CyberVista

Cyber Insights Report

Client: [redacted]
Course: NICE Workforce Diagnostic
Report Date: November 19, 2021

Quick Navigation:

- Executive Summary 2
- Knowledge/Skills Analysis 5
- Appendix A: 22

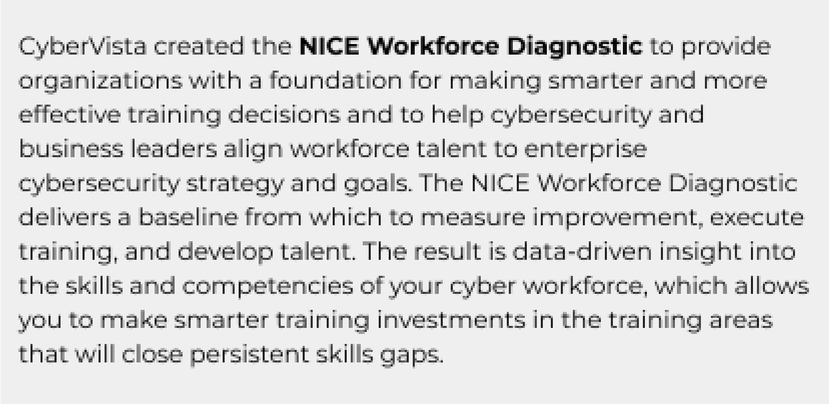
Executive Summary

CyberVista's Cyber Insights Reports provide clients with discrete analytical insights related to the knowledge and skill areas of teams. Cyber Insights Reports draw out specific conclusions based on the results of a diagnostic and/or a training implementation (i.e., a course or other training initiative).

We do this by analyzing a variety of data points including initial diagnostic scores, demographic data, course engagement (when applicable), and final assessment performance (when applicable). Using these data points – in addition to CyberVista's industry knowledge about the Cyber/IT workforce writ large – CyberVista illustrates skill/knowledge improvements as well as provides additional analytic findings related to the cohort itself.

Participants in this [redacted] cohort were enrolled in CyberVista's NICE Workforce Diagnostic. The NICE Workforce Diagnostic provides cybersecurity leaders and practitioners with visibility into cybersecurity competencies across all seven categories of the NICE Cybersecurity Workforce Framework. Those categories are: Analyze, Collect & Operate, Investigate, Operate & Maintain, Oversee & Govern, Protect & Defend, and Securely Provision.

Analyze | Collect and Operate | Investigate | Operate and Maintain | Oversee and Govern | Protect and Defend | Securely Provision



CyberVista created the **NICE Workforce Diagnostic** to provide organizations with a foundation for making smarter and more effective training decisions and to help cybersecurity and business leaders align workforce talent to enterprise cybersecurity strategy and goals. The NICE Workforce Diagnostic delivers a baseline from which to measure improvement, execute training, and develop talent. The result is data-driven insight into the skills and competencies of your cyber workforce, which allows you to make smarter training investments in the training areas that will close persistent skills gaps.

Key observations and recommendations:

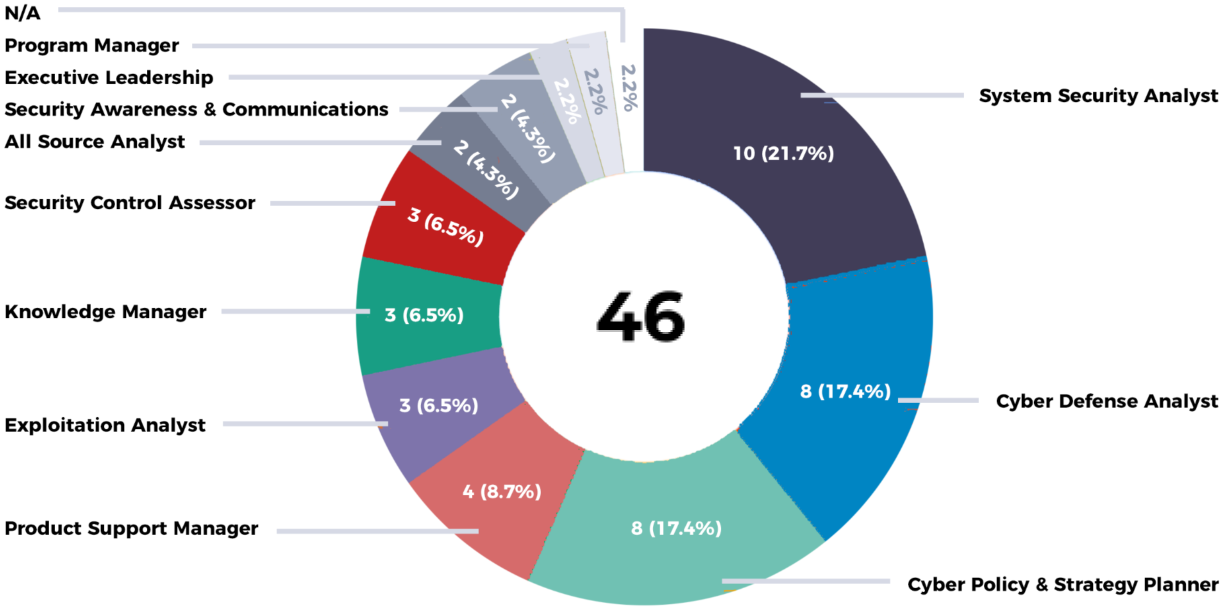
Collectively, the [redacted] cohort exhibited the greatest proficiency in Oversee & Govern (65% proficiency) and Collect & Operate (54% proficiency). As groups of participant scoring were analyzed by the NICE job role for which they are aligned, CyberVista was able to identify potential training opportunities for those groups to increase any identified knowledge/skills gaps. Performance scoring can always be positively or negatively skewed by an individual's results (outliers), therefore CyberVista always encourages our clients to also evaluate performance at the individual level when considering training implementations or opportunities. Key takeaways from our analysis of the job role groupings include:

Job Role	Training Considerations/Recommendations
SYSTEM SECURITY ANALYST (OM-ANA-001)	● CyberVista's Critical Knowledge Course, or a configured version of it (Threats & Attacks, Network Security, Security Engineering, and Offensive & Defensive Schema Units) ● CyberVista's Cloud Security Essentials course ● Security+ Certification
CYBER DEFENSE ANALYST (PR-CDA-001)	● CyberVista's SOC Analyst Course ● Evaluate needs of employees at the individual level as some may benefit from additional training opportunities such as CyberVista's Incident Response Course or even CyberVista's Critical Knowledge Course, or a configured version thereof (Threats & Attacks, Security Operations, and Offensive & Defensive Schema Units)
CYBER POLICY AND STRATEGY PLANNER (OV-SPP-002)	● CyberVista's Executive Cyber Risk Program ● CyberVista comprehensive CISM certification training course
PRODUCT SUPPORT MANAGER (OV-PMA-003)	● No significant recommendations at this time. [redacted] should evaluate training needs on an individual basis.
EXPLOITATION ANALYST (AN-EXP-001)	● CyberVista's comprehensive CEH Certification course ● CyberVista's Critical Knowledge Course, or a configured version thereof (Threats & Attacks, Security Operations, and Offensive & Defensive Schema Units) ● CyberVista's SOC Analyst Course ● GIAC Open Source Intelligence (GOSI)
KNOWLEDGE MANAGER (OM-KMG-001)	● No significant recommendations at this time. [redacted] should evaluate training needs on an individual basis.

SECURITY CONTROL ASSESSOR (SP-RSK-002)	● Due to scores, varies by individual performance, [redacted] should evaluate the needs of individuals with this job role on a case-by-case basis.
ALL-SOURCE ANALYST (AN-ASA-001)	● GIAC Cyber Threat Intelligence (GCTI), or EC-Council's Certified Threat Intelligence Analyst (C|TIA) certifications ● GIAC Open Source Intelligence (GOSI) ● Other all source intelligence focused courses or training programs
CYBER WORKFORCE DEVELOPER AND PLANNER' (OV-SPP-001)	● No significant recommendations at this time. [redacted] should evaluate training needs on an individual basis.
EXECUTIVE CYBER LEADERSHIP (OV-EXL-001)	● No significant recommendations at this time. [redacted] should evaluate training needs on an individual basis.
PROGRAM MANAGER (OV-PMA-001)	● No significant recommendations at this time. [redacted] should evaluate training needs on an individual basis.

Knowledge/Skills Analysis

The Participants:
The participants in this NICE Workforce Diagnostic consisted of a diverse group of 46 U.S-based [redacted] employees. The cohort included cybersecurity related professionals that represented a diverse set of cybersecurity job roles (11 roles, in fact); there was one participant of the diagnostic who does not currently hold a cyber-related role (categorized as “N/A” in the job role breakout). Overall, the results from the [redacted] cohort reflects a diverse set of knowledge/skills across the seven NICE categories for which they were assessed, which is to be expected given the diversity of the roles represented by the participants.



Certifications	Quantity
AWS CCP (Amazon)	2
Security+ (CompTIA)	3
PMP (PMI)	1
GSEC (GIAC)	3
CRISC (ISACA)	2
CISSP (IS2)	4
Other	6
None	8
Prefer not to answer	3

Overall Cohort Competency Profile

Collectively, the [redacted] cohort exhibited the greatest proficiency in Oversee & Govern (65% proficiency) and Collect & Operate (54% proficiency). When analyzing a cohort where the participants represent a number of different job roles, collective scoring and averages become less meaningful when looking at potential recommendations of improvement for teams, roles, or individuals; that said, the data can be useful as a general overview of the general proficiency of the larger workforce being analyzed. In other words, given the number of job roles represented by the participants, the data helps to answer the question "is there adequate coverage [or proficiency] across the NICE categories of skills." With more roles represented, the data would typically show well-roundedness of proficiency across the seven NICE categories. In this case with these [redacted] participants, the data does exhibit rounded representation of skill areas.

