Cytomate

Technical Proposal of Vulnerability Assessment and Penetration testing (VAPT) for QAPCO (RFQID P10-01-273)

Table of Contents

Document submission checklist

S. No		Description	Submitted		Remarks
			Yes	No	
1.0		Technical Compliance (All requested On-Demand Services covered)	Yes		Cytomate provides all the requested on-demand services mentioned in RFQ.
2.0		Technical Compliance – Compliance with On-Demand Services Call-In Procedure	Yes		Cytomate complies with Demand Services Call-In Procedure
	2.1	Availability of Manpower (with relevant level of expertise and qualification) - The CONTRACTOR shall deploy resource onsite maximum 30 days SLA on date from requirement received from QAPCO	Yes		Most of the activities in the Scope of Work can be done remotely. Therefore, onsite deployment of resources will not exceed 30 days.
	2.2	List of Deliverables	Yes		Mentioned under the section “Deliverables”.
	2.2	Man-days requirements against Activity/Services	Yes		Mentioned under the ”Man-days requirements” table in “Project Timeline” section.
3.0		Satisfy Technical Requirements for RFP Submission (All required documents are submitted for each services as per Scope)	Yes		Technical Requirement are satisfied.
	3.1	Demonstrate **experience with delivering similar engagements** - for the past five (5) years and accordingly share success stories highlighting past engagements and outcomes, and relevant references from previous clients	Yes		Mentioned under the ”Previous Experience” section.
	3.2	Demonstrate **personnel Competency and Experience**: CVs/resumes/profiles of key personnel, highlighting relevant projects and expertise; qualifications, certifications, and experience of the staff to be assigned to each on-demand activities.	Yes		CVs of key personnel are provided in Appendix A.
	3.3	**Methodology and approach**: including processes, techniques, risk management, Rules of Engagement (RoE), detailed plan outlining the phases of each activity, from initial scoping to final reporting	Yes		Provided under the section “Proposed Approach, Delivery Model, Methodology, Timing, and Outputs”.
	3.4	Describe **list of tools and software** that will be used for the activities, Justification for the selection of these tools and any relevant licenses.	Yes		Provided under the section “Tools”

	3.5	Provide **project timeline**: detailed timeline for each activity, including key milestones and deliverables; estimated durations, along with any critical dependencies; the actual start date will be determined by the QAPCO based on when the service is requested.	Yes		Detailed information is provided under the section "Project Timeline"
	3.6	**Compliance assurance** with Qatar's NCSA's Accreditation Penetration Testing Standard and other relevant industry standards and regulations (e.g., OWASP, NIST, ISO 27001); evidenced by certifications or accreditations held by the CONTRACTOR related to VAPT	Yes		NCSA's Accreditation Penetration Testing Standard certification is provided in Appendix B
	3.7	Approach to **confidentiality and data protection**: policies and procedures for ensuring the confidentiality and security of the QAPCO's data during the activities; data handling and storage practices	Yes		Provided under Appendix C
	3.8	**Communication and reporting** strategy throughout the engagement: format and frequency of interim and final reports	Yes		Communication strategy was briefly mentioned under the "Communication plan" section. More detailed strategy for communication was provided under Appendix D.
	3.9	Provide sample previous VAPT reports demonstrating the quality and depth of findings. Sample reports can be redacted, if necessary, to maintain client's confidentiality	Yes		Provided in Appendix E
	3.10	Describe post-assessment support and remediation assistance; availability for follow-up assessments or verification testing	Yes		Mentioned in the section: Phase 4 > Re-validation scan
	3.11	Satisfy following **minimum qualification and experience** for each of the following roles: a. Technical Consultants: • Holder of bachelor's degree preferably in information security, computer science, or systems engineering • Minimum of five (5) years of relevant experience. • Holder of, at least two (2), Information Security certifications in good standing: CISSP, CISA, GCFA, GCFE, C|HFI, CEH, ECSA, LPT, OSCP, OSCE, GPEN, GWAPT, GICSP, GRID, CREST Certified Simulated Attack Manager, or similar. b. Project Manager: Holder of Project Management certification(s) in good	Partial Yes		Technical consultants for this project satisfy the requirements of being the holder of Bachelor's Degree in Information Security and having minimum 5 years of experience. However, our technical consultants don't have the mentioned Information Security certification. Also, Project Manager for this project doesn't hold Project Management

		standing, such as PMI PMP or Prince2 Practitioner.			certification.
4.0		Satisfy General Requirements	Yes		General Requirements are satisfied.
	4.1	Activities execution approach: due care and diligence - Risks Management & Mitigation strategy to avoid disrupting processes or services in QAPCO environments	Yes		Risk Management is provided under Appendix F. Activities approach are explained in detail under the methodology and project timeline sections
	4.2	Hardware, software, tools etc. used during assessment shall be arranged by the CONTRACTOR	Yes		List of tools are mentioned in the section "Tools"
	4.3	Define which activities would be performed remotely and which activities to be conducted onsite. Coverage of the onsite activities have more weightage.	Yes		The table under the "Understanding of the Requirements for Services, including Assumptions" section outlines which activities will be performed remotely.
5.0		Optional: Subscription to Breach and Attack Simulation (BAS) Platform	Yes		Subscription BAS platform is mentioned in the commercial proposal.
6.0		Company Organization: 6.1 Clear Company organization and Management (Organization structure to be provided) 6.2 Company size and Resources	Yes		Organizational chart is provided in Appendix G.
7.0		Project Management: 7.1 Stakeholder Management. 7.2 Scope Management 7.3 Time Management 7.4 Project Risk Management 7.6 Project Communication Management	Yes		Stakeholder Management, Scope Management, and Time Management are mentioned under "Project Management" section. Risk management and Communication management are mentioned in appendices.
8.0		ISO Certification (Relevant documentation to be provided) or another International Certificate		No	Cytomate is currently in the process of acquiring ISO 270001 certification. Expected date: October 1st, 2024

Point of Contact

All communications relating to this Proposal shall be directed to the person designated to represent Cytomate. All notices shall be addressed to:

CYTOMATE SOLUTIONS AND SERVICES
Bilel B.A Al Souaied
Title: Chief Operating Officer
Email: bilel@cytomate.net
Phone: +(974) 3004 3010

Executive Summary

This document is for QAPCO, seeking Vulnerability Assessment & Penetration Testing services to improve the security posture of IT infrastructure and networks. Cytomate's approach to vulnerability assessment and penetration testing includes a thorough analysis of the QAPCO's infrastructure and application systems (**both grey box and black box**), using both automated and manual testing methods. Cytomate will simulate real-world attacks to identify vulnerabilities and provide recommendations for remediation and detailed actionable mitigations. Our testing will include both internal and external networks, network configurations, web-based applications, attack surface management and Internal Vulnerability assessment for QAPCO's servers. Cytomate will perform detailed compromise assessment of endpoints systems. Compromise assessment will include the scanning of handcrafted YARA, Sigma rules, and IoCs. This scanning includes thousands of latest YARA, Sigma and IoCs scanning of APT Campaigns. Cytomate will also perform detailed application testing. Application testing under grey and Blackbox covers the OWASP TOP 10, API security review, vulnerability scan. Our team will also work closely with the QAPCO's IT department to ensure minimal disruption to daily operations. In addition to the testing services, Cytomate will provide a comprehensive report of our findings and recommendations for QAPCO to improve its overall security posture. Our expertise and experience will enable us to comprehensively and effectively assess QAPCO's security posture.

Description of the Firm and the Firm's Qualifications

About the Company

Cytomate is an innovative Qatari cybersecurity company based in Doha, Qatar with the power of Automation & Autonomicity (Artificial Intelligence). ***Cytomate is evaluated, recommended, and invested in by Qatar Development Bank.*** Cytomate is the only Qatari company to have the Breach and Attack Simulation (BAS) solution empowered with Artificial Intelligence (SnipeX).

Why Us?

Cytomate believes in the importance of establishing a continuous testing mechanism for applications and security controls to guard against the latest threats. Our team comprises seasoned security professionals who dedicate substantial time to research and develop advanced exploits. These dynamic exploits cover a wide spectrum, simulating sophisticated cyberattacks employed by malicious actors in an automated and ongoing manner. Cytomate's approach involves executing a comprehensive series of attacks, spanning the entire MITRE ATT&CK matrix, to assess an organization's defense capabilities. We also craft unique exploits designed to bypass security controls, providing organizations with an accurate assessment of their defenses against advanced adversaries. This information empowers organizations to prioritize and take actionable steps to remediate vulnerabilities that may have been exploited successfully. Furthermore, Cytomate operates its dedicated research hub, the Cytomate Lab. Here, our team of experts, including Red Teamers, SOC Analysts, Deception Experts, and Reverse Engineers, collaborate on various projects to stay at the forefront of cybersecurity innovation and threat mitigation.

