**Threat Hunting**

**FY25 Performance Guidance**

**Engineering & Operations Services (EOS)**

**General guidance for EOS supervisors when creating performance plans.**

Goals and performance indicators are set for senior employees (GS-14 and GS-15). Supervisors should adjust the goals to meet the experience level of the employee. For example, if the goal states:  
Task completion percentage: This will be tracked quarterly to ensure that at least 90% of assigned tasks are completed on time.  
  
The measure should be adjusted to meet expectations based on the responsibilities and seniority of the employee.   
Midlevel: Task completion percentage: This will be tracked quarterly to ensure that at least 85% of assigned tasks are completed on time.

Junior: Task completion percentage: This will be tracked quarterly to ensure that at least 75% of assigned tasks are completed on time.

The expectations should be uniform for all employees at the same grade level.

|  |  |
| --- | --- |
| **Threat Hunting FY25 Performance Goal (25%)** | |
| Threat Hunting FY25 Performance Goal | |
| **Achieved Expectations** | **Achieved Excellence** |
| * Support inputs necessary that enable the organization to track and measure performance. Inputs will be provided though the appropriate channels at the cadence dictated by leadership. * Provide on the appropriate cadence and through appropriate channels to support inputs for measures and metrics. * Follow all “Flexible Work Environment Principles.” This includes that teammates will be on camera during virtual meetings when working from unclassified spaces; exceptions to this should be rare and explicitly approved by the meeting organizer. * Follow all TH policy and guidance regarding operational and programmatic decision making. Decisions shall be made at the appropriate levels of the organization (e.g., executive vs. manager) and be effectively communicated to relevant stakeholders. * Assist in process and procedure development in accordance with redesign goals. For example, support and assist in the development of branch or section-level concept of operations (CONOPS) or other project-related documents; participate in a working group relevant to your role, respond to project surveys on-time, or other equivalent asks. * Complete Federal Acquisition Certification (FAC) Training Course 043 - Ethics & Procurement Integrity. Provide certificate to direct supervisor by August 1, 2025 | * In addition to the “Achieved Expectations” requirements, * Identify at least three (3) innovative (concept, process improvement, and/or technology) improvements for the subdivision, document and submit:   + If only relevant to the section, submit to section chief.   + If only related to the branch, submit to branch chief.   + If related to subdivision, submit to AD/DAD review via chain of command. * Submit work-related achievements/ accomplishments at minimum once per month in writing to your supervisor and/or Branch Chief. * Be nominated by your Office, Branch Chief, Deputy Branch Chief, or first-line supervisor for a TH, CSD, and/or CISA individual award during the FY25 performance cycle. Award nominations should be made for individuals who have distinguished themselves by making outstanding and extraordinary contributions to CISA’s mission. |

|  |  |
| --- | --- |
| **Capability Development & Engineering (CDE) Section Goal (35%)** | |
| Establish a robust CDE section that effectively collaborates with stakeholders to deliver value-added capabilities that meet their needs. | |
| **Achieved Expectations** | **Achieved Excellence** |
| **Establish a deep understanding of stakeholder needs, pain points, and aspirations through engagement and analysis.**   * Directly contribute to at least 2 stakeholder engagements (meetings, workshops, surveys) with each primary stakeholder group (TH branch) by the end of Q4 FY25. * Collect feedback from stakeholders to inform future capability development. * Establish a basic understanding of stakeholder roles, responsibilities, and expectations.   **Design and develop innovative solutions to address specific stakeholder challenges.**   * Directly contribute to the development of at least two (2) innovative solutions to address specific stakeholder challenges by the end of FY25. * Collaborate with cross-functional teams to integrate capabilities into existing systems and processes. * Establish a culture of continuous learning and improvement, incorporating emerging technologies and best practices. | **Establish a deep understanding of stakeholder needs, pain points, and aspirations through engagement and analysis.**   * Conduct at least 1 comprehensive, in-depth stakeholder engagement (e.g., a workshop), with TH/PH or TH/IR, by the end of Q4 FY25. * Develop a detailed, data-driven analysis of stakeholder needs and pain points by end of Q4 FY25. * Establish a thorough, documented, understanding of stakeholder expectations, including specific requirements and constraints by the end of Q4 FY25.   **Design and develop innovative solutions to address specific stakeholder challenges.**   * Spearhead the development of four (4) innovative solutions to address specific stakeholder challenges by the end of FY25. * Successfully integrate capabilities into existing systems and processes, resulting in significant, measurable, and documented mission value. * Establish a deep understanding of emerging technologies and best practices, including ability to apply them to complex problems. |