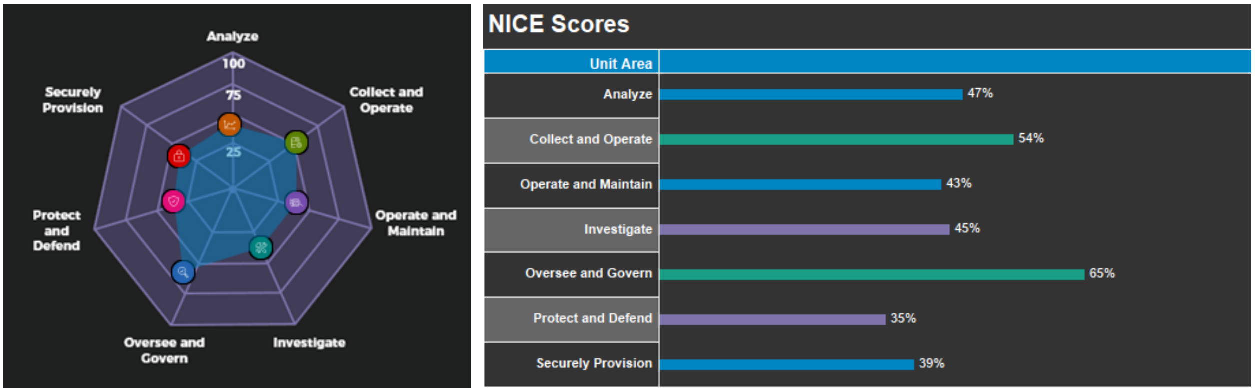
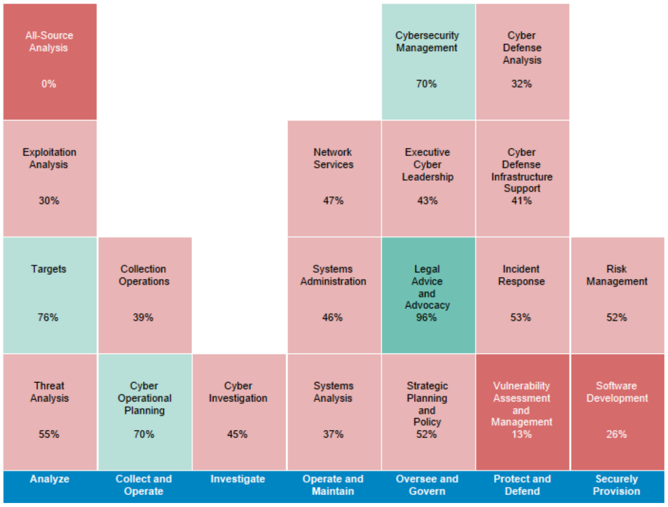


Figure 1 – Average scoring of all [redacted] participants across the seven categories of the NICE framework. Left image displays outcomes as a radar chart; right image illustrates the same results as a bar chart.

To dive into greater granularity of skills across these seven categories of the NICE framework, our diagnostic measures proficiencies at the specialty area. The CyberVista Workforce Diagnostic effectively measures against 20 of the 33 NICE specialty areas. Analyzing the performance outcomes at the specialty area allows us to evaluate whether proficiency is exhibited in the right area(s) for participants' indicated job roles. Typically with each job role there are one to five specialty areas of relevance; that is where we pay most of our attention when analyzing performance results.

Figure 2 illustrates the collective results of the [redacted] cohort at the specialty level. This view allows us to identify areas of knowledge and skill proficiency and deficiency when we analyze the participants grouped by their designated job roles.



Analyze	Collect and Operate	Investigate	Operate and Maintain	Oversee and Govern	Protect and Defend	Securely Provision
All-Source Analysis 0%				Cybersecurity Management 70%	Cyber Defense Analysis 32%	
Exploitation Analysis 30%			Network Services 47%	Executive Cyber Leadership 43%	Cyber Defense Infrastructure Support 41%	
Targets 76%	Collection Operations 39%		Systems Administration 46%	Legal Advice and Advocacy 96%	Incident Response 53%	Risk Management 52%
Threat Analysis 55%	Cyber Operational Planning 70%	Cyber Investigation 45%	Systems Analysis 37%	Strategic Planning and Policy 52%	Vulnerability Assessment and Management 13%	Software Development 26%

Performance Analysis by Job Role

SYSTEM SECURITY ANALYST (OM-ANA-001)

NICE describes the role of a System Security Analyst as: “Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.”

Of the [redacted] participants, 22% (n=10) represented the System Security Analyst job role, which nests underneath the ‘Operate & Maintain’ category and the ‘Systems Analysis’ specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the ‘**Systems Analysis**’ specialty area, as well as other periphery specialty areas such as ‘System Administration,’ and ‘Network Services,’ ‘Targets,’ and ‘Threat Analysis’ given some overlap in knowledge and skill areas shared between roles within those specialty areas.

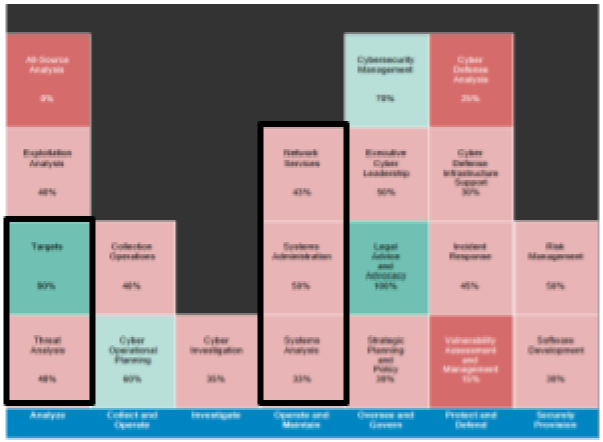
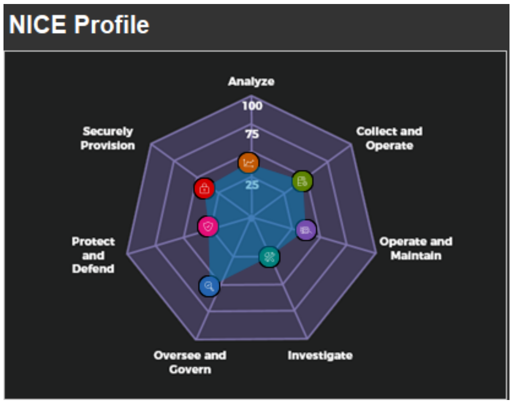


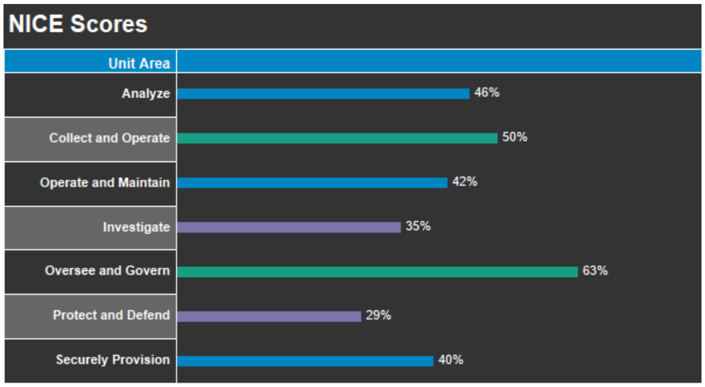
Figure 3 – Heat table scores at specialty area level for participants holding the job role “System Security Analyst”

<u>Observations & Recommendations</u>

While the Systems Security Analysts did well in ‘Targets,’ there is opportunity for skill development for this team. Consider:

1. CyberVista’s [Critical Knowledge Course](), or a configured version of it (Threats & Attacks, Network Security, Security Engineering, and Offensive & Defensive Schema Units)
2. CyberVista’s [Cloud Security Essentials]() course
3. [Security+]() Certification





CYBER DEFENSE ANALYST (PR-CDA-001)

NICE describes the role of a Cyber Defense Analyst as: “Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.”

Of the [redacted] participants, 17% (n=8) represented the Cyber Defense Analyst job role, which nests underneath the ‘Protect & Defend’ category and the ‘Cyber Defense Analysis’ specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the ‘**Cyber Defense Analysis**’ specialty area, as well as other periphery specialty areas such as ‘Incident Response,’ ‘Targets,’ ‘Threat Analysis,’ and ‘Network Services’ given some overlap in knowledge and skill areas shared between roles within those specialty areas.