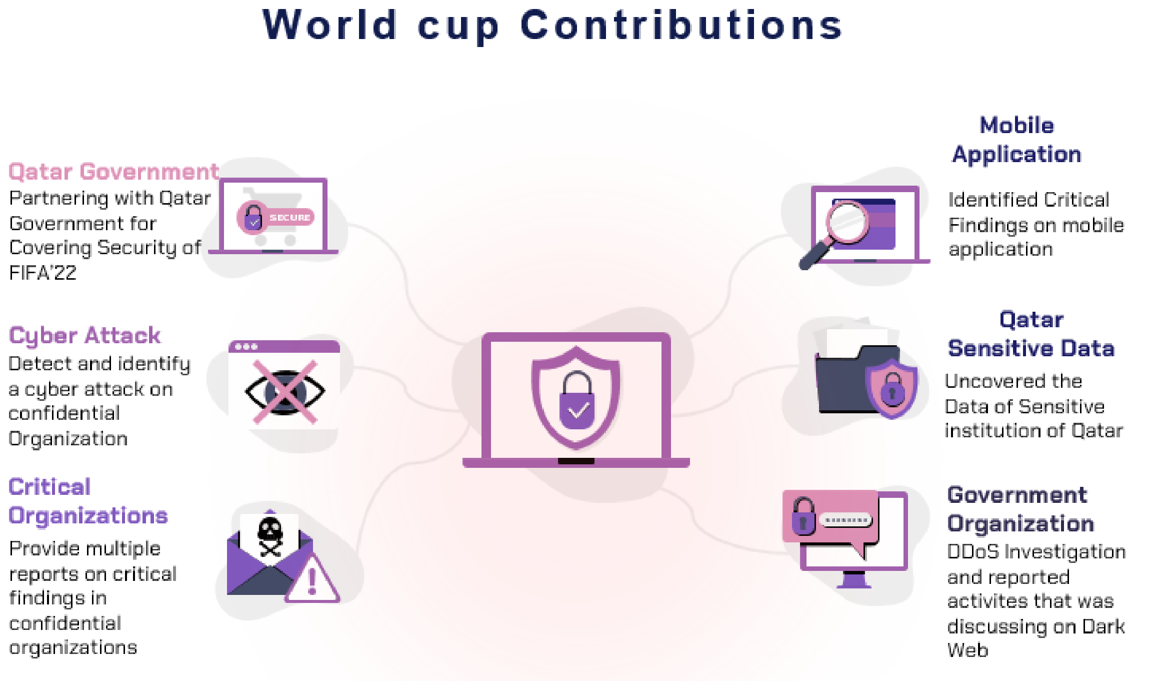
Previous Experience

Cytomate provided VAPT services to Sidra Medicine in 2024. The project scope included a comprehensive assessment covering Vulnerability Assessment, Applications Testing, Web Applications Testing, Internal Network Testing, Wireless and VOIP Testing, and a Security Configuration Review. Cytomate delivered these services with a high level of professionalism and expertise, meeting the expectations set by Sidra Medicine. The project successfully uncovered critical vulnerabilities, enhancing the security posture of Sidra Medicine. Additionally, Cytomate provided both executive and detailed reports outlining the findings, as well as presentation, which facilitated the mitigation of identified vulnerabilities and misconfigurations. The services contributed to ensuring regulatory compliance and reducing risk exposure, further strengthening Sidra Medicine's overall cybersecurity defenses.

Although Cytomate has been in the market for only 2.5 years, it provided comprehensive VAPT and Red Teaming Services to notable organizations in Qatar. During the FIFA World Cup 2022, Cytomate conducted security assessments on critical organizations from different industries, such as government, telecommunications, and banking.

FIFA’22 World cup Contributions

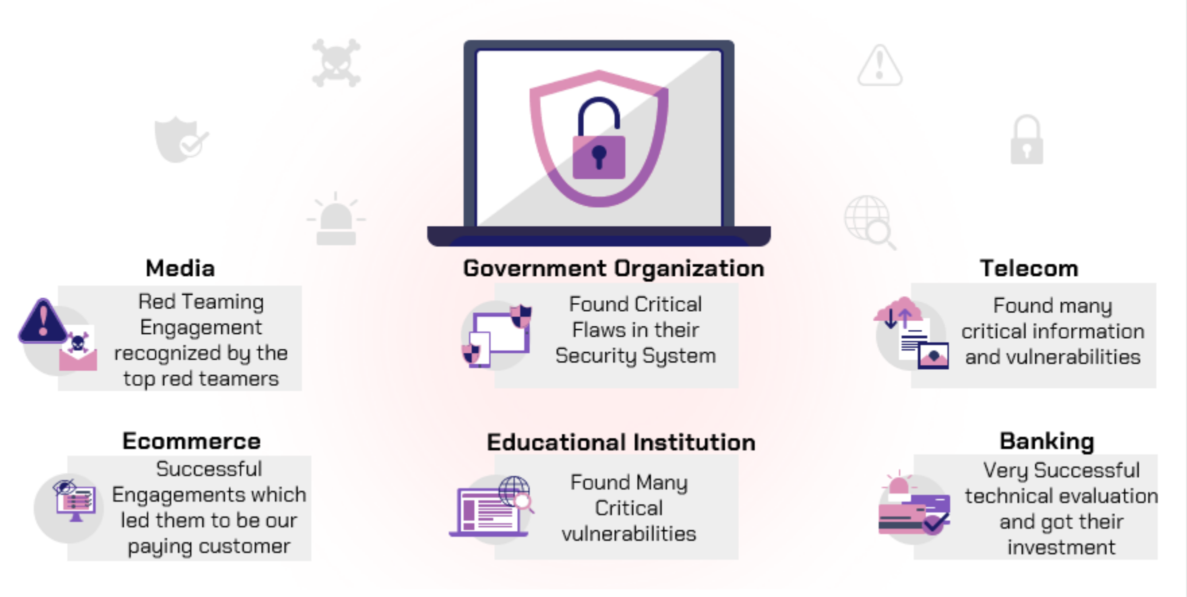
Cytomate was officially engaged by Amiri Diwan for covering the cyber security activities during the FIFA world cup 2022, following figures give very high-level details of such activities.


World cup Contributions
Qatar Government
Partnering with Qatar Government for Covering Security of FIFA'22
SECURE
Cyber Attack
Detect and identify a cyber attack on confidential Organization
Critical Organizations
Provide multiple reports on critical findings in confidential organizations
Mobile Application
Identified Critical Findings on mobile application
Qatar Sensitive Data
Uncovered the Data of Sensitive institution of Qatar
Government Organization
DDoS Investigation and reported activites that was discussing on Dark Web

What is SnipeX?

A Web Application Firewall (WAF) protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application and prevents any unauthorized data from leaving the app. SnipeX is an artificial intelligence (AI) tool that is created with the particular purpose of determining the type of firewall and how secure it is by crafting the payload by WAF behavior continuously and anonymously. SnipeX empowers cybersecurity professionals to customize and generate payloads that meet their specific requirements. This cutting-edge tool allows for the creation of tailored payloads, enabling users to simulate real-world attack scenarios and identify potential vulnerabilities in WAF. SnipeX also provides actionable feeds in addition to customized payload generation, which helps to harden the WAF.

Success Stories



Media
Red Teaming Engagement recognized by the top red teamers

Government Organization
Found Critical Flaws in their Security System

Telecom
Found many critical information and vulnerabilities

Ecommerce
Successful Engagements which led them to be our paying customer

Educational Institution
Found Many Critical vulnerabilities

Banking
Very Successful technical evaluation and got their investment

Understanding of the Requirements for Services, including Assumptions

QAPCO is currently in the process of executing a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) initiative, with the primary objective of thoroughly scrutinizing external network infrastructure, applications, systems, Internal servers’ vulnerability assessment, Endpoints compromise assessment and application security testing. This strategic undertaking forms an integral part of our routine cybersecurity measures, aimed at systematically validating the effectiveness of implemented security controls and proactively identifying and mitigating potential vulnerabilities. The VAPT process entails a meticulous examination of QAPCO's external and internal network infrastructure and systems. This involves a detailed analysis of hardware and software components, scrutinizing configurations, and assessing network architecture. The overarching goal is to gain a profound understanding of potential vulnerabilities that may exist within our digital ecosystem, identifying latent points of weakness susceptible to exploitation by malicious actors. Moreover, this assessment serves as a proactive measure to fortify the security landscape of the QAPCO external network infrastructure and systems. The insights derived from the VAPT process will play a pivotal role in refining our cybersecurity strategy. This, in turn, will enable us to implement targeted enhancements that specifically address identified vulnerabilities, thereby strengthening our defenses against potential cyber threats.

The objective of this VAPT assessment is to:

- Gain understanding of potential vulnerabilities of external network infrastructure, applications and systems.
- Gain understanding of potential vulnerabilities of Internal Servers.

- Evaluate the overall security posture of QAPCO endpoint systems by scanning 5000+ of YARA, Sigma, and IoCs.
- Evaluate the potential impact of identified vulnerabilities.
- Provide detailed recommendations for remediation and risk mitigation.
- Ensure compliance with relevant security standards and regulations (e.g., ISO 27001, CSF, OWASP, NIST).
- Enhance the organization's overall security posture through continuous improvement.

