(B) Details of Educational Qualification/ Certification/ Work Experience/ Specific Skills Required:

Post No / Post Name	1 – Deputy Manager- IT Security Expert
BASIC QUALIFICATION **(AS ON 31.01.2026)**	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER CERTIFICATIONS **(AS ON 31.01.2026)**	**Preferred Certifications:** (Valid as on 31.01.2026) OSCP, CEH, CHFI, GIFR, GIACC, GFSU.
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.01.2026)**	**Mandatory:** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain. **Preferred:** Experience in Cyber Defence operations (Threat Intel), Incident Response, Malware Analysis, Forensics, Threat Hunting **Training & Teaching experience will not be counted for eligibility**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of job, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of job and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Expertise in incident response, malware analysis, digital forensics, and cyber threat hunting. • Understanding of cloud, OT/ICS, and IoT security, red teaming, IR, Ethical hacking. • Strong technology leadership, people management, and stakeholder engagement skills. • Ability to handle high-pressure cyber crisis situations. • Excellent written and verbal communication, including ability to brief senior executives and policymakers.

Post No / Post Name	2 – Deputy Manager -Emerging Technology
BASIC QUALIFICATION **(AS ON 31.01.2026)**	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER CERTIFICATIONS **(AS ON 31.01.2026)**	**Preferred Certifications:** (Valid as on 31.01.2026) • Equivalent certifications in Innovation, Product Development, Web development etc in cyber security. • Java developer, mobile developer, Python developer, Web developer.
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.01.2026)**	**Mandatory:** Minimum Experience: 4 years of post-qualification experience in the Cybersecurity/Technology Innovation domain. **Preferred:** Hands-on work experience Preferably in cyber innovation labs. Product evaluation, prototyping, or applied cybersecurity solutioning is preferred.

	Exposure to handling R&D or applied Technology problem statements and experience in innovation environment is an added advantage. Cyber research, threat intelligence research etc. Understanding of cyber security principles, threat landscapes, and information security technologies. **<u>Training & Teaching experience will not be counted for eligibility</u>.** **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Ability to think creatively and develop original, effective solutions for complex security challenges. • Strong ability to analyze security incidents and assess the efficacy of new technologies and strategies. • A continuous learning mindset to stay abreast of cutting-edge technologies and evolving threats. • Strong understanding of emerging technologies: Artificial Intelligence (AI/ML), Blockchain, Quantum Computing, Cloud Security. • Proficiency in cyber threat modelling, simulation, and scenario-based evaluation. • Capability in prototyping, product validation, and applied research. • Ability to work with startups, academic institutions, and fintech innovators to co-develop solutions. • Excellent analytical, technical writing, and presentation skills. • Ability to translate innovation into deployable solutions aligned with the Bank's cybersecurity posture. • Exposure to banking, financial institutions (FIs), or PSU-led cybersecurity innovation projects. • Collaboration with academia, start-ups, and incubators in emerging technology/cybersecurity innovation. • Ability to contribute to national/international research initiatives or patents in technology/cybersecurity. • Ability to conduct deep-dive research on emerging cyber threats, tools, and trends • Experience with open-source intelligence (OSINT) tools and techniques • Data collection, synthesis, and interpretation from technical and non-technical sources. • Understanding of cybersecurity principles, technologies, and best practices, including network security, cloud security, endpoint security, and incident response. • Find security flaws in systems, applications, and networks before they can be exploited by malicious actors. • Create proof-of-concept exploits to demonstrate the real-world impact of vulnerabilities, helping to justify the need for security solutions • Ability to conduct research, analyse data, and identify innovative solutions or ideas to address complex cybersecurity challenges. • Ability to effectively communicate complex technical information to both technical and non-technical audiences. • Ability to identify and solve complex cybersecurity problems. • Driven by a deep curiosity to understand how systems work and have the persistence to investigate complex problems.