<u>Observations & Recommendations</u>

Collectively, the Cyber Defense Analysts scored well overall, however the scoring illustrates proficiency in the periphery specialty areas while highlighting potential improvement in the primary area of ‘Cyber Defense Analysis.’ Consider:

1. CyberVista’s SOC Analyst Course
2. Evaluate needs of employees at the individual level as some may benefit from additional training opportunities such as CyberVista’s Incident Response Course or even CyberVista’s Critical Knowledge Course, or a configured version thereof (Threats & Attacks, Security Operations, and Offensive & Defensive Schema Units)

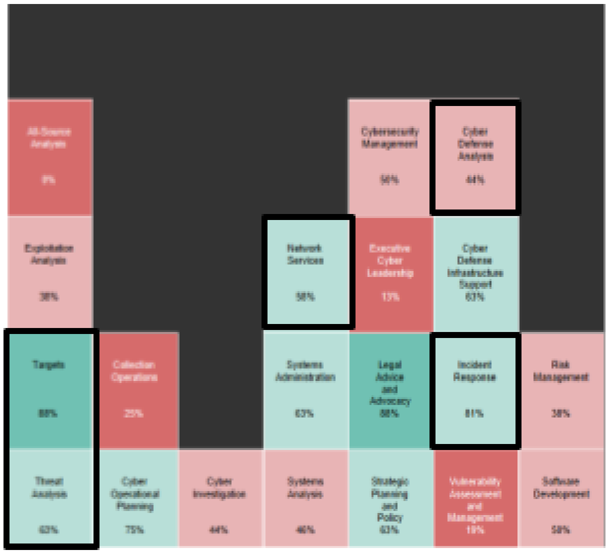
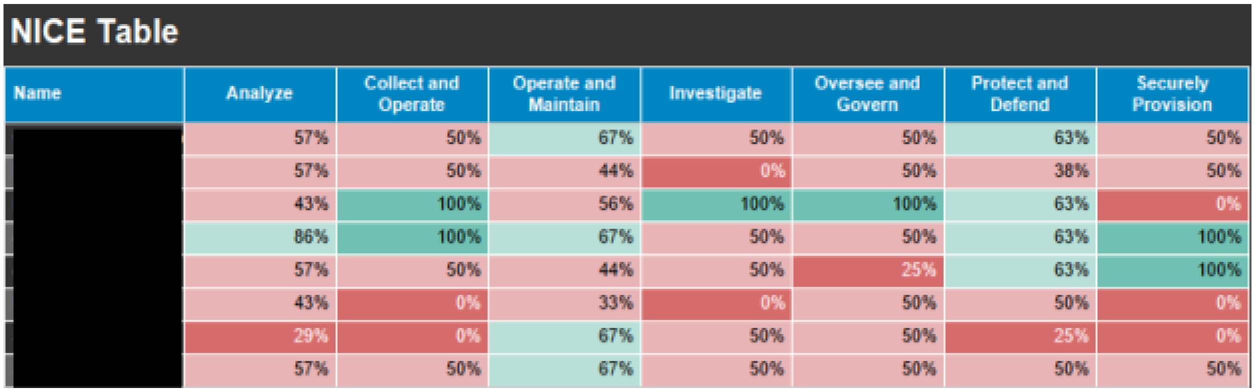


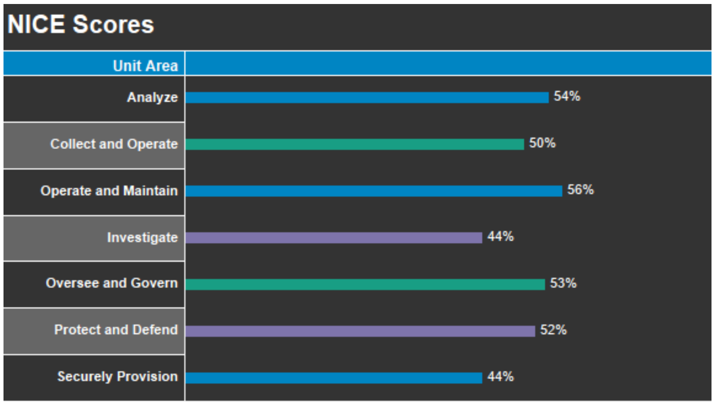
Figure 5 – Heat table scores at specialty area level for participants holding the job role "Cyber Defense Analyst"

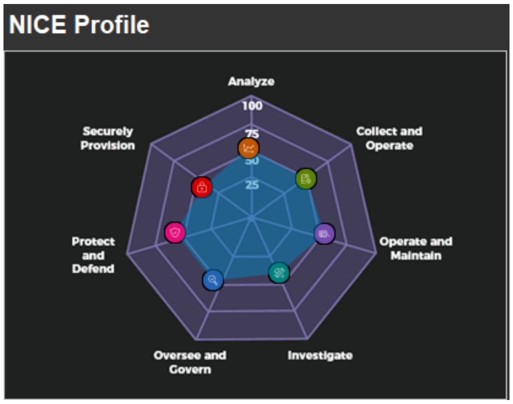


NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	57%	50%	67%	50%	50%	63%	50%
[redacted]	57%	50%	44%	0%	50%	38%	50%
[redacted]	43%	100%	56%	100%	100%	63%	0%
[redacted]	86%	100%	67%	50%	50%	63%	100%
[redacted]	57%	50%	44%	50%	25%	63%	100%
[redacted]	43%	0%	33%	0%	50%	50%	0%
[redacted]	29%	0%	67%	50%	50%	25%	0%
[redacted]	57%	50%	67%	50%	50%	50%	50%

Table 2 - Summary of scores at category-level by participants holding the job role “Cyber Defense Analyst”


NICE Scores
Unit Area
Analyze
54%
Collect and Operate
50%
Operate and Maintain
56%
Investigate
44%
Oversee and Govern
53%
Protect and Defend
52%
Securely Provision
44%


NICE Profile
Analyze
100
75
50
25
Collect and Operate
Operate and Maintain
Investigate
Oversee and Govern
Protect and Defend
Securely Provision

CYBER POLICY AND STRATEGY PLANNER (OV-SPP-002)

NICE describes the role of a Cyber Policy and Strategy Planner as: "Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance."

Of the [redacted] participants, 17% (n=8) represented the Cyber Policy and Strategy Planner job role, which nests underneath the 'Oversee & Govern' category and the 'Strategic Planning and Policy' specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the '**Strategic Planning and Policy**' specialty area, as well as other periphery specialty areas such as 'Cyber Operational Planning,' 'Cybersecurity Management,' and 'Legal Advice and Advocacy' given some overlap in knowledge and skill areas shared between roles within those specialty areas.

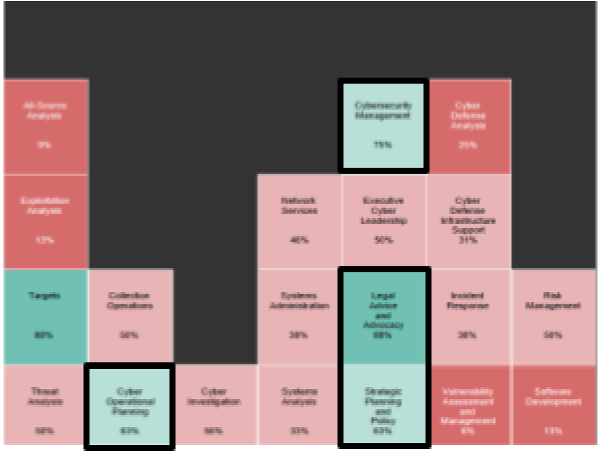
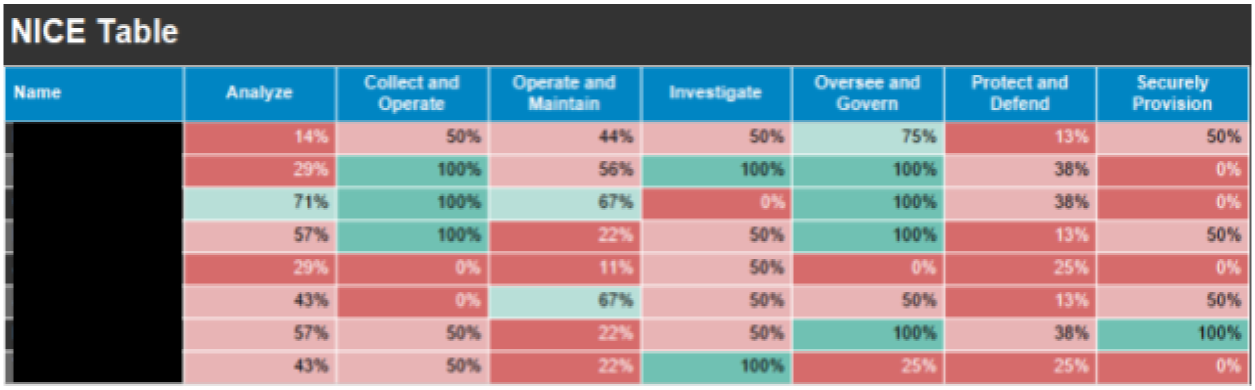


Figure 7 – Heat table scores at specialty area level for participants holding the job role "Cyber Policy & Strategic Planning"

<u>Observations & Recommendations</u>

Collectively, the Cyber Policy and Strategy Planners scored well overall, however at the individual level, some employees may benefit from some training opportunities. Due to score various by individual performance, [redacted] should evaluate the needs of individuals with this job role on a case-by-case basis. Some training programs to consider:

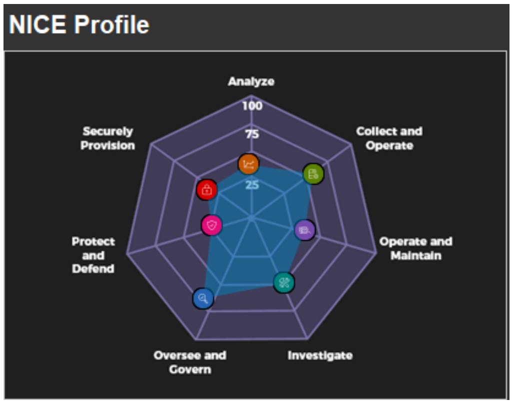
1. CyberVista's Executive [Cyber Risk Program]
2. CyberVista comprehensive [CISM certification training course]