|  |  |
| --- | --- |
| **Individual Goal (40%) – Helen Hauer** | |
| Improve data access and useability for Threat Hunting users and enhance the overall quality and governance of Threat Hunting data through strategic initiatives and collaborative efforts. Demonstrate the viability and effectiveness of migrating Threat Hunting data into a common standard. Develop a data pipeline to process, store, and analyze Threat Hunting data. Implement an overall data governance program to manage all Threat Hunting data. | |
| **Achieved Expectations** | **Achieved Excellence** |
| **Demonstrate the viability and effectiveness of migrating Threat Hunting data into a common standard.**   * Identify at least one analytic, query, or set of queries to assess using Open Cybersecurity Schema Framework (OCSF)-mapped data. * Transform an appropriate data set accessed by the analytic, query, or set of queries to OCSF to create a sample standardized data set. * Modify the analytic, query, or set of queries to use the sample standardized data set. * By the end of Q4 FY25, test at least one (1) data transformation with sample data in a development environment in the CISA Data as a Service (CDaaS) Platform.   **Develop a data pipeline to process, store, and analyze Threat Hunting data.**   * Directly contribute to the development of a data pipeline within the Threat Hunting and CISA/CSD Enterprise Architecture. * Migrate at least one (1) existing Threat Hunting data source to the data pipeline service. * Standardize at least one (1) existing migrated data source within the data pipeline service to a common data standard. * By the end of Q4 FY25, test at least one (1) Use Case within the CDaaS Platform development environment using sample data.   **Implement an overall data governance program to manage all Threat Hunting data.**   * Directly contribute to the management of all Threat Hunting data into the CSD Data Catalog. * Catalog at least one (1) Threat Hunting data asset within the CSD Data Catalog. * Catalog at least one (1) Threat Hunting data analytic within the CSD Data Catalog. | **Demonstrate the viability and effectiveness of migrating Threat Hunting data into a common standard.**   * Demonstrate an improvement in query performance that makes the sample data set more manageable and searchable. * Demonstrate Indicator of Compromise (IOC) detections by utilizing sample data transformed into a common standard. * Create a new analytic, query, or set of queries to demonstrate a novel use of the standardized data set. * By the end of Q4 FY25, test at least two (2) data transformations with sample data in a development environment in the CDaaS Platform.   **Develop a data pipeline to process, store, and analyze Threat Hunting data.**   * Spearhead the development of a data pipeline within the Threat Hunting and CISA/CSD Enterprise Architecture. * Migrate at least two (2) existing Threat Hunting data sources to the data pipeline service. * Standardize at least two (2) existing migrated data sources within the data pipeline service to a common data standard. * By the end of Q4 FY25, test at least two (2) Use Cases within the CDaaS Platform development environment using sample data.   **Implement an overall data governance program to manage all Threat Hunting data.**   * Spearhead the management of all Threat Hunting data by leading the Data Maturity Assessment on behalf of Threat Hunting and coordinating responses across the Subdivision. * Catalog at least two (2) Threat Hunting data assets within the CSD Data Catalog. * Catalog at least two (2) Threat Hunting data analytics within the CSD Data Catalog. |

|  |  |
| --- | --- |
| **Individual Goal (40%) – Laura Malone** | |
| Spearhead a data normalization pilot project to map and transform Threat Hunting data into a common data standard. Demonstrate the viability and effectiveness of migrating Threat Hunting data into a common standard. Develop a data pipeline to process, store, and analyze Threat Hunting data. | |
| **Achieved Expectations** | **Achieved Excellence** |
| **Spearhead a data normalization pilot project to map and transform Threat Hunting data into a common data standard.**   * Conduct research on the Open Cybersecurity Schema Framework (OCSF) as a common data standard. * Complete field mappings for at least one (1) data source to OCSF. * Document the data transformation logic to normalize fields to OCSF for at least one (1) data source.   **Demonstrate the viability and effectiveness of migrating Threat Hunting data into a common standard.**   * Identify at least one analytic, query, or set of queries to assess using OCSF-mapped data. * Transform an appropriate data set accessed by the analytic, query, or set of queries to OCSF to create a sample standardized data set. * Modify the analytic, query, or set of queries to use the sample standardized data set. * By the end of Q4 FY25, test at least one (1) data transformation with sample data in a development environment in the CISA Data as a Service (CDaaS) Platform.   **Develop a data pipeline to process, store, and analyze Threat Hunting data.**   * Directly contribute to the development of a data pipeline within the Threat Hunting Enterprise Architecture. * Migrate at least one (1) existing Threat Hunting data source to the data pipeline service. * Standardize at least one (1) existing migrated data source within the data pipeline service to a common data standard. * By the end of Q4 FY25, test at least one (1) Use Case within the CDaaS Platform development environment using sample data. | **Spearhead a data normalization pilot project to map and transform Threat Hunting data into a common data standard.**   * Conduct research into at least one (1) additional common data standard as an alternative to OCSF. * Complete field mappings for at least two (2) data sources to OCSF. * Document the data transformation logic to normalize fields to OCSF for at least two (2) data sources.   **Demonstrate the viability and effectiveness of migrating Threat Hunting data into a common standard.**   * Demonstrate an improvement in query performance that makes the sample data set more manageable and searchable. * Demonstrate Indicator of Compromise (IOC) detections by utilizing sample data transformed into a common standard. * Create a new analytic, query, or set of queries to demonstrate a novel use of the standardized data set. * By the end of Q4 FY25, test at least two (2) data transformations with sample data in a development environment in the CDaaS Platform.   **Develop a data pipeline to process, store, and analyze Threat Hunting data.**   * Spearhead the development of a data pipeline within the Threat Hunting and CISA/CSD Enterprise Architecture. * Migrate at least two (2) existing Threat Hunting data sources to the data pipeline service. * Standardize at least two (2) existing migrated data sources within the data pipeline service to a common data standard. * By the end of Q4 FY25, test at least two (2) Use Cases within the CDaaS Platform development environment using sample data. |