Post No / Post Name	**3 – Deputy Manager -Cyber Security Analyst**
BASIC QUALIFICATION **(AS ON 31.01.2026)**	**<u>Mandatory:</u>** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **<u>Preferred:</u>** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER CERTIFICATIONS **(AS ON 31.01.2026)**	**<u>Preferred Certifications:</u>** (Valid as on 31.01.2026) OSCP, OSCE, CRTE, CRTP, CEH, CISSP, OSEP, CCSP, SANS.
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.01.2026)**	**<u>Mandatory:</u>** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain.

	Preferred: Experience in offensive security, focusing on Ethical Hacking red teaming and penetration testing. **Training & Teaching experience will not be counted for eligibility.** **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Understanding of IT Security technology & processes particularly related to Web/Mobile Applications and Network Security. • Understanding of OWASP Web and Mobile Top 10 Application Security Vulnerabilities, Threat modelling, Red Teaming & Secure code review. • Ability to perform security assessment of Web and Mobile (Android and iOS) applications to identify OWASP Top 10 related vulnerabilities. • Knowledge of tools like Kali Linux, Burp suite, Nmap, Qualys/Nessus, Metasploit, HCL AppScan, Tenable SC, NMAP, etc. • Basic Knowledge of at least one programming knowledge such as C, C++, Python, Java, ASP.NET will be preferred. • Hands-on security testing of mobile applications (Static/ Dynamic/Memory Analysis) and experience on Dynamic instrumentation tools like Frida/Objection, Magisk etc. Knowledge on Android Development tools. • Proficiency in languages such as Python, Bash/Shell, C/C++, Java, and JavaScript, Burp Suit, Kali-Linux is crucial for scripting, automation, exploit development, and understanding system vulnerabilities. • Expertise in various penetration testing & red Team Testing methodologies (MITRE, OWASP Testing Guide, NIST SP 800-115, etc.), tools (Nmap, Metasploit, Burp Suite, Wireshark, John the Ripper, etc.), and techniques (reconnaissance, scanning, exploitation, post-exploitation, privilege escalation) • Knowledge of wireless protocols (Wi-Fi), security standards (WPA2, WPA3), and hacking methods (packet sniffing, encryption cracking). • Ability to analyse complex situations, identify challenges, and devise effective and innovative solutions through critical and lateral thinking, coupled with a knack for identifying potential security risks.

Post No / Post Name	**4 – Deputy Manager -Incident Management & Forensics**
BASIC QUALIFICATION (AS ON 31.01.2026)	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER QUALIFICATION (AS ON 31.01.2026)	**Preferred Certifications:** (Valid as on 31.01.2026) CHFI, Encase Certified Examiner (EnCE), Access Data Certified Examiner (ACE), GIAC Certified Incident Handler (GCIH). Certified Information Systems Security Professional (CISSP), GIAC Certified Forensic Analyst (GCFA). CEH, OSCP, OCEP.
WORK EXPERIENCE (POST-BASIC QUALIFICATION) (AS ON 31.01.2026)	**Mandatory:** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain. **Preferred:** Experience in Incident Response, forensic and malware Analysis. With hands-on experience in malware analysis, digital forensics, mobile forensics, Network forensics, Database forensics, Email forensics, cloud forensics. experience in cybersecurity, with a strong focus on incident response and security operations.