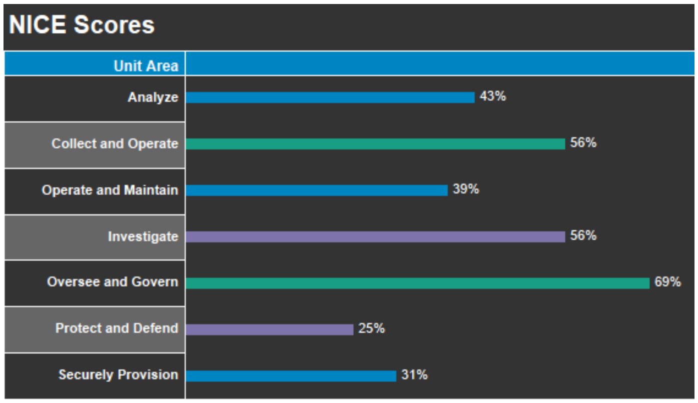
NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	14%	50%	44%	50%	75%	13%	50%
[redacted]	29%	100%	56%	100%	100%	38%	0%
[redacted]	71%	100%	67%	0%	100%	38%	0%
[redacted]	57%	100%	22%	50%	100%	13%	50%
[redacted]	29%	0%	11%	50%	0%	25%	0%
[redacted]	43%	0%	67%	50%	50%	13%	50%
[redacted]	57%	50%	22%	50%	100%	38%	100%
[redacted]	43%	50%	22%	100%	25%	25%	0%

Table 3 - Summary of scores at category-level by participants holding the job role "Cyber Policy & Strategic Planning"



NICE Profile



NICE Scores

PRODUCT SUPPORT MANAGER (OV-PMA-003)

NICE describes the role of a Cyber Policy and Strategy Planner as: “Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.”

Of the [redacted] participants, 9% (n=4) represented the Product Support Manager job role, which nests underneath the ‘Oversee & Govern’ category and the ‘Program/Project Management (PMA) and Acquisition’ specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the ‘**PMA and Acquisition**’ specialty area (not directly accounted for in CyberVista’s NICE Workforce Diagnostic), as well as other periphery specialty areas such as ‘Cybersecurity Management,’ and ‘Strategic Planning and Policy’ given some overlap in knowledge and skill areas shared between roles within those specialty areas.

<u>Observations & Recommendations:</u>

The Product Support Managers scored very well in the specialty areas that the diagnostic could assess for this job role. Given that the diagnostic does not directly account for the ‘PMA and Acquisition’ specialty area, and that the periphery specialty areas illustrate proficiency, CyberVista has no training recommendations for the individuals in this role at this time.

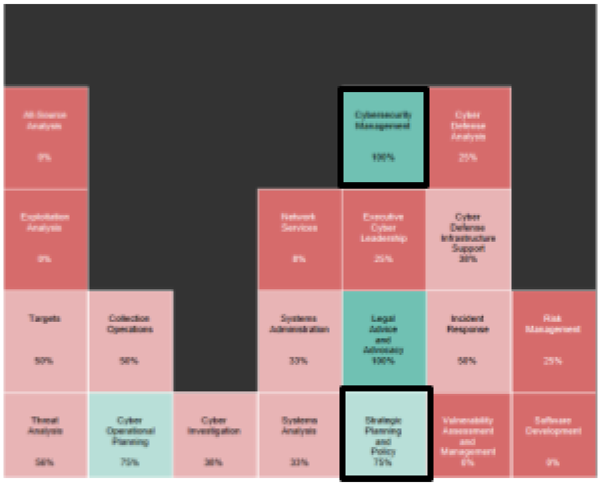
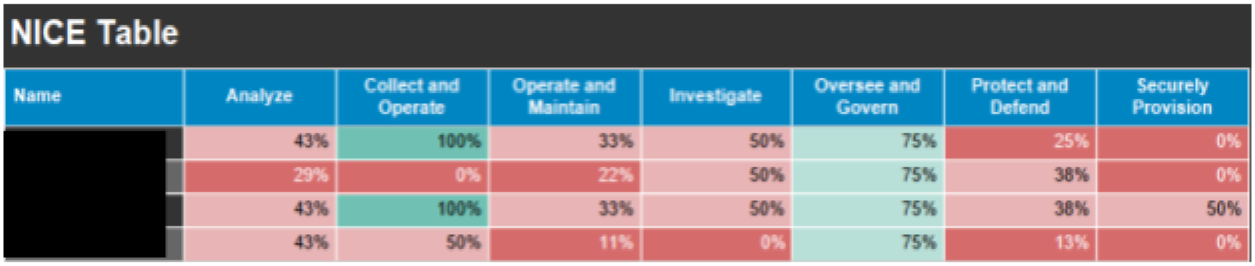


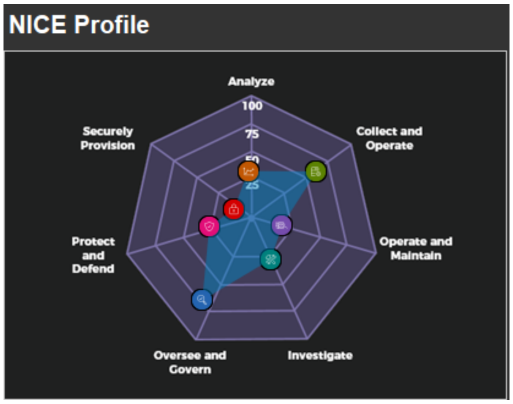
Figure 9 – Heat table scores at specialty area level for participants holding the job role “Product Support Manager”



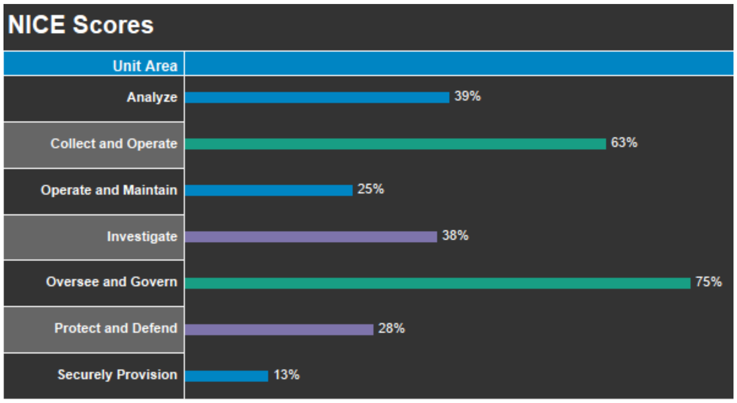
NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	43%	100%	33%	50%	75%	25%	0%
[redacted]	29%	0%	22%	50%	75%	38%	0%
[redacted]	43%	100%	33%	50%	75%	38%	50%
[redacted]	43%	50%	11%	0%	75%	13%	0%

Table 4 - Summary of scores at category-level by participants holding the job role “Product Support Manager”



NICE Profile



NICE Scores

Unit Area	
Analyze	39%
Collect and Operate	63%
Operate and Maintain	25%
Investigate	38%
Oversee and Govern	75%
Protect and Defend	28%
Securely Provision	13%

EXPLOITATION ANALYST (AN-EXP-001)

NICE describes the role of an Exploitation Analyst as: “Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.”

Of the [redacted] participants, 7% (n=3) represented the Exploitation Analyst job role, which nests underneath the ‘Analyze” category and the ‘Exploitation Analysis’ specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the ‘**Exploitation Analysis**’ specialty area, as well as other periphery specialty areas such as ‘Targets,’ ‘All-Source Analysis,’ and ‘Cyber Operations’ given some overlap in knowledge and skill areas shared between roles within those specialty areas.

Observations & Recommendations

Collectively, the Exploitation Analysts would benefit from training opportunities to increase areas of proficiency as indicated from the diagnostic scoring. There are several options [redacted] could consider for individuals in this role:

1. CyberVista’s comprehensive CEH Certification course
2. CyberVista’s Critical Knowledge Course, or a configured version thereof (Threats & Attacks, Security Operations, and Offensive & Defensive Schema Units)
3. CyberVista’s SOC Analyst Course
4. GIAC Open Source Intelligence (GOSI)