Note: Some terms will be used in the rest of the document which refers to Cytomate's products that will be used in assessments:

- **Racid:** Cytomate External Attack Surface Management
- **Breach+:** Cytomate Breach & Attack Simulation
- **SnipeX:** AI powered component of Breach+ for attacking WAF

The VAPT assessment include the following activities:

Assessment Phases	**Activity**	**Scope**
Phase 1 (remote)	External Vulnerability Assessment and Penetration Testing - **Black Box and Grey Box**	Cytomate external penetration testing service meticulously tests and evaluates the security of your organization's digital assets, leveraging the PTES (Penetration Testing Execution Standard) and OWASP (Open Web Application Security Project) frameworks. These services can be provided in 2 types which are BlackBox, Whitebox. Our detailed assessments cover the following areas to **QAPCO** external assets: • **Web Application:** Comprehensive testing QAPCO web applications to identify vulnerabilities such as SQL injection, cross-site scripting, and other exploitable weaknesses based on OWASP Top 10. • **Mobile Application:** Security assessments of mobile applications to detect issues like insecure data storage, improper session handling, and security misconfigurations. • **Cloud Infrastructure:** Evaluation QAPCO cloud-based infrastructure to ensure robust security against unauthorized access, data breaches, and other cloud-specific vulnerabilities. • **API Security Review:** Evaluate external API's connected to QAPCO web and mobile applications against OWASP API security guidelines for best practices. • **Enterprise 3rd party applications:** Evaluate enterprise 3rd party applications like ERP, Oracle, HRP system against vulnerabilities. *Step 1 (Automated):* Cytomate will perform Automated assessment using *Racid* (Cytomate external attack surface management proprietary solution), Burp, and Nessus to identify vulnerabilities.
		Step 2 (Manual): Cytomate will perform vulnerability assessment based on the findings and results of *Racid* and other solutions to validate the findings and results and provide the **risks** of vulnerabilities and their **mitigations**.
Phase 2 (remote)	External Web Application Security	Cytomate external penetration testing service meticulously tests and evaluates the security of your organization's digital assets, leveraging the POWASP (Open Web Application Security Project) frameworks.

	Testing - **Black Box and Grey Box**	These services can be provided in 2 types which are BlackBox, Whitebox. Our detailed assessments cover the following areas to **QAPCO** external assets: **OWASP & CWE Validation:** Comprehensive testing QAPCO web applications to identify vulnerabilities such as SQL injection, cross-site scripting, and other exploitable weaknesses based on OWASP Top 10 and CWE. **DoS Protection Validation:** Comprehensive testing QAPCO web applications to test DOS prevention and protection mechanism **WAF evasions:** Use of SnipeX tool to test WAF evasion with dynamic payloads to bypass WAF **Step 1 (Automated):** With some knowledge of application's Cytomate will perform security assessment and penetration testing on QAPCO's applications using **Next-Gen ASM** to validate the security posture and identify the misconfigurations and vulnerabilities of systems and applications. Cytomate will test and verify the encryption at different layers like **Transport Layer Encryption (TLS/SSL)** validity of the **SSL certificate**, Application Layer (**key management practices**). This assessment includes **session hijacking**, **Sensitive data exposure**, **Known vulnerabilities**, **Authentication and encryption** mechanisms, authorizations, **OWASP Top 10.**
		Step 2 (Manual): Cytomate will perform penetration on deployed applications manually to access the **QAPCO Web application-level** security. This assessment includes the testing of running **Published Apps**, **Portals**, **Websites** like session management, **Authentication mechanism** (MFA), Manually exploring interfaces, **Session/Cookies** security and may include the installation of tools on deployed server to perform penetration testing. Cytomate will check **OWASP TOP 10** vulnerability like **Injection, Broken Authentication and session, IDOR, XSS, Sensitive data exposure, CSRF, TLS security** and other unknown attack vectors.
Phase 3 (on-site or remote)	Internal Penetration Testing – **Black Box and White Box**	**Cytomate** internal penetration testing service meticulously tests and evaluates the security of your organization's digital assets, leveraging the PTES (Penetration Testing Execution Standard) and OWASP (Open Web Application Security Project) frameworks. These services can be provided in 2 types which are Black-Box, Gray-Box. Our detailed assessments cover the following areas to **QAPCO's** internal assets: • **Web Application**: Comprehensive testing of your web applications to identify vulnerabilities such as SQL injection, cross-site scripting, and other exploitable weaknesses based on OWASP Top 10. • **Active Directory:** Evaluate the security posture of the Active Directory environment, focusing on configuration vulnerabilities, password policies, and access controls, and provide recommendations for strengthening overall security. Active Directory testing is done to identify and exploit potential weaknesses, ensuring robust defenses against unauthorized access and privilege escalation.

		• **Wireless and VOIP:** Cytomate will evaluate the integrity and resilience of network components, including routers, switches, OS fingerprinting, network sniffing, spoofing, default credentials and **wireless** access points, WPA cracking and security. It includes vulnerability assessments, penetration testing, and traffic analysis to identify weaknesses and potential points of compromise. • **API Security Review:** Evaluate internal API's connected to QAPCO web and mobile applications against OWASP API security guidelines for best practices. • **Enterprise 3rd party applications:** Evaluate enterprise 3rd party applications like ERP, Oracle, HRP system against vulnerabilities. **Internal Databases:** Evaluate Internal databases for access controls, data exposure, and misconfigurations. **Container Security Review:** Evaluate container security for vulnerabilities in container configurations, access controls, and runtime security. ***Step 1 (Automated):*** Cytomate will perform internal penetration testing on QAPCO's network using Cytomate **Racid**, ***Breach+*** (Breach and attack simulation proprietary solution) and other tools like Nessus and OpenVAS to validate the security controls and identify the misconfigurations and vulnerabilities in above mentioned assets. In the case of Active Directory environment ***Breach+*** will perform automated Lateral movement and Active Directory exploitation to test the misconfigurations.
		Step 2 (Manual): Cytomate will perform internal penetration on deployed systems, applications manually using tools and exploitation kits to access the QAPCO's security. This assessment includes the testing of active directory and internal network devices, desktops, servers etc.
Phase 4 (on-site or remote)	Network Security Controls Validation	Breach+ has capabilities to validate the **In-line security controls** by replicating and replaying malicious traffic. This traffic is captured by real world APT attacks. Breach+ agent replays APT traffic in a unique manner to validate the In-line security controls such as **firewalls (Fortinet), IPS/IDS (FortiGate), Palo Alto, Cisco** or any network level security control. Assessment will cover: • Firewall Basiline Policies Validation • URL Filtering Validation • Anti Malware Validation • Intrusion Prevention Validation • File Blocking Validation • Application & Web Filtering Validation • PCAP Replay Risk reports will be provided based on MITRE. Assessment will be done once a month for.

Phase 5 (on-site or remote)	Email Gateway Security Controls Validation	**Email Infiltration:** Breach+ fortifies email gateway security through a **dual-method** strategy, focusing on **Threat Intelligence validation** and by sending malicious attachments, including APT (**Advanced Persistent Threat**) threats and **phishing links mapped on MITRE ATT&CK framework**. This approach is powered by AI-based models that generate sophisticated and realistic content, simulating a broad spectrum of email-based threats to test and validate the gateway's defenses. Simultaneously, Breach+ tailors' organization-specific policy-based mitigations, offering a proactive layer of defense designed to preemptively thwart email-based attacks. **Threat Intel. Validation:** Breach+ uses **AI-Based** custom models to generate content and send live real-world malware phishing links to validate the security of email gateway. This method validates solutions like **Sandboxing** and **CDR solutions**. **Advanced Evasion:** Breach+ validates the email gateway security by sending advanced custom created and APT threats based **malicious attachments**. This method checks the misconfigurations of organization policies, allows extensions and also validates the security of email gateway.
Phase 6 (on-site or remote)	Endpoint Security Controls Validation	Cytomate Assess the security of QAPCO Endpoint security controls, ensuring they are effectively protecting against malware, unauthorized access, and other threats. **Node Breach:** Cytomate Breach+ solution has large repository of exploits based on **MITRE ATT&CK** and contains APT groups emulation capabilities. Breach+ will perform simulation and emulation based on real **APT groups** TTPs, create custom campaigns for real world samples and validate the security posture. Cytomate Breach+ solution has capability to perform all simulation and emulation automatically and in safe manner. **Threat Intel. Validation:** Cytomate Breach+ validates endpoint security controls by utilizing three methods. Threat Intel. Validation is one of the methods to validate endpoint and network security controls. In this method, Breach+ agents download real-world malware samples, files and check the static detection of malware. This method validates that organization security controls has updated threat intelligence. **Adversary Emulation:** Breach+ emulates the behavior of **real-world** malware in the presence of security controls to validate the security controls. In adversary emulation method, Cytomate R&D team reverse engineered the real-world malwares and extracted the TTP's of APT threats. Cytomate R&D team re-created extracted TTPs in the same manner with **behavior code mirroring** techniques and emulate all created TTPs in a sequence to provide TTP based insight about real world malwares. **Advanced Evasion:** Cytomate breach and attack simulation platform (Breach+) performs real emulation to check the endpoint as well as network level security controls by making command and control session using **C2 and C3** (Custom command and control). Cytomate