	Experience with various security incidents, such as malware, ransomware, phishing, DDoS attacks, and data breaches. **<u>Training & Teaching experience will not be counted for eligibility</u>**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	**Core Forensic Skills** • **Digital Forensics:** Expertise in acquiring, preserving, analysing, and reporting digital evidence from devices, servers, and networks. • Detection & Investigation: In-depth knowledge of detecting, investigating, and documenting fraud schemes such as money laundering, insider trading, and cyber frauds. • Incident Response: Ability to Execute and investigate data breaches, cyber incidents, and security threats efficiently. **Technical Skills** • **Forensic Tools Expertise:** EnCase, FTK, Magnet Axiom, X-Ways, Autopsy, Wireshark, Cellebrite, Oxygen Forensics (for mobile forensics) etc. • Forensic Imaging Tools: Tableau TX1/TDU/write blockers, Logicude Image etc. • SIEM & Threat Intelligence Tools: Splunk, IBM QRadar, ArcSight • Data Analysis & Scripting: SQL for data extraction from core banking systems • Python, PowerShell for scripting and automation • Malware Analysis & Reverse Engineering (preferred for cyber forensics roles) **BFSI, Regulatory & Legal Domain Knowledge** • Understanding of Financial Products & Systems • RBI Guidelines on Cybersecurity & Forensics • SEBI and IRDAI regulations • Chain of Custody: Ability to maintain legally admissible evidence trails • Report Writing: Skill in preparing detailed forensic reports and executive summaries. • Excellent communication and presentation skills. Ability to effectively communicate technical information to both technical and non-technical audiences. • Knowledge of network protocols and operating systems. • Hands-on experience in malware analysis, digital forensics, mobile forensics, Network forensics, Database forensics, Email forensics, cloud forensics. • Execute and coordinate the full lifecycle of cybersecurity incidents – identification, containment, eradication, recovery, and post-incident analysis. • Act as the primary responder for high-severity security incidents including malware outbreaks, DDoS, ransomware, phishing, data breaches, and insider threats. • Monitor and analyse logs and alerts from SIEM tools (e.g., Splunk, QRadar, ArcSight) to detect anomalies and potential threats across endpoints, networks, and applications. • Develop and maintain incident playbooks, escalation protocols, and response workflows in line with RBI cybersecurity directives. • Perform forensic analysis on compromised systems to determine the root cause, impact, and indicators of compromise (IOCs). • Collaborate with SOC analysts, threat intelligence teams, IT, legal, and external vendors during incident handling. • Prepare detailed incident reports and dashboards for senior management and regulators (e.g., RBI, SEBI). • Conduct post-incident reviews (PIRs) and contribute to improving the security posture through lessons learned and preventive controls. • Support compliance initiatives by aligning incident response processes with ISO 27001, RBI cybersecurity framework, NIST, and CERT-In advisories. • knowledge of incident response methodologies, frameworks, and best practices (e.g., NIST, ISO 27001, MITRE ATT&CK). • Proficiency with incident response tools and technologies, including SIEM, EDR, forensics tools, and security orchestration and automation (SOAR) platforms. • Solid understanding of networking, operating systems (Windows, Linux), cloud platforms (e.g., AWS, Azure, GCP), and security vulnerabilities.

	• Experience with scripting or programming languages (e.g., Python, PowerShell) for automation and analysis is a plus. • Excellent written and verbal communication skills, including the ability to communicate technical information effectively to both technical and non-technical stakeholders, including senior leadership. • Exceptional analytical, problem-solving, and decision-making abilities, with the capacity to think critically and strategically under pressure. • Ability to prioritize and manage multiple incidents concurrently, demonstrating strong organizational and time management skills.