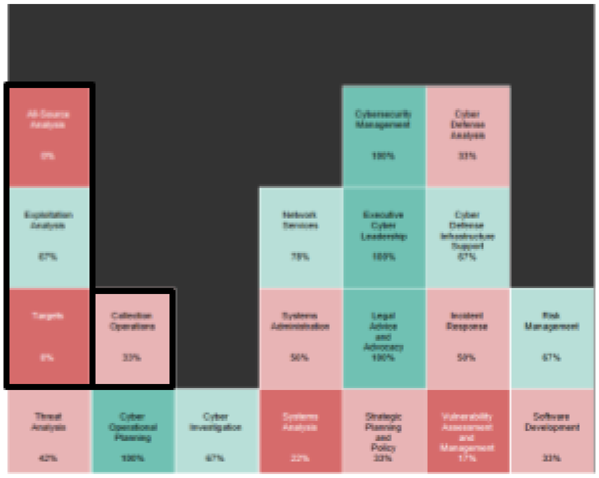
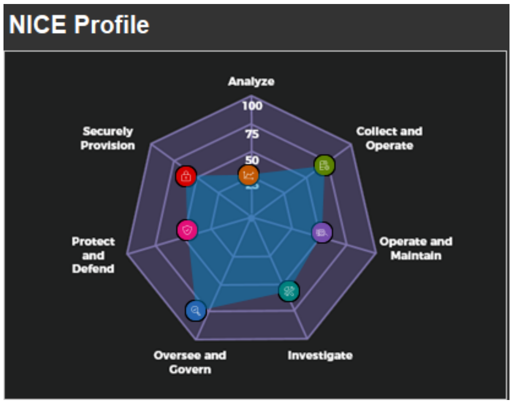
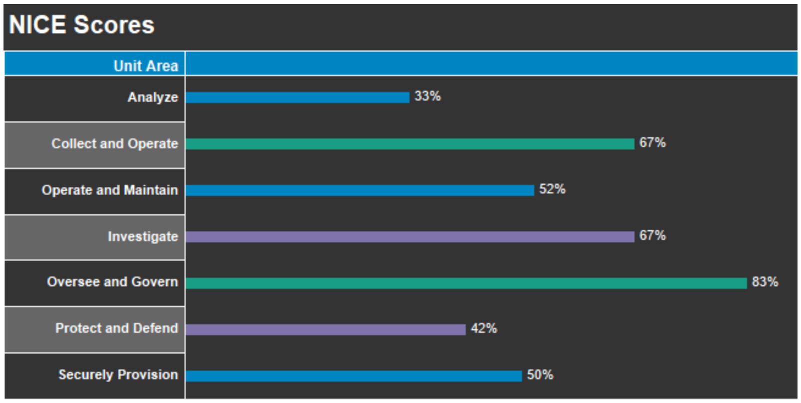
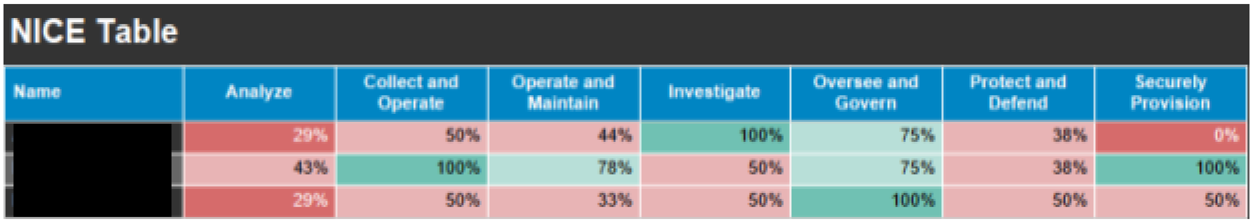


Figure 11 – Heat table scores at specialty area level for participants holding the job role “Exploitation Analyst”







NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	29%	50%	44%	100%	75%	38%	0%
[redacted]	43%	100%	78%	50%	75%	38%	100%
[redacted]	29%	50%	33%	50%	100%	50%	50%

Table 5 - Summary of scores at category-level by participants holding the job role "Exploitation Analyst"

KNOWLEDGE MANAGER (OM-KMG-001)

NICE describes the role of a Knowledge Manager as: "Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content."

Of the [redacted] participants, 7% (n=3) represented the Knowledge Manager job role, which nests underneath the 'Operate and Maintain" category and the 'Knowledge Management' specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the '**Knowledge Management**' specialty area (not directly accounted for in CyberVista's NICE Workforce Diagnostic), as well as other periphery specialty areas such as 'Systems Requirements Planning' (not directly accounted for in CyberVista's NICE Workforce Diagnostic), 'Risk Management,' and 'Legal Advice and Advocacy' given some overlap in knowledge and skill areas shared between roles within those specialty areas.

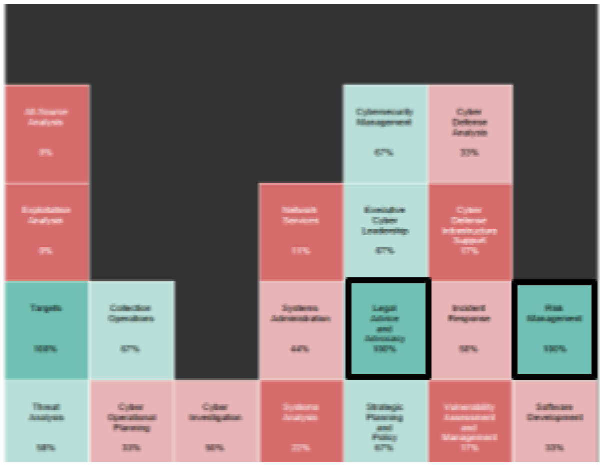
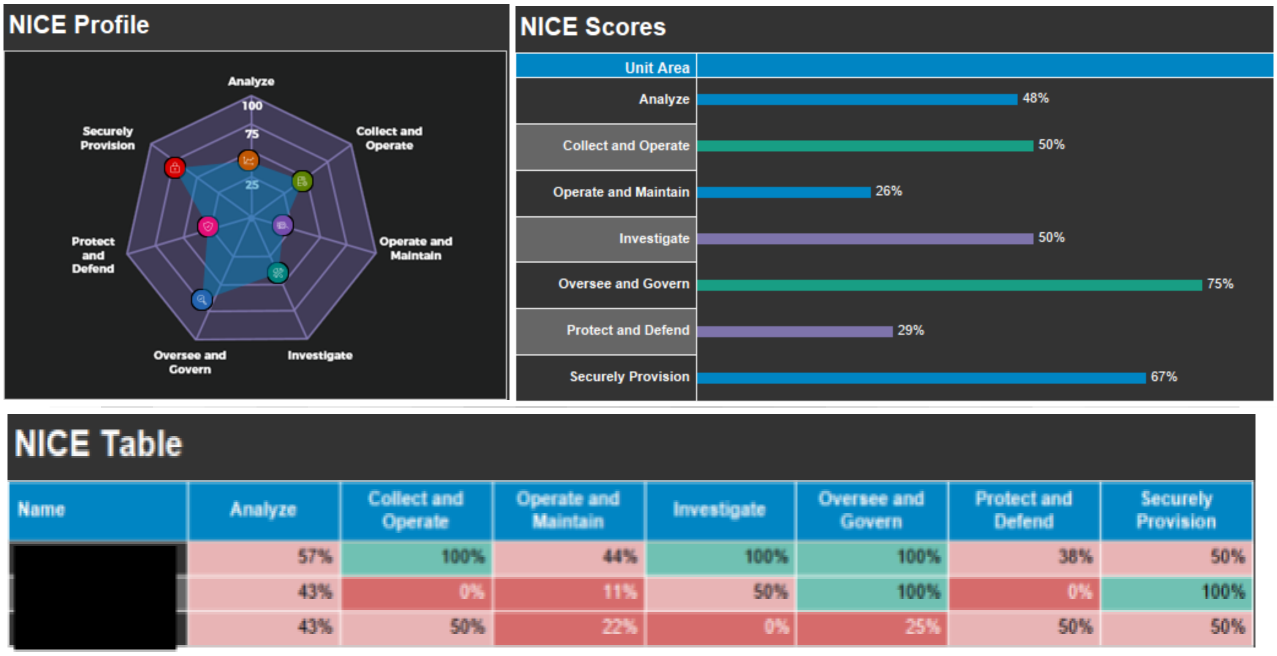


Figure 13 – Heat table scores at specialty area level for participants holding the job role "Knowledge Manager"

Observations & Recommendations:

The Knowledge Managers scored very well in the specialty areas that the diagnostic could assess for this job role. Given that the diagnostic does not directly account for the 'Knowledge Management' specialty area, and that the periphery specialty areas illustrate proficiency, CyberVista has no training recommendations for the individuals in this role at this time.



NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	57%	100%	44%	100%	100%	38%	50%
[redacted]	43%	0%	11%	50%	100%	0%	100%
[redacted]	43%	50%	22%	0%	25%	50%	50%

Table 6 - Summary of scores at category-level by participants holding the job role "Knowledge Manager"

SECURITY CONTROL ASSESSOR (SP-RSK-002)

NICE describes the role of a Security Control Assessor as: "Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37)."

Of the [redacted] participants, 7% (n=3) represented the Security Control Assessor job role, which nests underneath the 'Securely Provision' category and the 'Risk Management' specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the '**Risk Management**' specialty area, as well as other periphery specialty areas such as 'Systems Analysis,' 'Cybersecurity Management,' 'Incident Response,' and 'Systems Analysis' given some overlap in knowledge and skill areas shared between roles within those specialty areas.

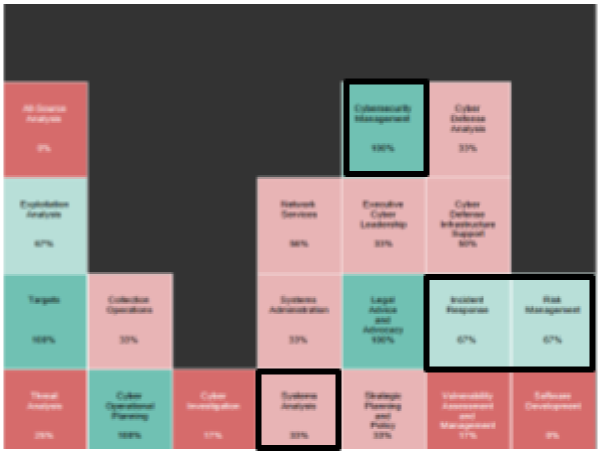
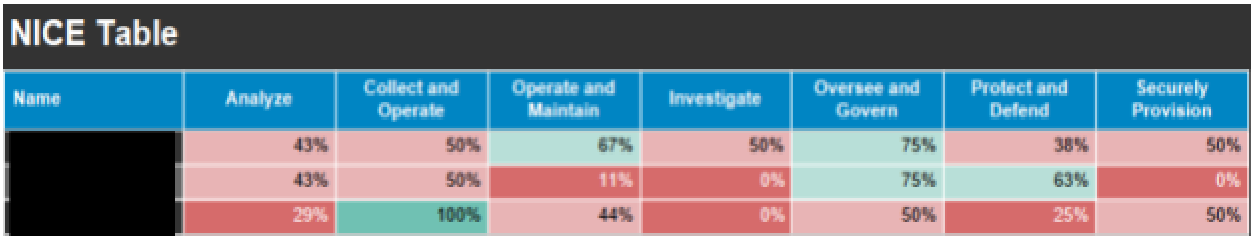