		executes ransomware and emulates all behavior of ransomware in the presence of security controls to validate the security posture of organization. Cytomate utilizes **attack scenario language (ASL)** and **polymorphic** approach to validate the security posture of organization. **APT Campaign:** Cytomate Breach+ executes **APT campaigns** to validate the security controls and to identify the attack paths. This feature enable organization to access **cyber kill chain** from initial access to post-exploitation. Users can create their custom APT campaigns according to real-world threats. Detailed and risk reports will be provided. Assessment will be done once quarterly.
Phase 7 (on-site or remote)	Security Architecture Review	Cytomate provides two approaches to validate the configuration of security controls. One approach includes simulating advanced attack paths and exploiting them in safe manner to validate the endpoint and network level security controls and also provide threat intelligence and signature to block threats. The second approach is to check the ***access control***, ***password policies***, ***firmware version*** and vulnerabilities,etc. This process involves a detailed examination and validation of previously **identified vulnerabilities** within a system or network. By conducting a **confirmatory** scan, security professionals can verify that these vulnerabilities have been adequately addressed and remediated. It also helps in identifying any new or overlooked vulnerabilities that might have emerged since the last assessment.
Phase 8 (on-site or remote)	Configuration review	Cytomate identifies potential security risks, compliance issues, and performance inefficiencies. Cytomate also verifies that the configurations support system stability and adhere to organizational policies. The review helps prevent vulnerabilities and ensures that changes are managed appropriately. Cytomate verifies that the configuration complies with relevant standards, regulations, and policies.
Phase 9 (remote)	Social Engineering	Cytomate Social Engineering Service encompasses a comprehensive range of activities aimed at fortifying your organization's defenses against social engineering attacks. The scope of our service includes: **Employee Training and Awareness:** • Developing and delivering customized training programs to educate employees about the various forms of social engineering attacks, such as phishing, pretexting, baiting, and tailgating. Providing practical exercises and simulations to enhance employees' ability to recognize and respond to social engineering attempts.
Phase 10 (on-site)	Compromise Assessment - Network Forensic Analysis	Cytomate will examine network traffic, logs, and configurations to identify indicators of compromise (IoCs) such as unusual data flows, unauthorized connections, or malware communication. This assessment will help to determine if a breach has occurred, the extent of the compromise, and the methods used by attackers. The findings will be used to enhance security measures and prevent future incidents.
Phase 11 (on-site)	Compromise Assessment - Host Forensic	Cytomate will analyze files, processes, system logs, and memory for indicators of compromise (IoCs) such as unauthorized access, malware, or abnormal behavior. This will help to determine if a system has been

	Analysis	breached, understand the nature and scope of the compromise, and identify how the attacker gained access. The results will help in remediating the issue and strengthening the system's defenses against future attacks.
Phase 12 (on-site or remote)	Source Code review	**Automated:** Cytomate will use SonarQube for inspection of code to perform automatic reviews with *static analysis* of code to detect bugs. **Manual:** Manual Source Code Analysis will be done to identify bugs, vulnerabilities, inefficiencies, or deviations from coding standards.

Proposed Approach, Delivery Model, Methodology, Timing, and Outputs

Project Initiation & Planning

In the beginning, a formal, typically short document (project charter) describes the project in its entirety, including the objectives, how it will be carried out, and who the stakeholders are. It is used throughout the project lifecycle.

The planning phase includes developing a roadmap for everyone to follow. In that phase, a Project Management Plan, which is a document that defines how a project is executed, monitored, and controlled will be created by our experienced project managers; it is much more than a schedule chart. It may be a summary or a detailed document and may include baselines, subsidiary management plans, and other planning documents. This document is used to define the approach the project team takes to deliver the intended project management scope of the project.

Service Delivery Models

Cytomate Company offers a range of Penetration Testing delivery models, including Onsite, Offsite, and Managed services. We tailor our approach to meet the specific needs of QAPCO, providing flexibility and top-notch cybersecurity solutions and services.

- **On-site testing model:** The Cytomate shall have the Penetration Testing team physically deployed at the QAPCO's location to perform the testing. This model is used for internal network/application testing, wireless Penetration Testing, and social engineering assessments that might require physical access to the facilities as per scope of work.
- **Remote testing model:** The Cytomate conducts without being physically present at the QAPCO's location.

Testing Approaches

- **Black Box Testing:** In Black Box Testing, Cytomate conducts assessments without prior knowledge of the internal workings or infrastructure details. This approach simulates an external threat scenario, allowing for a more realistic evaluation of how a potential attacker might target and exploit vulnerabilities. By focusing on the system's observable inputs and outputs, this testing method helps identify vulnerabilities from an outsider's perspective.
- **White Box Testing:** White Box Testing involves complete disclosure of the digital environment to the testing provider. Unlike Black Box Testing, in this approach, the tester has full access to the internal workings, source code, and architecture of the system. This method provides a detailed insight into the internal logic and structures, allowing for a thorough examination of potential vulnerabilities from within. White Box Testing is

particularly effective in identifying issues related to code quality, logic flaws, and overall system design.

- **Grey Box Testing:** Grey Box Testing allows for a more nuanced assessment, combining the advantages of both Black Box and White Box approaches. It is useful when complete disclosure may not be practical, yet a deeper understanding of the system is required for a more targeted evaluation.

Methodology

Cytomate's methodology for conducting the vulnerability assessment and penetration testing includes the following steps:

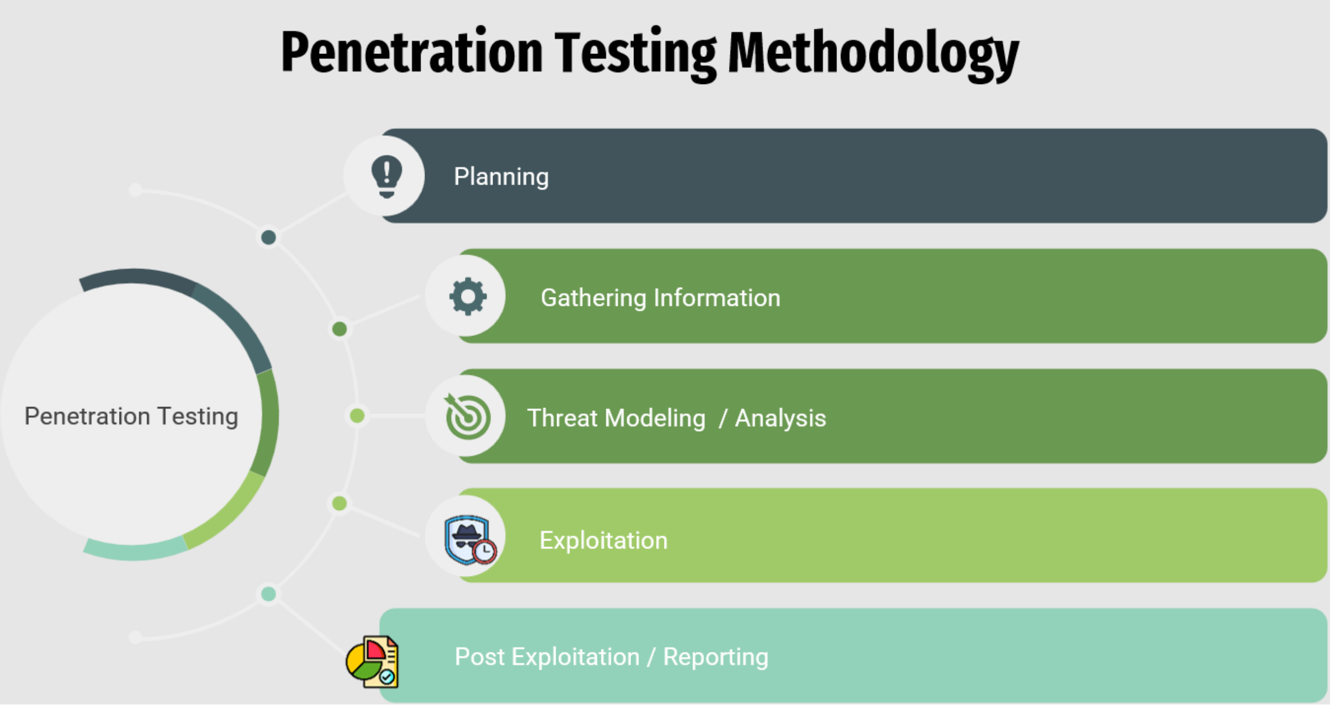
1. Planning & Reconnaissance:
In this initial phase, the penetration testing team gathers as much information as possible about the target system or network. This includes identifying potential entry points, understanding the technology stack, and profiling potential vulnerabilities. Threat modeling plays a crucial role here by helping the team anticipate and categorize potential threats and risks based on the gathered information.

2. Scanning & Enumeration:
Once the target is identified, the scanning and enumeration phase begins. The goal is to identify live hosts, open ports, and services running on the target system. This step involves using tools and techniques to map the network architecture, discovering potential weaknesses that could be exploited. Threat modeling continues to be relevant here, helping to assess the potential impact of vulnerabilities and prioritize them based on the level of risk they pose.

3. Gaining Access:
Exploiting identified vulnerabilities comes in the gaining access phase. This step involves attempting to penetrate the target system by leveraging the vulnerabilities discovered during the scanning and enumeration phase. Threat modeling guides the penetration testing team in understanding how these vulnerabilities could be exploited in real-world scenarios and the potential consequences of successful exploitation.

4. Maintaining Access:
Simulating a real-world attacker's behavior is the objective in this phase. Once access is gained, the team works to understand the depth of access an attacker could achieve. This involves moving laterally within the network, escalating privileges, and maintaining persistent access. Threat modeling helps in anticipating the potential paths an attacker might take and the critical assets they might target for long-term access.

5. Analysis & Reporting:
In the final phase, the penetration testing team collates findings, recommends fixes for identified vulnerabilities, and presents a detailed report. Threat modeling aids in providing a comprehensive understanding of the security posture, helping prioritize recommendations based on the severity and potential impact on the organization.


