On-the-Job Training Blueprint		
Month	**New Analyst - Cybersecurity DFIR**	
S/N	**Technical Skills and Competencies**	**Training Duration (Month)***
1	**Onboarding/Access Requests**	1st Month
2	**SIEM/Tools Training**	1st Month
3	**Email Analysis**	2nd Month (Last week July 2023)
4	**Incident Handling**	2nd - 6th Month
5	**DLP**	2nd month
6	**Host-based Analysis**	2nd Month
7	**Network-based Analysis**	3rd Month
8	**Endpoint Detection and Response (EDR) / Antivirus**	3rd - 4th Month
9	**Threat Intelligence and Detection**	4th - 6th Month (out of scope for practicum project)
10	**Tabletop Exercise and Assessment**	3rd Month; 6th Month (After Practicum)
	Total Duration	6 Months

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
1	**Onboarding/Access Request**	• Organizational Structure • Roles and Responsibility • Incident Response Life Cycle • Incident Response Plan • Incident Escalation Procedure • Key Stakeholder group	• Familiar with incident management and response procedure for detection, reporting and handling of incidents • Familiar with remediation and resolution of cyber incidents at organizational level • How to communicate incidents to different critical stakeholders • Cross-region communicate and collaboration	• Incident and Case Handling • Incident Response Procedure/playbook • Email Notification/Response Template • Cross-region handover • Different accounts	1st Month	• Able to identify various SME • Complete CISP and CIRP • Familiarity with CMDB tool
2	**SIEM/Tools Training**	• [SIEM Tools] • CMDB service • Email Security Appliance • Email Archive • Domain Name Server resolution service	• Able to access and use org tools	• Cyber Dashboard with tools • Tool Documentation(s)	1st Month	• Able to access org tools
3	**Email Analysis**	• Lifecycle of an email (SMTP) • Analyze message headers and gauge email authenticity using SPF and DKIM • Extract and review document metadata present • Merge event logs and perform advanced filtering to easily get through large events • Malicious attachment analysis • Phishing Response Tool	• Perform log analysis • Case writeup and handling • Phishing email analysis • Identify if any email clickers • Analyze email header and authenticity • Malicious attachment analysis • Malicious url analysis • Blocking of C2/phishing Domains • Email removal/quarantine • Ticket queue	• Phish email analysis tool • Case management • Malware file or link analysis • Email releases • ticket	2nd Month	• Able to manage Email Triage Queue • Able to triage Phish Report Incidents without assistance • Able to triage tickets
4	**Incident Handling**	• Phish Report Triage • Ticket handling • Incident handling	• Handles phish reports • Basic ticketing and cyber-Incident investigation	• varies	2nd month – 6th month	• Able to triage cases/ cyber incidents without assistance
5	**DLP**	• Classification of Data • Escalation • Review Daily DLP	• Able to work on DLP daily triage	• DLP tool(s)	2nd month	• Able to work on DLP Daily triage Incidents

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
6	**Network-based Analysis**	• Network protocol analysis • Hypertext Transfer Protocol (HTTP) • Domain Name Service (DNS) • File Transfer Protocol (FTP) • Server Message Block (SMB) and related Microsoft protocols • Simple Mail Transfer Protocol (SMTP) • Log collection, aggregation, and analysis • Pcap/wireshark analysis - etraining	• Analyze network traffic • Architecture and core functionality • Tunneling • Fast flux and domain name generation algorithms (DGAs) • Logging methods • Amplification attacks • Filtering network activity to identify indicators of compromise • Assessing encrypted network traffic with multiple data sources • Identifying compromised host beaconing with proxy server logs	• Packet Capture Analysis • Wireshark • Network investigations cases • SIEM tools - log analysis ○ Syslog ○ Windows Event ○ HTTP server logs ○ Firewalls, Intrusion Detection Systems (IDS), ○ Network Security Monitoring (NSM) Platforms ○ Log collection, aggregation, and analysis ○ Web proxy server examination	3rd month	• Able to triage network-based cases/ cyber incidents without assistance • Able to review packet capture using wireshark *
7	**Host-based Analysis**	• Incident Response and Intrusion Forensics Methodology • Advanced Incident Response and Threat Hunting Tactics and Procedure • Cyber-kill chain strategies • ATT&CK - MITRE • Web Browser Forensics • Windows Artifact Analysis • Registry Analysis, Application Executions • Memory Forensics • Timeline Analysis • Advanced Adversary & Anti-forensics Detection • Living of the land techniques • scenario	• Track a suspect's activity in browser history and cache files and identify local file access • Examine which files a suspect downloaded • Determine URLs that suspects typed, clicked on, bookmarked, or were merely re-directed to while web browsing • Investigate browser auto-complete • Identify artifact and evidence locations to answer crucial questions, including ○ application execution, ○ file access, ○ data theft, ○ external device usage, ○ device geolocation, ○ Browser history,	• Endpoint Detection and Response (EDR) console and agents • ATT&CK - MITRE's Adversarial Tactics, Techniques, and Common Knowledge	2nd & 3rd Month	• Able to triage host-based cases/tickets without assistance

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
			○ file download, ○ anti-forensics, ○ detailed system, ○ and user activity ○			
8	**Endpoint Detection and Response (EDR) / Antivirus**	• Hands-on exercise modeled after real-world attack • Parent Child Processes • Common process	• Respond, detect, scope, and stop intrusions and data breaches. • Identify compromised and affected systems • Perform damage/compromise assessments, such as: ○ Identity attack mechanism ○ Identify and track malware beaconing to C2 ○ Memory analysis ○ Registry analysis ○ Privilege escalation ○ Lateral movement analysis ○ Deep-dive timeline creation and analysis ○ Detect anti-forensics and hiding techniques ○ Data exfiltration • Contain and remediate incidents • Organize findings for use in ○ incident response, ○ internal investigations, ○ intellectual property theft inquiries, ○ and civil or criminal litigation.	• Endpoint Detection and Response (EDR) console and agents • ATT&CK - MITRE's Adversarial Tactics, Techniques, and Common Knowledge • Kill process • Quarantine host	• 3rd – 4th month	• Threat Hunt • Investigate Host • Able to perform forensic investigation on given host
9*	**Threat Intelligence and Detection**	• Cyber intelligence • Emerging threats, perpetrators, doctrines, and methods of operations	• Gather intelligence with OSINT platforms and tools • Manage the research, analysis, and data integration across wide variety of information sources/ intel feeds	• Cyber intelligence feeds • Regulator/Gov • 3rd Party Intel Vendor • Incident response and threat hunting	• 4th - 6th month	• Threat assessment and case write up

S/N	Technical Skills and Competencies	Knowledge	Abilities	Range of Application	Training Duration (Months)	Performance Evidence
			• Determine tactics, techniques and procedures used for intrusions and attacks • Articulate significance of evolving cyber security threats to global cyber team, critical decision makers and senior management in organization • Present impact assessment			

10	**Tabletop Exercises**	• Full Incident Response Life Cycle Walkthrough	• Be able to Respond to a simulated breach and follow the incident response life cycle all the way through:
			  ○ Mainly **Identification**
			  ○ **Containment**
			  ○ **Eradication**
			  ○ **Recovery**
			  ○ And **Lessons Learned**
				• Varies	• 3rd month and again on 6th month	• No missed alerts
						• Indicators of Compromise identified
						• Root cause identified
						• Threat contained and eradicated where applicable

* out of scope of practicum project