Figure 15 – Heat table scores at specialty area level for participants holding the job role "Security Control Assessor"

Observations & Recommendations:

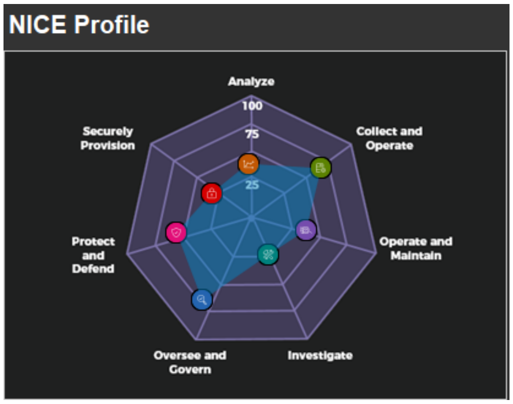
Collectively, the Security Control Assessors scored well overall, however at the individual level, some employees may benefit from some training opportunities. Due to score various by individual performance, [redacted] should evaluate the needs of individuals with this job role on a case-by-case basis.



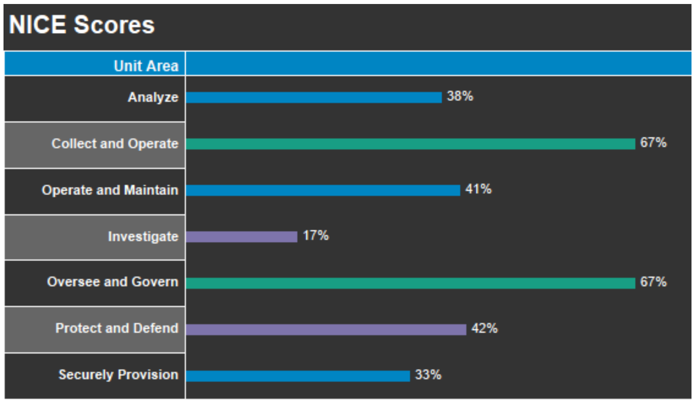
NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	43%	50%	67%	50%	75%	38%	50%
[redacted]	43%	50%	11%	0%	75%	63%	0%
[redacted]	29%	100%	44%	0%	50%	25%	50%

Table 7 - Summary of scores at category-level by participants holding the job role "Security Control Assessor"



NICE Profile



NICE Scores

ALL-SOURCE ANALYST (AN-ASA-001)

NICE describes the role of an All-Source Analyst as: "Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations."

Of the [redacted] participants, 4% (n=2) represented the All-Source Analyst job role, which nests underneath the 'Analysis' category and the 'All-Source Analysis' specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the '**All-Source Analysis**' specialty area, as well as other periphery specialty areas such as 'Threat Analysis' given some overlap in knowledge and skill areas shared between roles within those specialty areas.

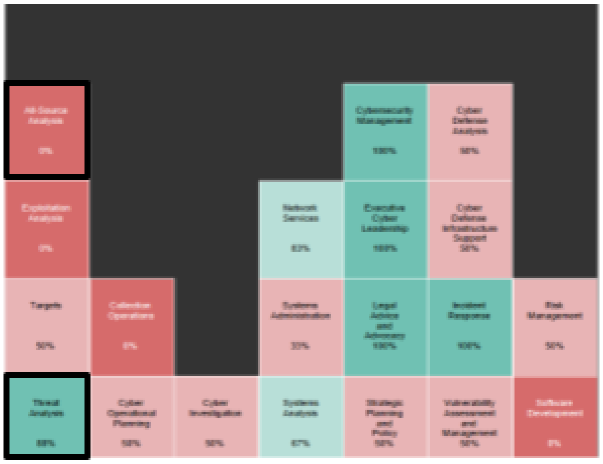
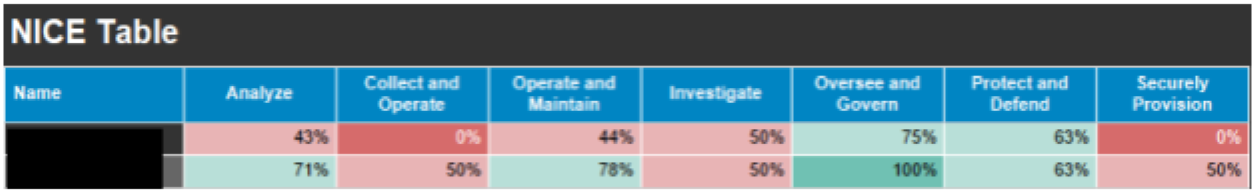


Figure 15 – Heat table scores at specialty area level for participants holding the job role "All-Source Analyst"

Observations & Recommendations

The All-Source Analysts scored well in Threat Analysis but demonstrated potential improvement areas in the All Source Analysis specialty area. Given the performance scoring, these analysts may consider:

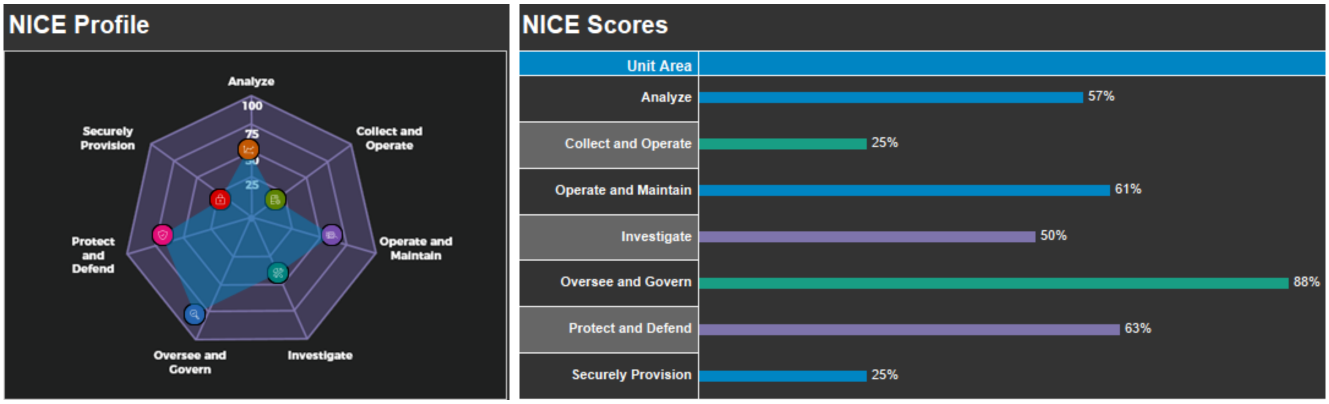
1. GIAC Cyber Threat Intelligence (GCTI), or EC-Council's Certified Threat Intelligence Analyst (C|TIA) certifications
2. GIAC Open Source Intelligence (GOSI)
3. Other all source intelligence focused courses or training programs



NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	43%	0%	44%	50%	75%	63%	0%
[redacted]	71%	50%	78%	50%	100%	63%	50%

Table 8 - Summary of scores at category-level by participants holding the job role "All-Source Analyst"



SECURITY AWARENESS AND COMMUNICATIONS OFFICER (OV-TEA-003)

Note: Currently, there is no official NIST-NICE Work Role of Security Awareness and Communications Officer. The most aligned role to this job title according to NICE would be '**Cyber Workforce Developer and Planner' (OV-SPP-001)**. NICE describes the role of a Cyber Workforce Developer and Planner as: "Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements."

Of the [redacted] participants, 4% (n=2) represented the Cyber Workforce Developer and Planner job role, which nests underneath the 'Oversee and Govern' category and the 'Strategic Planning and Policy' specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the '**Strategic Planning and Policy**' specialty area, as well as other periphery specialty areas such as 'Training, Education, and Awareness,' (not directly accounted for in

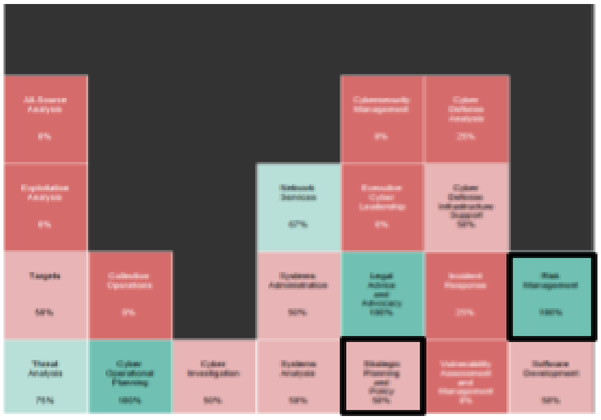
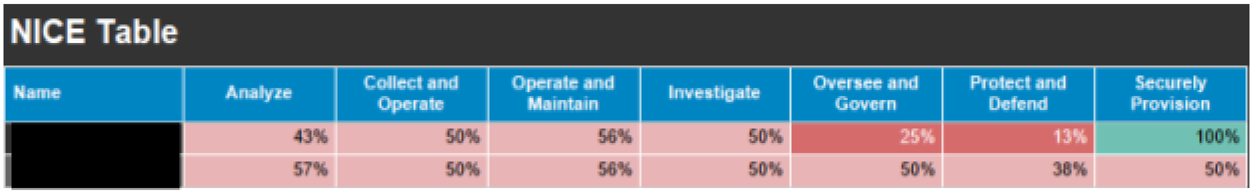


Figure 17 – Heat table scores at specialty area level for participants holding the job role "Cyber Workforce Developer and Planner"

CyberVista's NICE Workforce Diagnostic) and 'Risk Management' given some overlap in knowledge and skill areas shared between roles within those specialty areas.