Penetration Testing Methodology
Penetration Testing
Planning
Gathering Information
Threat Modeling / Analysis
Exploitation
Post Exploitation / Reporting

Phase 1

External Security Assessment and Penetration Testing - Black Box

Attack Surface Management and Vulnerability Management

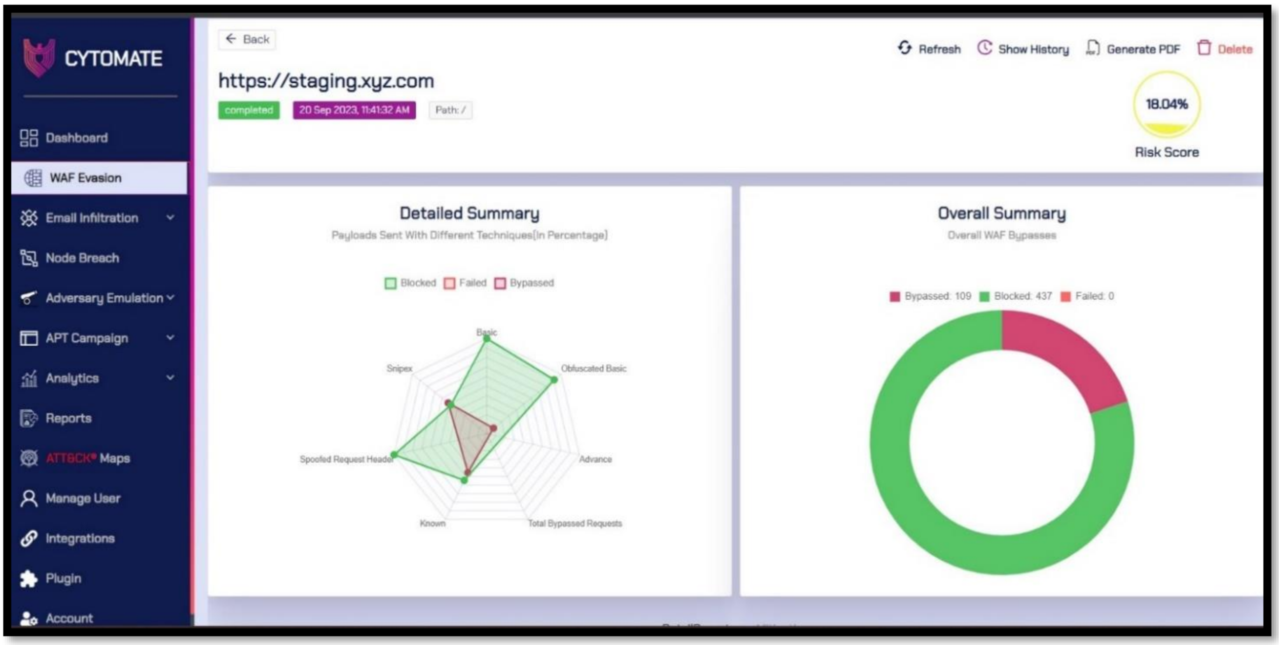
- **Asset inventory:** The first step is to identify all the assets and resources that are part of an organization's attack surface, including hardware, software, and network components.
- **Vulnerability scanning:** The next step is to perform vulnerability scanning to identify any vulnerabilities that exist in the assets identified in the asset inventory.
- **Risk analysis:** Once the vulnerabilities have been identified, the next step is to analyze the risks associated with each vulnerability to prioritize remediation efforts.
- **Exploitation and Command & Control:** We will exploit identified vulnerabilities, test the QAPCO's web application firewall (WAF) using the SnipeX (Our AI tool as described in above section), create custom payloads using SnipeX that bypasses the given WAF. Upon finding a vulnerability these payloads can be used by analysts to check whether the said vulnerability can be exploited or not after permission.
- **Reporting and Recommendation:** We will provide a comprehensive report detailing our findings and recommendations for QAPCO to improve their overall security posture.

AI-Based WAF Assessment

- **Asset inventory:** The first step is to identify all the web applications that are protected by the WAF, along with their functionalities and criticality.
- **Configuration review:** To review the configuration of the WAF to ensure that it is properly configured to protect against the identified attack vectors.
- **Attack simulation:** The next step is to simulate attacks against the web applications to test the effectiveness of the WAF in blocking the attacks.
- **Attack Vectors:** Cytomate validates the WAF by sending malicious payloads. These payloads include different categories such as XSS, SQLi, CMDi, LFI.
- **SnipeX:** Cytomate has in-house build tool SnipeX which use Artificial Intelligence (AI) to

mutate the payloads in order to bypass web application firewalls.

- **Agent-less:** Breach+ perform all web attacks and WAF testing without any agent. This component is external to validate the web application.
- **Efficacy analysis:** Based on the results of the attack simulation, an efficacy analysis is performed to identify any gaps in the WAF's protection and to prioritize remediation efforts.
- **Remediation planning:** Based on the efficacy analysis, a remediation plan is created that outlines the steps needed to address the gaps in the WAF's protection.



AI-Based WAF Evasion

Breach+ employs SnipeX tools, which utilize machine learning algorithms to dynamically mutate payloads, aiming to evade detection by web application firewalls (WAFs). This sophisticated approach to web application testing represents a significant advancement for Breach+, enhancing its capabilities in assessing security measures. Of particular interest is the notable bypass success rate observed with SnipeX payloads when tested against industry-leading WAF vendors such as F5 Big-IP and Cloudflare. Recognizing the importance of advanced WAF testing methodologies, organizations like QAPCO are encouraged to incorporate similar techniques to strengthen and update their defense mechanisms effectively.

Phase 1.1

External Security Assessment and Penetration Testing - Grey Box and BlackBox

Black Box Testing

1. Information Gathering

- *Step 1 Identify the Target:* This is the first step in any black box testing, which involves identifying the target web application.
- *Step 2 Observe Publicly Available Information:* Cytomate will look for any information available publicly, such as the technologies used, software versions, email addresses, etc.
- *Step 3 Crawl the Application:* Cytomate will use automated tools and manually crawl the website to understand the application structure and functionalities.

2. Vulnerability Identification

- *Step 4 Conduct Automated Scanning:* Cytomate will use automated tools to conduct a surface-level vulnerability assessment of the web application. This will help in identifying common issues quickly.
- *Step 5 Manual Testing:* Cytomate will go through the OWASP Top 10 vulnerabilities and manually test for these vulnerabilities.
- **Step 6 Encryption Testing:** Cytomate will verify proper implementation of transport layer security (TLS/SSL) for secure communication. Test for data at rest encryption in databases and storage systems, if applicable.
- **Step 7 Authorization and Access Control:** Cytomate will test user roles and permissions to ensure users can only access appropriate resources. Verify that users cannot access unauthorized functionalities or data.
- **Step 8 Input Validation and Injection:** Cytomate will test input fields for SQL injection, XSS (Cross-Site Scripting), and other injection attacks. Ensure proper input validation and output encoding to prevent injection vulnerabilities.

3. Exploitation

- *Step 9 Exploit Identified Vulnerabilities:* Once the vulnerabilities have been identified, Cytomate will exploit them to understand their severity and potential impact.

Technical Details

- **Injection**
  Description: Testing for injection vulnerabilities by inserting malicious input into queries or commands.
  Techniques: SQL Injection, NoSQL Injection, Command Injection.
- **Broken Authentication and Session Management**
  Description: Evaluating the strength of authentication mechanisms and session controls.
  Techniques: Brute force attacks, session fixation, session hijacking.
- **Insecure Direct Object References**
  Description: Identifying direct access to internal objects via manipulated URLs or forms.
  Techniques: Modifying URL parameters, form inputs to access unauthorized data.
- **Cross-Site Scripting (XSS)**
  Description: Injecting malicious scripts into web pages that other users will view.
  Techniques: Reflected XSS, Stored XSS, DOM-based XSS.
- **Insufficient Transport Layer Protection**
  Description: Assessing the encryption of data in transit.
  Techniques: Inspecting HTTPS implementations, checking for outdated encryption protocols.
- **Failure to Restrict URL Access**
  Description: Testing for unauthorized access to restricted pages.
  Techniques: Manual URL manipulation, automated scanning for access control gaps.
- **Sensitive Data Exposure**
  Description: Identifying exposure of sensitive data through weak encryption or misconfigurations.
  Techniques: Examining data storage practices, inspecting transmitted data for encryption.

- **Cross-Site Request Forgery (CSRF)**
  Description: Testing for CSRF vulnerabilities by crafting requests that perform actions on behalf of authenticated users.
  Techniques: Creating and submitting malicious forms or requests.
- **Un-validated Redirects and Forwards**
  Description: Identifying unvalidated redirects or forwards that could be exploited for phishing or malicious redirection.
- Techniques: Modifying redirect parameters, analyzing HTTP headers for unsafe redirects.

Grey Box Testing

4. Information Gathering

- ***Step 10 Utilize Provided Information:*** In grey box testing, QAPCO will provide some information about the application. Cytomate will use this information to better understand the target.

5. Vulnerability Identification

- ***Step 11 Authenticated Scanning:*** Unlike black box testing, grey box testing often involves testing while authenticating the application. This can uncover vulnerabilities that might not be visible to unauthenticated users, such as session hijacking.
- **Step 12 Multi-Factor Authentication (MFA) Testing:** Test MFA enforcement for applicable user roles and actions. Verify that MFA can't be bypassed or easily disabled.
- **Step 13 Conditional Access Testing:** Cytomate will test different access scenarios based on the conditional access policies defined. For example, Cytomate will test accessing resources from different devices, locations, or times of day. Cytomate will verify that conditional access policies are correctly applied and that users are blocked or granted access as expected.
- **Step 14 Encryption Testing:** Cytomate will verify proper implementation of transport layer security (TLS/SSL) for secure communication. Cytomate will test for data at rest encryption in databases and storage systems, if applicable.

