSIGHT FUNCTIONS THIS SECTION IS FOR SUPERVISORY POSITIONS ONLY

a. How many employees are directly supervised by this position? N/A

How many employees are supervised through a subordinate supervisor? 0

b. Which of the following activities does this position do?

□ Plan work
□ Assigns work
□ Approves work
□ Responds to grievances
□ Disciplines and rewards

□ Coordinates schedules
□ Hires and discharges
□ Recommends hiring
□ Gives input for performance evaluations
□ Prepares & signs performance evaluations

SECTION 10. ADDITIONAL POSITION-RELATED INFORMATION

ADDITIONAL REQUIREMENTS: List any knowledge and skills needed at time of hire that are not already required in the classification specification:

This position is subject to a criminal records check, which may require fingerprints. If you are offered employment, the offer will be contingent upon the outcome of a criminal records check (FBI). Any history of criminal activity will be reviewed and could result in the withdrawal of the offer or termination of employment.

This position is required to maintain an active Criminal Justice Information Services (CJIS) background clearance and must successfully complete annual CJIS security awareness training to retain access to sensitive systems and data.

You are responsible to promote and foster a diverse and discrimination/harassment-free workplace; establish and maintain professional and collaborative working relationships with all contacts; contribute to a positive, respectful and productive work environment; maintain regular and punctual attendance; perform all duties in a safe manner; and comply with all policies and procedures. Working in a team oriented environment requires participative decision making and cooperative interactions among staff and management. You are to be aware of Affirmative Action and the department's Diversity strategies and goals.

Additional skills, abilities and requirements:

Technical

- Strong experience with: Microsoft Defender for Endpoint, Identity, Office 365, and Cloud Apps, Attack surface reduction (ASR), device timeline, evidence& response actions, Live response sessions and EDR forensics.
- Ability to perform deep incident investigation using Sentinel's Investigation Graph and entity behavior analysis.
- Ability to pivot across tools (e.g., Defender → Sentinel → Purview → Entra logs → Tenable One).
- Advanced KQL (Kusto Query Language) capability including ability to build complex queries, joins, unions, time-series queries, anomaly detection patterns, custom hunting queries, and scheduled analytics rules.
- Strong proficiency in analyzing logs from: Entra ID sign-in logs, Office 365 audit logs, Windows event logs (including Sysmon),Network/Firewall logs
- Skilled in analyzing telemetry across multiple data sources, especially cloud + identity + endpoint
- Understanding of attacker TTPs and how to map alerts to the MITRE ATT&CK matrix.
- Capable of drafting response actions, such as isolating devices, blocking IPs, disabling accounts, or updating detection rules.
- Demonstrated ability to develop and implement statewide strategies, standards, and policies governing vulnerability management operations across multiple agencies and jurisdictions.
- Ability to evaluate, select, and manage vendor solutions, including defining technical requirements, overseeing procurement, and monitoring contractual performance.
- Ability to work under pressure during active threats or spikes in alert volume.
- Strong documentation and report-writing skills (RCA reports, detection logic, hunting notes).
- Ability to mentor or guide junior analysts (typical for Analyst II roles).
- Capacity to assess statewide risk, identify strategic improvement opportunities, and develop multi-year roadmaps and plans for vulnerability management program maturity.
- Strong leadership and collaboration skills to build consensus among stakeholders, including agency leadership, executive sponsors, federal partners, and vendor representatives.
- Ability to interpret, implement, and enforce complex regulatory requirements, such as CJIS, IRS Pub 1075, HIPAA, and State of Oregon Information Security Standards.
- Demonstrated commitment to maintaining an active CJIS background clearance and completing annual CJIS security training as required.

Problem Solving

- Capable of developing hypothesis-driven hunting campaigns (threat intel, MITRE ATT&CK-based, behavior-based).
- Ability to understand and evaluate Lateral movement patterns, Persistence mechanisms, Living of the land activity, suspicious cloud or identity behaviors.
- Must be capable of approaching complex technical and organizational problems logically and systematically, often in environments with no established precedent.
- Ability to quickly learn and apply new concepts, tools, and techniques in dynamic situations.
- Requires advanced technical and analytical skills demonstrated in enterprise or highly secure environments.
- Strong analytical mindset; able to draw conclusions from incomplete data.
- Ability to troubleshoot multi-layered technical issues, including cross-platform integration failures, data consistency problems, and performance bottlenecks.
- Skill in analyzing and interpreting large, complex vulnerability datasets to support risk decisions and reporting.

Interpersonal and Communication

- Effective communication with both technical and non-technical stakeholders.

- Ability to explain complex cybersecurity and data architecture issues clearly to non-technical stakeholders, including agency executives and policy makers.
- Proven skill in establishing and maintaining effective working relationships across agency teams, leadership groups, and external partners.
- Ability to prioritize, schedule, and manage multiple high-impact initiatives concurrently to meet critical deadlines and program objectives.

BUDGET AUTHORITY: If this position has authority to commit agency operating money, indicate the following:

Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*

Operating Area	Biennial Amount ($00000.00)	Fund Type
N/A	N/A	N/A

SECTION 11. ORGANIZATIONAL CHART

Attach a current organizational chart. Be sure the following information is shown on the chart for each position: classification title, classification number, salary range, employee name and position number.

SECTION 12. SIGNATURES

Employee Signature　　Date　　Supervisor Signature　　Date

Appointing Authority Signature　　Date