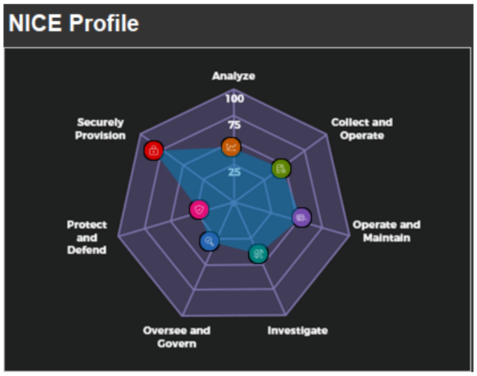
Observations & Recommendations:
The Cyber Workforce Developer and Planners scored well in the areas that applied to this job role. Given the small sample size of employees in this grouping and the distinct responsibilities of this role, [redacted] should evaluate training needs on an individual basis. It's also noteworthy that conferences often serve as great training/learning opportunities for individuals in this role, so training options should consider attending industry conferences that focus on content related to cyber workforce development and cybersecurity awareness training (such as the annual NICE Conference, RSAC, and variety of conferences on security awareness training).

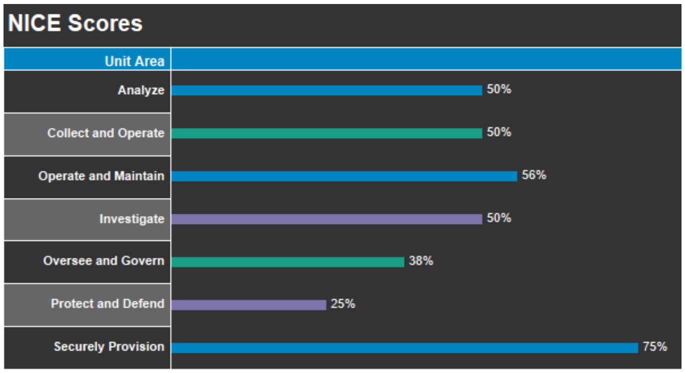


NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	43%	50%	56%	50%	25%	13%	100%
[redacted]	57%	50%	56%	50%	50%	38%	50%

Table 9 - Summary of scores at category-level by participants holding the job role "Cyber Workforce Developer and Planner"





EXECUTIVE CYBER LEADERSHIP (OV-EXL-001)

NICE describes the role of Executive Cyber Leadership as: “Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.” Of the [redacted] participants, 2% (n=1) represented the Executive Cyber Leadership job role, which nests underneath the ‘Oversee and Govern’ category and the ‘Executive Cyber Leadership’ specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the ‘**Executive Cyber Leadership**’ specialty area, as well as other periphery specialty areas such as ‘Strategic Planning and Policy,’ ‘Legal Advice and Advocacy,’ ‘Cybersecurity Management,’ and ‘Risk Management’ given some overlap in knowledge and skill areas shared between roles within those specialty areas.

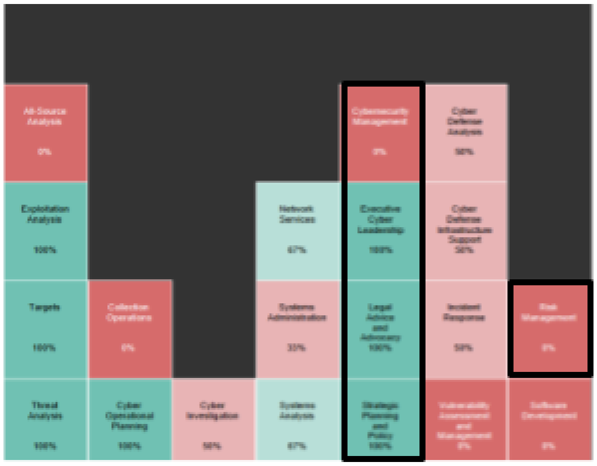
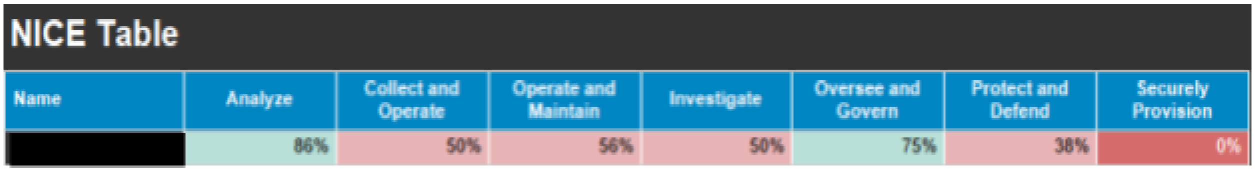


Figure 19 – Heat table scores at specialty area level for participants holding the job role “Executive Cyber Leadership”

Observations & Recommendations:

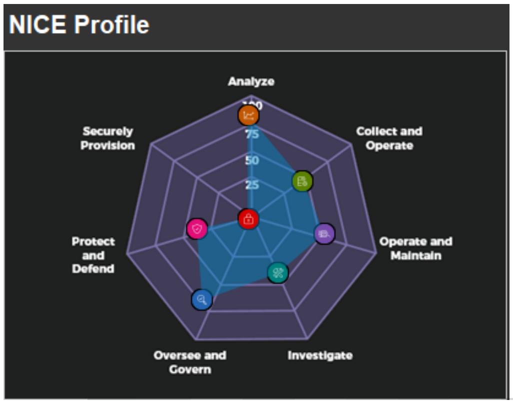
The Executive Cyber Leader scored respectably in the areas that applied to this job role. Given the small sample size of employees in this grouping and the distinct responsibilities of this role, [redacted] should evaluate training needs on an individual basis. CyberVista’s Cyber Risk Program, or adding a cybersecurity credential, such as CISM or CISSP may also be worth considering.

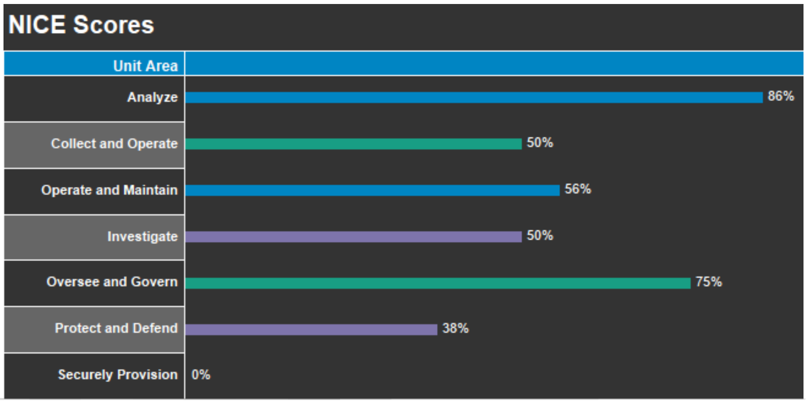


NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	86%	50%	56%	50%	75%	38%	0%

Table 10 - Summary of scores at category-level by participants holding the job role “Executive Cyber Leadership”





PROGRAM MANAGER (OV-PMA-001)

NICE describes the role of a Program Manager as: “Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.” Of the [redacted] participants, 2% (n=1) represented the Program Manager job role, which nests underneath the ‘Oversee and Govern’ category and the ‘Executive Cyber Leadership’ specialty area. Given the expected knowledge and skills for this job role, proficiency expectations are expected under the ‘**PMA and Acquisition**’ specialty area (not directly accounted for in CyberVista’s NICE Workforce Diagnostic), as well as other periphery specialty areas such as ‘Cybersecurity Management,’ ‘Strategic Planning and Policy,’ and ‘Risk Management’ given some overlap in knowledge and skill areas shared between roles within those specialty areas.

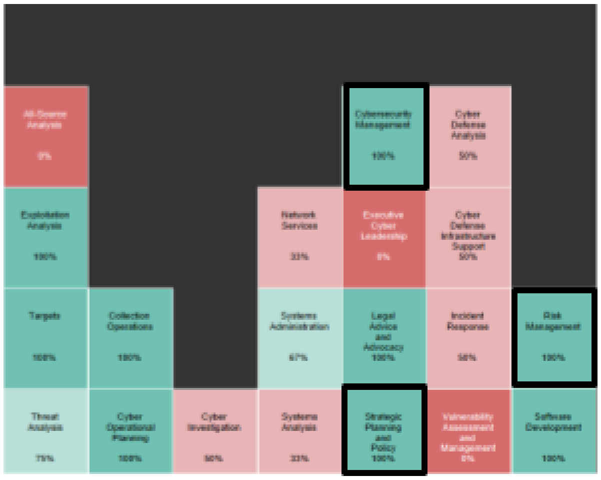
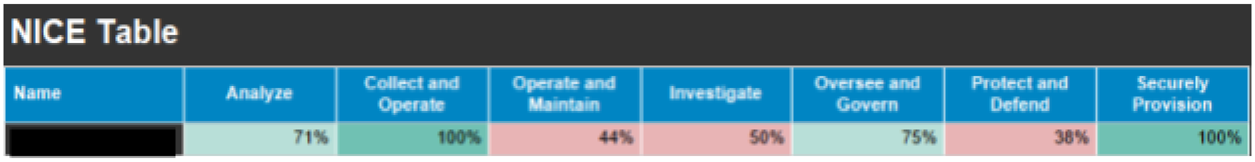


Figure 21 – Heat table scores at specialty area level for participants holding the job role “Program Manager”

<u>Observations & Recommendations</u>

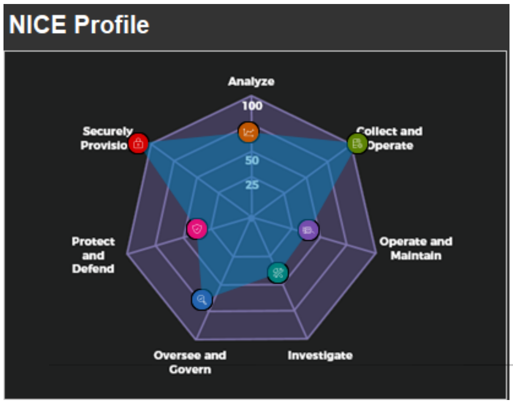
The Program Manager scored very well in the specialty areas that the diagnostic could assess for this job role. Given that the diagnostic does not directly account for the ‘PMA and Acquisition’ specialty area, and that the periphery specialty areas illustrate proficiency, CyberVista has no training recommendations for the individual in this role at this time.