|  |  |
| --- | --- |
| **Individual Goal (40%) – Michael Tipton** | |
| Redesign the Technical Engagement Network (TEN) to reduce or eliminate redundant capabilities, integrate with Enterprise Services, implement zero-trust principles, and refactor and modernize Threat Hunting capabilities. Develop a comprehensive service map of all CISA capabilities and applications utilized by Threat Hunting across all Agency networks, ensuring seamless integration, efficient resource allocation, and improved user experience. Develop a data pipeline to process, store, and analyze Threat Hunting data. | |
| **Achieved Expectations** | **Achieved Excellence** |
| **Redesign the TEN to reduce or eliminate redundant capabilities, integrate with Enterprise Services, implement zero-trust principles, and refactor and modernize Threat Hunting capabilities.**   * Directly contribute to the development of a comprehensive Threat Hunting Enterprise (TEN and Cloud) network redesign plan that outlines the scope, timeline, and budget for the project by Q4 FY25. * Ensure the plan includes clear objectives, metrics, and key performance indicators (KPIs) to measure success. * Implement the reduction or elimination of two (2) redundant CDE Team-managed capabilities by Q3 FY25. * Integrate two (2) CDE Team-managed capabilities with CISA and CSD Enterprise Services by Q4 FY25.   **Develop a comprehensive service map of all CISA capabilities and applications utilized by Threat Hunting across all Agency networks, ensuring seamless integration, efficient resource allocation, and improved user experience.**   * Identify and document all TH tools and applications used across all CISA networks by the end of Q3 FY25. * Categorize and group similar services into logical categories by Q3 FY25. * Develop an understanding of how service dependencies and integrations impact the overall service map, taking into account factors like network enclave, service owner, and customer utilization, by Q4 FY25   **Develop a data pipeline to process, store, and analyze Threat Hunting data.**   * Directly contribute to the development of a data pipeline within the Threat Hunting and CISA/CSD Enterprise Architecture. * Migrate at least one (1) existing Threat Hunting data source to the data pipeline service. * Standardize at least one (1) existing migrated data source within the data pipeline service to a common data standard. * By the end of Q4 FY25, implement at least one (1) Use Case within the CDaaS Platform. | **Redesign the TEN to reduce or eliminate redundant capabilities, integrate with Enterprise Services, implement zero-trust principles, and refactor and modernize Threat Hunting capabilities.**   * Ensure TEN Redesign plan and implementation complies with CISA Zero-trust and Secure by Design guidelines. * Implement the reduction or elimination of four (4) redundant CDE Team-managed capabilities by Q4 FY25. * Integrate four (4) CDE Team-managed capabilities with CISA and CSD Enterprise Services by Q4 FY25. * Refactor and modernize two (2) CDE Team-managed capabilities by Q4 FY25.   **Develop a comprehensive service map of all CISA capabilities and applications utilized by Threat Hunting across all Agency networks, ensuring seamless integration, efficient resource allocation, and improved user experience.**   * The service map is accessible to stakeholders through a user-friendly interface by the end of Q4 FY25. * The service map should include alerts and notifications for potential issues or anomalies in the service map by the end of Q4 FY25. * A report on the current state of the service map and its implications for resource allocation and user experience must be generated and presented to TH senior management by the end of Q4 FY25.   **Develop a data pipeline to process, store, and analyze Threat Hunting data.**   * Spearhead the development of a data pipeline within the Threat Hunting and CISA/CSD Enterprise Architecture. * Migrate at least two (2) existing Threat Hunting data sources to the data pipeline service. * Standardize at least two (2) existing migrated data sources within the data pipeline service to a common data standard. * By the end of Q4 FY25, implement at least two (2) Use Cases within the CDaaS Platform. |