6. Exploitation

- ***Step 14 Exploit Identified Vulnerabilities:*** Cytomate will try to exploit the vulnerabilities identified during the authenticated scanning phase.

Technical Details

- **Injection**
  Description: Input validation testing for injection attacks in input fields.
  Techniques: SQL Injection, NoSQL Injection, Command Injection.
- **Broken Authentication and Session Management**
  Description: Evaluating the strength of authentication mechanisms and session controls.
  Techniques: Brute force attacks, session fixation, session hijacking.
- **Insecure Direct Object References**
  Description: Identifying direct access to internal objects via manipulated URLs or forms.
  Techniques: Modifying URL parameters, form inputs to access unauthorized data.
- **Cross-Site Scripting (XSS)**
  Description: Injecting malicious scripts into web pages that other users will view.

Techniques: Reflected XSS, Stored XSS, DOM-based XSS.

- Insufficient Transport Layer Protection

  Description: Assessing the encryption of data in transit.

  Techniques: Inspecting HTTPS implementations, checking for outdated encryption protocols.
- Failure to Restrict URL Access

  Description: Testing for unauthorized access to restricted pages.

  Techniques: Manual URL manipulation, automated scanning for access control gaps.
- Sensitive Data Exposure

  Description: Identifying exposure of sensitive data through weak encryption or misconfigurations.

  Techniques: Examining data storage practices, inspecting transmitted data for encryption.
- Cross-Site Request Forgery (CSRF)

  Description: Testing for CSRF vulnerabilities by crafting requests that perform actions on behalf of authenticated users.

  Techniques: Creating and submitting malicious forms or requests.
- Un-validated Redirects and Forwards

  Description: Identifying unvalidated redirects or forwards that could be exploited for phishing or malicious redirection.

  Techniques: Modifying redirect parameters, analyzing HTTP headers for unsafe redirects.

Post-Testing

- *Step 15 Report Preparation:* Cytomate will prepare a detailed report documenting the vulnerabilities identified, their potential impact, and recommended mitigations.
- *Step 16 Presentation to the Stakeholders:* Cytomate will present the report to the stakeholders to help them understand the security posture of the application and what steps need to be taken to address the identified vulnerabilities.
- *Step 17 Re-*Validation: Cytomate team will decide the timestamp with QAPCO to re-validate the all-exploited issues and vulnerabilities after applying the mitigations.

API Security Pentesting

1. API Discovery

- *Step 1 Identify Existing APIs:* The first step is to identify all existing APIs across the infrastructure, both SOAP and REST APIs will be included.

2. Authentication & Authorization

- *Step 2 Inspect Authentication Mechanisms:* Cytomate will check if the APIs implement strong authentication. For REST APIs, standard methods include OAuth or JWT. For SOAP APIs, WS-Security standard will be used.
- *Step 3 Review Authorization Checks:* Cytomate will ensure that APIs have appropriate authorization checks in place, and the principle of least privilege is applied.

3. Input Validation

- *Step 4 Input Validation:* Cytomate will verify that the APIs perform sufficient input validation to prevent attacks such as SQL injection, XML external entity (XXE) attacks (for SOAP APIs), or JSON injection (for REST APIs).

4. Key Management

- **Step 5 Secure Storage:** Cytomate will verify that keys are stored securely, ideally in a dedicated key vault or secure configuration store.
- **Step 6 Avoid Hardcoding**: Cytomate will ensure keys are not hardcoded directly into the source code or configuration files.

5. Encryption

- ***Step 7 Check Encryption:*** Cytomate will ensure that data is encrypted in transit using protocols like HTTPS.

6. Error Handling

- ***Step 8 Review Error Handling:*** Errors will be handled properly and should not disclose sensitive information.

7. Rate Limiting

- ***Step 9 Rate Limiting:*** Cytomate will check if the APIs implement rate limiting to protect against DDoS attacks and brute-force attacks.

8. Logging & Monitoring

- ***Step 10 Logging and Monitoring:*** Cytomate will ensure that all API calls are logged, and an effective monitoring system is in place to detect any suspicious activity.

9. Automated Security Scanning

- ***Step 11 Scan for Vulnerabilities:*** Cytomate will use automated tools to scan APIs for common vulnerabilities.

10. Manual Testing

- ***Step 12 Manual Testing:*** Cytomate will conduct manual testing to identify vulnerabilities that automated tools might miss.

11. Report

- ***Step 13 Compile and Present Report:*** Finally, Cytomate will compile a detailed report documenting the identified vulnerabilities, their potential impact, and recommended mitigations. This report will be shared with relevant stakeholders for review and action.
- ***Step 14 Re*-Validation:** Cytomate team will decide the timestamp with QAPCO to re-validate the all-exploited issues and vulnerabilities after applying the mitigations.

Mobile Application Penetration Testing

- *Scope*: Cytomate will gather scope from QAPCO for IOS and Android application testing. The scope will include which components of the application will be tested and information will be provided by QAPCO for testing. User accounts will be provided by QAPCO for testing. QAPCO will provide apk and ipa for Android and IOS testing
- *Static Analysis:* Cytomate will start application testing with static analysis of applications. Static analysis will include checking for sensitive information in configuration files, such as API keys or passwords. Cytomate will also look for weak encryptions, local file storage and other weak ciphers. During static analysis reverse engineering will be done to read code of application to test obfuscation. During the static analysis, the app's resistance to tampering, such as modifying or repackaging the app without detection will be tested. Cytomate will also test the security of IPC mechanisms like intents, broadcast receivers, and content providers. Cytomate will also use their own tool Racid for static analysis of the application and discovery of any rogue application.

- *Dynamic Analysis:* Cytomate will perform dynamic analysis of applications after static analysis. Cytomate will test the app during runtime to identify issues like insecure data storage, improper session handling, and weak encryption. Cytomate will perform input validation testing to detect vulnerabilities such as SQL injection, XSS, and buffer overflows. Cytomate will also verify the effectiveness of authentication and authorization mechanisms, ensuring they are robust against attacks like brute-force or session hijacking Verify the effectiveness of authentication and authorization mechanisms, ensuring they are robust against attacks like brute-force or session hijacking.
- *Compile and Present Report:* After the test, Cytomate team compiles a detailed report outlining the methodology used, the vulnerabilities identified and exploited, the data that was accessed, and recommendations for improving security. This report is then presented to QAPCO.
- **Retest**: After remediation, Cytomate will conduct another round of testing to ensure that vulnerabilities have been effectively addressed.

Cloud Assessment Methodology

Scope Definition:

- Clearly define the scope of the assessment, including assets, services, and data within the cloud environment.
- Identify the specific cloud service providers and configurations under assessment.

Information Gathering:

- Collect information about the target organization, its cloud architecture, and relevant technologies in use.
- Enumerate cloud assets, such as servers, databases, storage, and networking components.

Threat Modeling:

- Identify potential threats and risks to the cloud environment.
- Prioritize threats based on their impact and likelihood.

Vulnerability Analysis:

- Perform automated vulnerability scanning to identify common weaknesses.
- Manually analyze the results to eliminate false positives and prioritize critical vulnerabilities.

Identity and Access Management (IAM) Testing:

- Evaluate the effectiveness of user authentication and authorization mechanisms.
- Check for misconfigurations in roles and permissions.

Data Storage and Encryption Testing:

- Assess the security of data storage solutions.
- Verify encryption mechanisms for data at rest and in transit.

Network Security Testing:

- Analyze network configurations and firewall rules.
- Test for the effectiveness of network segmentation and isolation.

Web Application Testing:

- Assess the security of web applications hosted in the cloud.
- Test for common web application vulnerabilities, such as SQL injection and cross-site scripting.

Container Security Testing:

- Evaluate the security of containerized applications and orchestration platforms.
- Check for container escape vulnerabilities.

Phase 1.2

External Web Application Penetration Testing

- *Identify the Target:* This is the first step in any black box testing, which involves identifying the target web application. Information related to user roles and credentials will be provided by QAPCO.
- *Observe Publicly Available Information:* Cytomate will look for any information available publicly, such as the technologies used, software versions, email addresses, etc.
- *Crawl the Application:* Cytomate will use automated tools and manually crawl the website to understand the application structure and functionalities.
- *Conduct Automated Scanning:* Cytomate will use automated tools to conduct a surface-level vulnerability assessment of the web application. This will help in identifying common issues quickly.
- *Manual Testing:* Cytomate will go through the OWASP Top 10 vulnerabilities and manually test for these vulnerabilities.
- **Encryption Testing:** Cytomate will verify proper implementation of transport layer security (TLS/SSL) for secure communication. Test for data at rest encryption in databases and storage systems, if applicable.
- **Authorization and Access Control:** Cytomate will test user roles and permissions to ensure users can only access appropriate resources. Verify that users cannot access unauthorized functionalities or data.
- **Input Validation and Injection:** Cytomate will test input fields for SQL injection, XSS (Cross-Site Scripting), and other injection attacks. Ensure proper input validation and output encoding to prevent injection vulnerabilities.
- *Authenticated Scanning:* Cytomate will perform authenticated scans to uncover vulnerabilities in session management. This can uncover vulnerabilities that might not be visible to unauthenticated users, such as session hijacking.
- **Multi-Factor Authentication (MFA) Testing:** Test MFA enforcement for applicable user roles and actions. Verify that MFA cannot be bypassed or easily disabled.
- **Conditional Access Testing:** Cytomate will test different access scenarios based on the conditional access policies defined. For example, Cytomate will test accessing resources from different devices, locations, or times of day. Cytomate will verify that conditional access policies are correctly applied and that users are blocked or granted access as expected.
- *Exploit Identified Vulnerabilities:* Cytomate will try to exploit the vulnerabilities identified during the authenticated scanning phase.
- *Report Preparation:* Cytomate will prepare a detailed report documenting the vulnerabilities identified, their potential impact, and recommended mitigations.
- *Presentation to the Stakeholders:* Cytomate will present the report to the stakeholders to help them understand the security posture of the application and what steps need to be taken to address the identified vulnerabilities.
- **Retest**: After remediation, Cytomate will conduct another round of testing to ensure that vulnerabilities have been effectively addressed.