Post No / Post Name	**5 – Deputy Manager -Test Engineers**
BASIC QUALIFICATION (AS ON 31.01.2026)	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER QUALIFICATION (AS ON 31.01.2026)	**Preferred Certifications:** (Valid as on 31.01.2026) ISTQB, STQC STANDARD MAPPING, CTFL, CSTE, CAST, CISSP, CISM, Technology Hardware related certifications are preferred.
WORK EXPERIENCE (POST-BASIC QUALIFICATION) (AS ON 31.01.2026)	**Mandatory:** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain. **Preferred:** Experience testing hardware / software and finding bugs. Must have experience in designing and executing test plans and procedures. This includes creating automated tests using scripting languages like Python. Needs strong debugging and troubleshooting skills to perform root-cause analysis of hardware/ software issues. Analysis of technology products and services. Experience as an analyst in a finance, business, or operational/technology setting. **Training & Teaching experience will not be counted for eligibility**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Strong understanding of hardware design principles, computer architecture, and electrical/electronic systems. • Experience with hardware testing methodologies, test equipment, and test automation tools. • Excellent analytical and problem-solving skills to diagnose and troubleshoot hardware faults. • Strong communication and documentation skills for creating clear and concise test plans and reports. • The ability to work in a fast-paced, dynamic environment and adapt to changing project requirements. • Strong understanding of computer hardware, hardware testing, and analysis, along with strong problem-solving, critical-thinking, and communication abilities to evaluate hardware, design systems, manage upgrades, and assist users. • **Programming and Scripting:** Knowledge of languages like Java or Python helps testers understand the software's architecture and automate tests. • **Operating Systems:** Familiarity with various OS platforms like Windows, macOS, Linux, iOS, and Android ensure compatibility testing. • **Test Automation Tools:** Proficiency with tools for test case management, defect tracking, and automation is essential for efficiency.

	• **Analytical & Critical Thinking:** The ability to meticulously assess software, break down complex problems, and identify root causes of defects. • **Communication:** Strong verbal and written skills are needed to communicate findings, document issues clearly, and collaborate effectively with development teams. • **Problem-Solving:** Testers must be able to systematically find solutions to issues encountered during the testing process. • **Attention to Detail:** A keen eye for detail is crucial for accurately identifying and documenting all defects and their nuances. • **Adaptability and Flexibility:** The software landscape is constantly changing, requiring testers to be adaptable and willing to learn new technologies and methodologies. • **User-Centric Mindset:** A focus on meeting user needs ensures the final software product is high-quality and user-friendly. • Strong analytical and problem-solving skills with a high degree of accuracy and attention to detail. • Adept at interpreting complex data, identifying trends, and proposing effective solutions. • Expertise in Microsoft Excel for data modelling, analysis, and reporting. • Proficiency with business intelligence (BI) and data visualization tools (e.g., Power BI, Tableau). • Excellent written and verbal communication skills. • Strong stakeholder management skills with the ability to influence and collaborate effectively across different teams and levels. • Builds and maintains strong, collaborative relationships with internal and external partners. • Understands business needs and strategic objectives to clarify the purpose of benchmarking efforts.

IMPORTANT POINTS:

1 The educational qualification prescribed for the post is minimum. Candidate must possess the Post Basic qualification and relevant full-time experience as on specified dates.

2 **The relevant experience certificate from the employer must contain specifically that the candidate had experience in that related field as required.**

3 In cases the certificate of degree/diploma does not specify the field of specialization, the candidate will have to produce a certificate from the concerned university/college specifically mentioning the specialization.

C. DETAILS OF BRIEF JOB PROFILE, ROLE & RESPONSIBILITIES, FUNCTIONS & ACTIVITIES:

Sl	POST	Detail description of Job Profile, Role, Responsibilities, and Functions.
1.	**Deputy Manager-** **IT Security Expert**	**Job Profile:** The IT Security Experts will operate as Cyber Defense Specialists and will execute the operations of the Cyber Defense Centre within the Cyber Security Centre of Excellence. The role involves building, managing, and operating advanced cyber defense capabilities covering Threat Intelligence, Incident Response, and Cyber Resilience functions. He/She will be responsible for monitoring, detecting, analyzing, and responding to cyber threats while ensuring compliance with regulatory and organizational requirements. **KRAs:** **On Ground Execution:** • Work with team of Cyber analysts, threat hunters, incident responders, and security engineers. • Drive collaboration with government agencies, regulators, industry partners, and academia. **Operational Management** • Ensure timely detection, triage, and response to security incidents. • Develop and implement playbooks for Incident Response and Cyber Crisis Management. • Manage Threat Intelligence lifecycle: collection, analysis, dissemination, and actioning. • Oversee vulnerability management and proactive threat hunting initiatives. • Maintain cyber resilience by conducting red team/blue team exercises, simulations, and drills. **Governance & Compliance** • Ensure alignment to national and international cybersecurity standards (ISO 27001, NIST, CERT-In guidelines, RBI/SEBI/MeitY advisories). • Prepare periodic risk, threat, and incident reports for leadership and regulatory bodies. • Support audits, compliance assessments, and cybersecurity maturity evaluations. **Capacity Building & Innovation** • Contribute to the CoE's knowledge repository through research, frameworks, and best practices. • Mentor and upskill team members on emerging cyber defense technologies (AI/ML in security, SOAR, SIEM, XDR, Cloud Security). • Foster innovation by engaging with startups, academia, and global cyber defense forums.