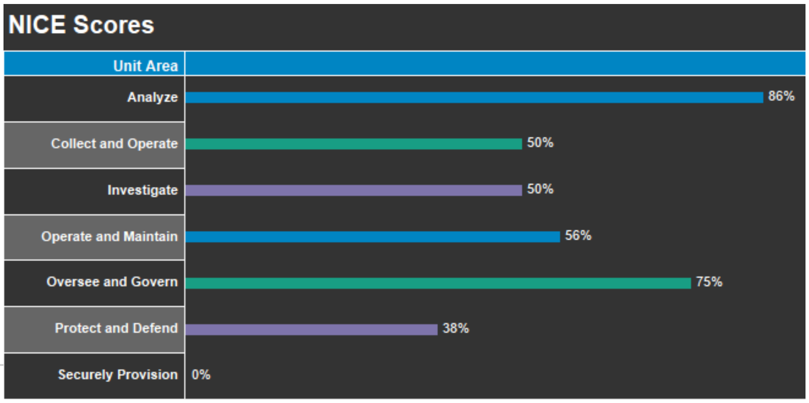


NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	71%	100%	44%	50%	75%	38%	100%

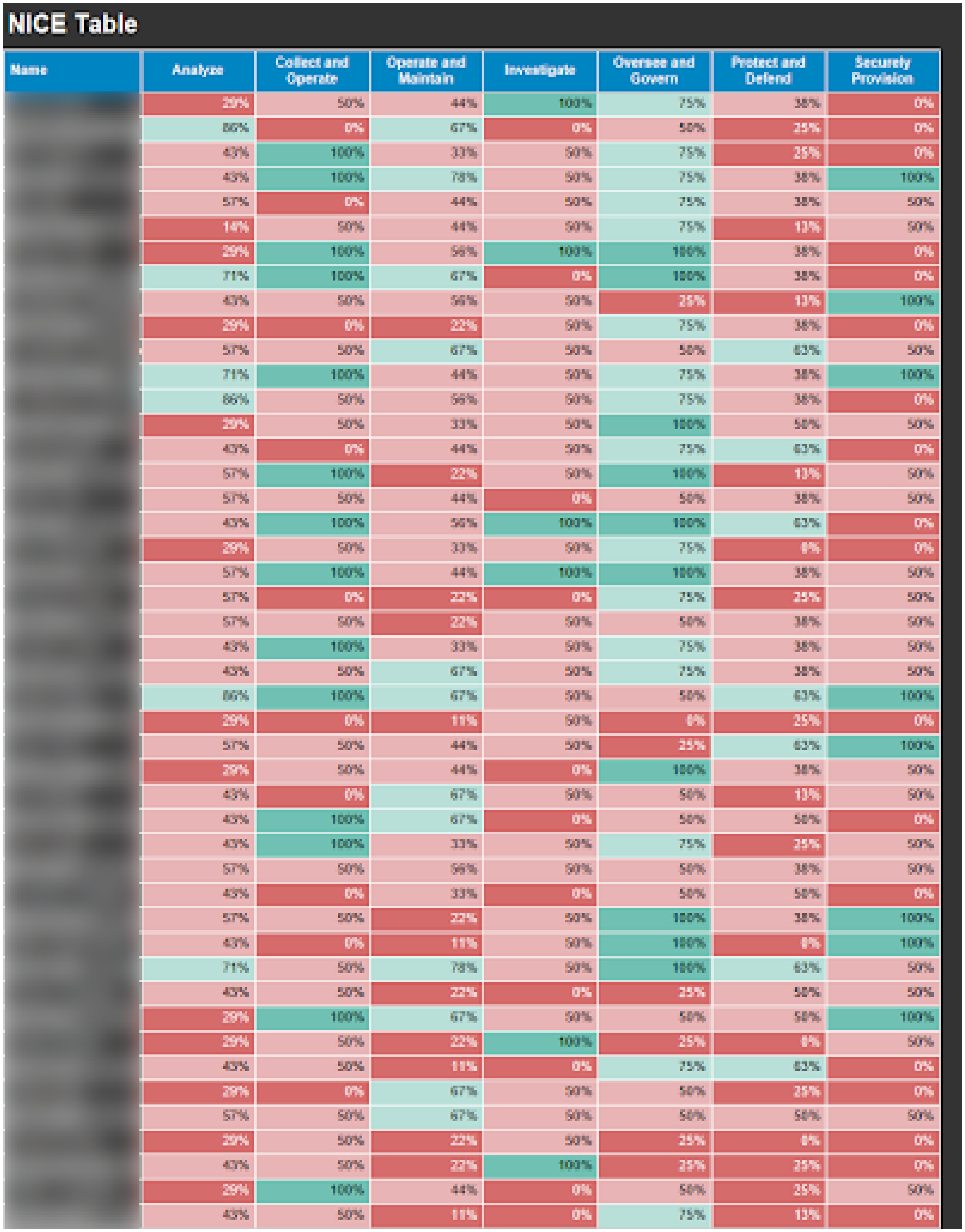
Table 11 - Summary of scores at category-level by participants holding the job role “Program Manager”





Appendix A:

Individual Diagnostic Results



NICE Table

Name	Analyze	Collect and Operate	Operate and Maintain	Investigate	Oversee and Govern	Protect and Defend	Securely Provision
[redacted]	29%	50%	44%	100%	75%	38%	0%
[redacted]	86%	0%	67%	0%	50%	25%	0%
[redacted]	43%	100%	33%	50%	75%	25%	0%
[redacted]	43%	100%	78%	50%	75%	38%	100%
[redacted]	57%	0%	44%	50%	75%	38%	50%
[redacted]	14%	50%	44%	50%	75%	13%	50%
[redacted]	29%	100%	56%	100%	100%	38%	0%
[redacted]	71%	100%	67%	0%	100%	38%	0%
[redacted]	43%	50%	56%	50%	25%	13%	100%
[redacted]	29%	0%	22%	50%	75%	38%	0%
[redacted]	57%	50%	67%	50%	50%	63%	50%
[redacted]	71%	100%	44%	50%	75%	38%	100%
[redacted]	86%	50%	56%	50%	75%	38%	0%
[redacted]	29%	50%	33%	50%	100%	50%	50%
[redacted]	43%	0%	44%	50%	75%	63%	0%
[redacted]	57%	100%	22%	50%	100%	13%	50%
[redacted]	57%	50%	44%	0%	50%	38%	50%
[redacted]	43%	100%	56%	100%	100%	63%	0%
[redacted]	29%	50%	33%	50%	75%	0%	0%
[redacted]	57%	100%	44%	100%	100%	38%	50%
[redacted]	57%	0%	22%	0%	75%	25%	50%
[redacted]	57%	50%	22%	50%	50%	38%	50%
[redacted]	43%	100%	33%	50%	75%	38%	50%
[redacted]	43%	50%	67%	50%	75%	38%	50%
[redacted]	86%	100%	67%	50%	50%	63%	100%
[redacted]	29%	0%	11%	50%	0%	25%	0%
[redacted]	57%	50%	44%	50%	25%	63%	100%
[redacted]	29%	50%	44%	0%	100%	38%	50%
[redacted]	43%	0%	67%	50%	50%	13%	50%
[redacted]	43%	100%	67%	0%	50%	50%	0%
[redacted]	43%	100%	33%	50%	75%	25%	50%
[redacted]	57%	50%	56%	50%	50%	38%	50%
[redacted]	43%	0%	33%	0%	50%	50%	0%
[redacted]	57%	50%	22%	50%	100%	38%	100%
[redacted]	43%	0%	11%	50%	100%	0%	100%
[redacted]	71%	50%	78%	50%	100%	63%	50%
[redacted]	43%	50%	22%	0%	25%	50%	50%
[redacted]	29%	100%	67%	50%	50%	50%	100%
[redacted]	29%	50%	22%	100%	25%	0%	50%
[redacted]	43%	50%	11%	0%	75%	63%	0%
[redacted]	29%	0%	67%	50%	50%	25%	0%
[redacted]	57%	50%	67%	50%	50%	50%	50%
[redacted]	29%	50%	22%	50%	25%	0%	0%
[redacted]	43%	50%	22%	100%	25%	25%	0%
[redacted]	29%	100%	44%	0%	50%	25%	50%
[redacted]	43%	50%	11%	0%	75%	13%	0%