Phase 2

Internal Vulnerability Assessment (Black Box-Grey Box)

1. Preparation and Planning
    - **Objective Definition:** Clearly define the scope and objectives of the assessment, including which systems, networks, and applications are in scope.
    - **Asset Inventory:** Compile a detailed inventory of all Windows and Linux servers within the scope.
    - **Permission and Access:** Obtain necessary permissions and access credentials to conduct the assessment without disrupting operations.
2. Environment Setup
    - **Tools Selection:** Choose appropriate vulnerability assessment tools compatible with both Windows and Linux environments (e.g., Nessus, OpenVAS, Qualys).
    - **Network Configuration:** Ensure network configuration allows the tools to communicate with the target servers. This may involve configuring firewall rules and network segmentation.
3. Information Gathering
    - **Network Mapping:** Use network discovery tools to map the network topology and identify active devices and open ports.
    - **Service Identification:** Identify running services on each server using tools like Nmap.
    - **OS and Software Enumeration:** Gather information about the operating systems, installed software, and their versions on each server.
4. Vulnerability Scanning
    - **Credentialed vs. Non-Credentialed Scans:** Decide on the use of credentialed (authenticated) or non-credentialed (unauthenticated) scans. Credentialed scans provide more comprehensive results.
    - **Configure Scans:** Configure the scanning tools with appropriate plugins and settings for both Windows and Linux systems.
    - **Execute Scans:** Run vulnerability scans during off-peak hours to minimize the impact on system performance.
    - **Scan Scheduling:** Schedule regular scans to maintain an up-to-date assessment of vulnerabilities.
5. Vulnerability Analysis
    - **Results Collection:** Collect and aggregate scan results from all tools used.
    - **False Positive Identification:** Validate findings to identify and eliminate false positives.
    - **Vulnerability Prioritization:** Prioritize vulnerabilities based on their severity, potential impact, and exploitability. Use Common Vulnerability Scoring System (CVSS) for standardization.
    - **Dependency Analysis:** Consider dependencies and the potential impact on interconnected systems.
6. Reporting
    - **Detailed Report Generation:** Generate a detailed report outlining identified vulnerabilities, their severity, potential impacts, and remediation recommendations.
    - Executive Summary: Create an executive summary for non-technical stakeholders highlighting key findings and overall security posture.
7. Remediation Guidance
    - **Patch Management:** Recommend patching and updating operating systems, software, and applications to mitigate identified vulnerabilities.
    - **Configuration Changes:** Suggest configuration changes to enhance security, such as disabling unnecessary services, closing open ports, and adjusting firewall rules.

- **Access Control:** Provide recommendations on improving access control mechanisms, including the principle of least privilege and multi-factor authentication.

Internal Application Testing (BlackBox-GreyBox)

GreyBox Testing:

- Cytomate may request QAPCO to provide architecture diagrams or credentials.
- The goal is to evaluate the authentication and authorization mechanisms more deeply.
- This approach allows for a comprehensive analysis by understanding the internal workings of the application while maintaining an external testing perspective.

BlackBox Testing:

- Conducted without any prior knowledge of the internal workings of the application.
- Simulates an external attack to identify vulnerabilities that an attacker might exploit without insider knowledge.

Testing Methodology

Common Vulnerabilities:

Broken Authentication:

- Evaluate the mechanisms in place for user authentication.
- Ensure that multi-factor authentication (MFA) is implemented where necessary.
- Test for vulnerabilities in password reset functionalities and session handling.

Improper Session Management:

- Assess the methods used for session creation, management, and termination.
- Ensure session tokens are securely generated and exchanged.
- Check for session expiration and invalidation mechanisms.

Data Transmission Security:

- Verify that all data transmitted between clients and servers is encrypted using TLS/SSL protocols.
- Ensure proper implementation of certificate pinning and validate the strength of the encryption algorithms used.

Single Sign-On (SSO) and Role-Based Access Controls (RBAC):

- Review the implementation of SSO to ensure that it is properly integrated and secure.
- Assess the configuration and enforcement of RBAC to ensure users have appropriate permissions based on their roles.
- Verify that least privilege principles are applied and that roles are clearly defined and managed.

Network Scans

Open Ports and Services:

- Conduct network scans to identify all open ports and services running on the servers.
- Evaluate the security configurations of these services to identify potential vulnerabilities.
- Ensure that unnecessary services are disabled or properly secured.
- Vulnerability Identification:
- Utilize automated tools and manual techniques to identify vulnerabilities associated with the identified services.
- Prioritize findings based on their potential impact and ease of exploitation.

OWASP Top 10 Vulnerability Assessment

Cytomate will specifically focus on identifying and mitigating vulnerabilities listed in the OWASP Top 10, including but not limited to:

Injection:

- Test for SQL, NoSQL, OS, and LDAP injection vulnerabilities.
- Ensure proper use of parameterized queries and input validation.

Broken Authentication and Session Management:

- As previously detailed, evaluate the robustness of authentication and session management mechanisms.

Insecure Direct Object References (IDOR):

- Check for improper access controls that allow unauthorized access to sensitive data.

Cross-Site Scripting (XSS):

- Identify and mitigate reflected, stored, and DOM-based XSS vulnerabilities.
- Ensure proper input sanitization and output encoding.

Sensitive Data Exposure:

- Verify that sensitive data is properly encrypted both at rest and in transit.
- Assess the implementation of data protection mechanisms for personally identifiable information (PII) and other sensitive data.

Cross-Site Request Forgery (CSRF):

- Test for CSRF vulnerabilities and ensure that proper anti-CSRF tokens are implemented and validated.

TLS Security:

- Confirm the proper configuration and use of TLS to secure data transmission.
- Evaluate the strength of the encryption protocols and ciphers in use.

Other Unknown Attack Vectors:

- Continuously assess for emerging threats and unknown vulnerabilities using the latest threat intelligence and security research.

Reporting and Remediation

- Cytomate will provide a detailed report outlining all identified vulnerabilities, their potential impact, and recommended remediation steps.
- The report will prioritize vulnerabilities based on their severity and potential business impact.
- Cytomate will work closely with QAPCO to ensure that remediation efforts are effectively implemented and validated through follow-up testing.

Wireless Penetration Testing

- **Wireless Testing:** Cytomate will evaluate Wi-Fi security using tools like Aircrack-ng for WEP/WPA2/WPA3 cracking.
- **Wireless Attack Surface**: Cytomate will identify potential attack vectors, such as weak passwords, misconfigured APs, exposed management interfaces, and vulnerable client devices.
- **Rogue AP Detection**: Cytomate will try to find any unauthorized access points that are rogue and can try to steal information from clients.
- **Packet Sniffing:** Capture and analyze network traffic with Wireshark to identify sensitive data exposure.
- **ARP Spoofing:** Use tools like Ettercap and bettercap for ARP spoofing attacks to intercept network traffic.

- **Default Credential:** To check for default credential of network devices, Brute force attack to crack the password, DDoS attack to validate the network level security controls, and phishing attacks.
- **Reporting and Documentation:** Cytomate will compile comprehensive findings and impact assessment, detailing vulnerabilities, exploitation paths, and potential impact on patient data.
- **Remediation Recommendations:** Cytomate will provide actionable recommendations to remediate vulnerabilities and enhance security, including specific steps for securing internal networks and applications.
- **Collaboration and Debriefing:** Cytomate will collaborate with the organization's teams to discuss findings, impacts, and recommended remediation strategies.
- **Retest**: After remediation, Cytomate will conduct another round of testing to ensure that vulnerabilities have been effectively addressed.