2.	Deputy Manager – Emerging Technology	**Job Profile:** It identifies, develops, and implements new strategies, technologies, and methodologies to enhance an organization's security posture against evolving cyber threats. They are responsible for leading cybersecurity initiatives, assessing new solutions, and ensuring that an organization remains resilient and secure in a dynamic threat landscape, requiring technical expertise and an innovative mindset to create novel approaches to threat management. It will play a key role in bridging business needs with technology or cyber solutions. The analyst works closely with business units, developers and project teams to ensure that technology / cyber initiatives align with organizational goals. Drive Cybersecurity innovation and applied research in the cybersecurity domain. Conduct evaluation of emerging security technologies and assess applicability in the banking environment. Build proof-of-concepts (PoCs) and pilot projects for advanced cybersecurity solutions. Engage with start-ups, incubators, and research institutions to scout, validate, and adapt innovative solutions. Assist in designing in-house tools, frameworks, and methodologies for cybersecurity innovation. Is responsible for collecting, analysing and interpreting data to help organizations make informed decisions. The role requires strong analytical and communications skills, attention to detail, and the ability to transform complex data into actionable insights. This role involves carrying out research initiatives, driving innovation in cybersecurity, and ensuring the organization's cyber defenses are robust and effective. **KRAs:** **Technology Analysis & Evolution:** • Evaluate new and existing technologies to determine suitability and potential impact on the business requirements. • Stay ahead of the curve by anticipating new cyber threats and vulnerabilities in the digital landscape. • Conduct feasibility studies and cost benefit analysis for technology /Cyber solutions. • Research, design, and implement innovative technical solutions and frameworks to strengthen cybersecurity defense. • Spearhead projects that introduce cutting-edge technologies and processes to protect networks, systems, and data. **Business and systems analysis:** • Collaborate with business stakeholders to gather and analyse technical and business requirements. • Translate business needs into functional and technical specifications. • Support business process reengineering and digital transformation initiatives. **Solution Design & implementation Support:** • Design system architectures, data flows and integration points. • Work with software developers, IT-Engineers and vendors during implementations. • Ensure solutions meet business, technical and compliance requirements. **Technical Documentations & Reporting:** • Prepare system and process documentations user guides and technical manuals. • Provide technical reports and dashboards to management stakeholders. • Present findings, technology options and recommendations in a clear business friendly manner. • Engage with internal and external stakeholders, including research institutions and industry partners, to foster a collaborative ecosystem for cybersecurity innovation. **Planning:** Developing and implementing the center's strategic vision and roadmap for cybersecurity research and development. **Research and Innovation:** Overseeing research projects focused on identifying and mitigating emerging cyber threats, developing new security technologies, and enhancing existing security protocols. **Collaboration and Partnerships:** Working with internal teams, external research institutions, and industry partners to advance cybersecurity knowledge and capabilities. **Knowledge Sharing:** Disseminating research findings and best practices throughout the organization and potentially to the broader cybersecurity community. **Staying Ahead of Threats:** Keeping abreast of the latest cybersecurity trends, threats, and technologies to ensure the organization remains protected.