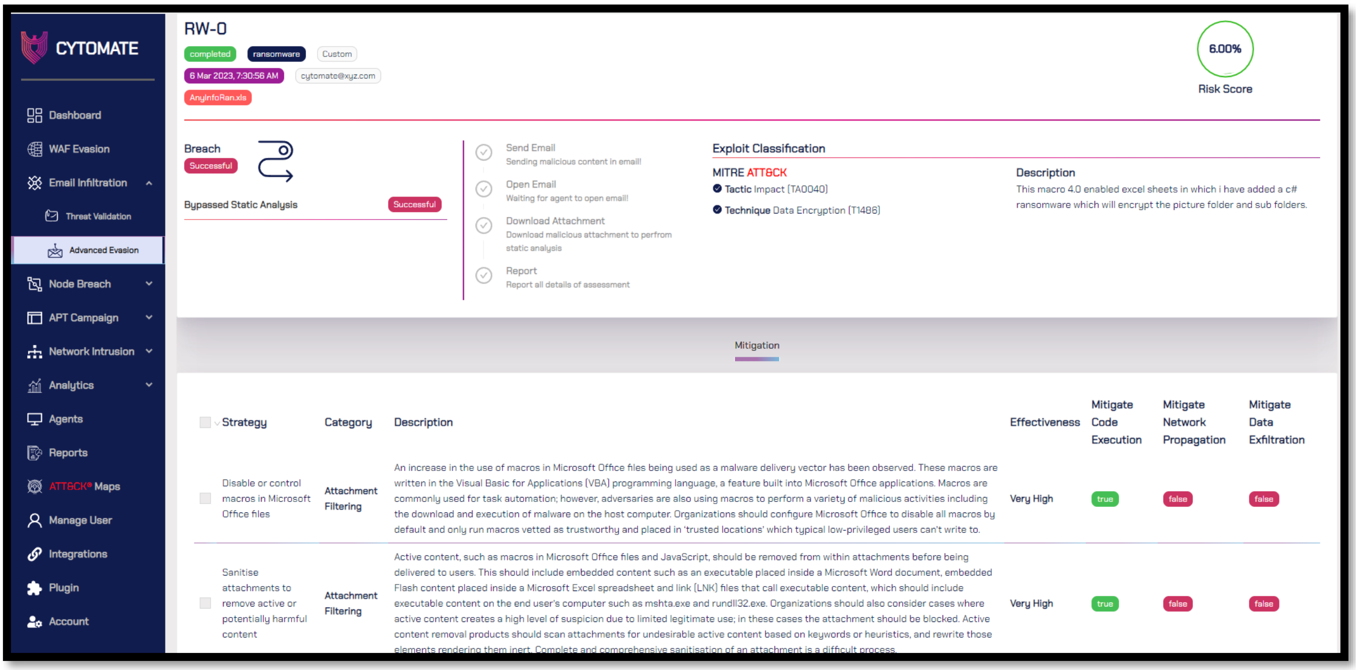
Phase 3

Email Gateway Security Controls Validation

Breach+ utilizes a sophisticated email gateway validation process by sending live APT threats files and phishing links, augmented with LLM (Large Language Model) technology to assess email security robustness. Breach+ conducts comprehensive evaluations on various security vendors, including Cisco and Microsoft. However, these solutions often prove inadequate due to outdated threat intelligence. Remarkably, Breach+'s advanced AI-based testing consistently outperforms these conventional security measures, highlighting its unparalleled success in bypassing them.

- **Threat Intelligence Validation:** Breach+ initiates its security protocol by leveraging threat intelligence to identify and understand the latest email threats, ensuring that the gateway's defenses are always aligned with current threat landscapes.
- **Simulation of Malicious Activities:** Utilizing AI-based models, Breach+ generates sophisticated and realistic simulations of malicious attachments, APT threats, and phishing links. This step tests the resilience of the email gateway against a wide array of email-based threats.
- **Malicious Attachments development:** Cytomate create custom malicious attachment and use public attachments used by APT groups in Initial access and send those attachments to organization email to validate the security and misconfiguration of email server.
- **Simulation execution:** The simulations are then executed against the email gateway to evaluate the effectiveness of the email security controls in detecting and preventing the simulated attacks.
- **Results analysis:** The results of the simulations are analyzed to identify any gaps or weaknesses in the organization's email security controls. This analysis includes identifying the TTPs that were successful in bypassing the security controls and understanding the reasons for the success.
- **Organization-Specific Policy Mitigations:** In parallel to threat simulation, Breach+ crafts tailored policy-based mitigations. These policies are designed to align with the specific needs and security posture of the organization, providing a proactive layer of defense against potential email attacks.

- **Retest**: After remediation, Cytomate will conduct another round of testing to ensure that identified issues have been effectively addressed.



RW-0

completed | ransomware | Custom

6 Mar 2023, 7:30:56 AM | cytomate@xyz.com

AnyInfoRan.xls

6.00%
Risk Score

Breach Successful

Bypassed Static Analysis Successful

Send Email
Sending malicious content in email!

Open Email
Waiting for agent to open email!

Download Attachment
Download malicious attachment to perfrom static analysis

Report
Report all details of assessment

Exploit Classification

MITRE ATT&CK
- **Tactic** Impact (TA0040)
- **Technique** Data Encryption (T1486)

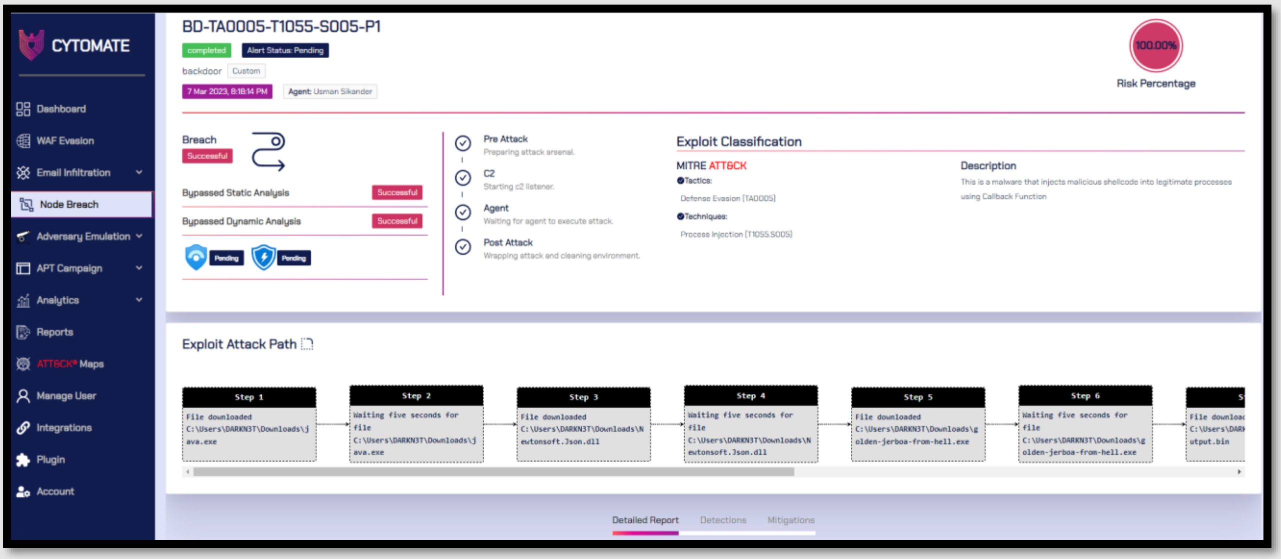
Description
This macro 4.0 enabled excel sheets in which i have added a c# ransomware which will encrypt the picture folder and sub folders.

Strategy	Category	Description	Effectiveness	Mitigate Code Execution	Mitigate Network Propagation	Mitigate Data Exfiltration
Disable or control macros in Microsoft Office files	Attachment Filtering	An increase in the use of macros in Microsoft Office files being used as a malware delivery vector has been observed. These macros are written in the Visual Basic for Applications (VBA) programming language, a feature built into Microsoft Office applications. Macros are commonly used for task automation; however, adversaries are also using macros to perform a variety of malicious activities including the download and execution of malware on the host computer. Organizations should configure Microsoft Office to disable all macros by default and only run macros vetted as trustworthy and placed in 'trusted locations' which typical low-privileged users can't write to.	Very High	true	false	false
Sanitise attachments to remove active or potentially harmful content	Attachment Filtering	Active content, such as macros in Microsoft Office files and JavaScript, should be removed from within attachments before being delivered to users. This should include embedded content such as an executable placed inside a Microsoft Word document, embedded Flash content placed inside a Microsoft Excel spreadsheet and link (LNK) files that call executable content, which should include executable content on the end user's computer such as mshta.exe and rundll32.exe. Organizations should also consider cases where active content creates a high level of suspicion due to limited legitimate use; in these cases the attachment should be blocked. Active content removal products should scan attachments for undesirable active content based on keywords or heuristics, and rewrite those elements rendering them inert. Complete and comprehensive sanitisation of an attachment is a difficult process.	Very High	true	false	false

Endpoint Security Controls Validation

Cytomate breach and attack simulation platform (Breach+) performs real emulation to check the endpoint as well as network level security controls by making command and control session using C2 and C3 (Custom command and control). Cytomate executes ransomware and emulates all behavior of ransomware in the presence of security controls to validate the security posture of the organization. Cytomate utilizes attack scenario language (ASL) and polymorphic approach to validate the security posture of organization.

- **Asset inventory:** The first step is to identify all the endpoints within the organization's network and install Breach+ agent on Windows, Linux or MacOS.
- **Simulation development:** Attacks are developed to emulate real-world attacks against the organization's endpoints. The simulations involve different TTPs, such as malware execution, lateral movement, privilege escalation, and data exfiltration.
- **Simulation execution:** The simulations are then executed against the endpoints to evaluate the effectiveness of the endpoint security controls in detecting and preventing the simulated attacks.
- **Results analysis:** The results of the simulations are analyzed to identify any gaps or weaknesses in the organization's endpoint security controls. This analysis includes identifying the TTPs that were successful in bypassing the security controls and understanding the reasons for the success.
- **Remediation planning:** Based on the analysis, a remediation plan is created that outlines the steps needed to address the identified gaps or weaknesses in the endpoint security controls.



BD-TA0005-T1055-S005-P1

completed | Alert Status: Pending

backdoor | Custom

7 Mar 2023, 8:18:14 PM | Agent: Usman Sikander

Breach: Successful

Bypassed Static Analysis: Successful

Bypassed Dynamic Analysis: Successful

Pre Attack
Preparing attack arsenal.

C2
Starting c2 listener.

Agent
Waiting for agent to execute attack.

Post Attack
Wrapping attack and cleaning environment.

Exploit Classification

MITRE ATT&CK

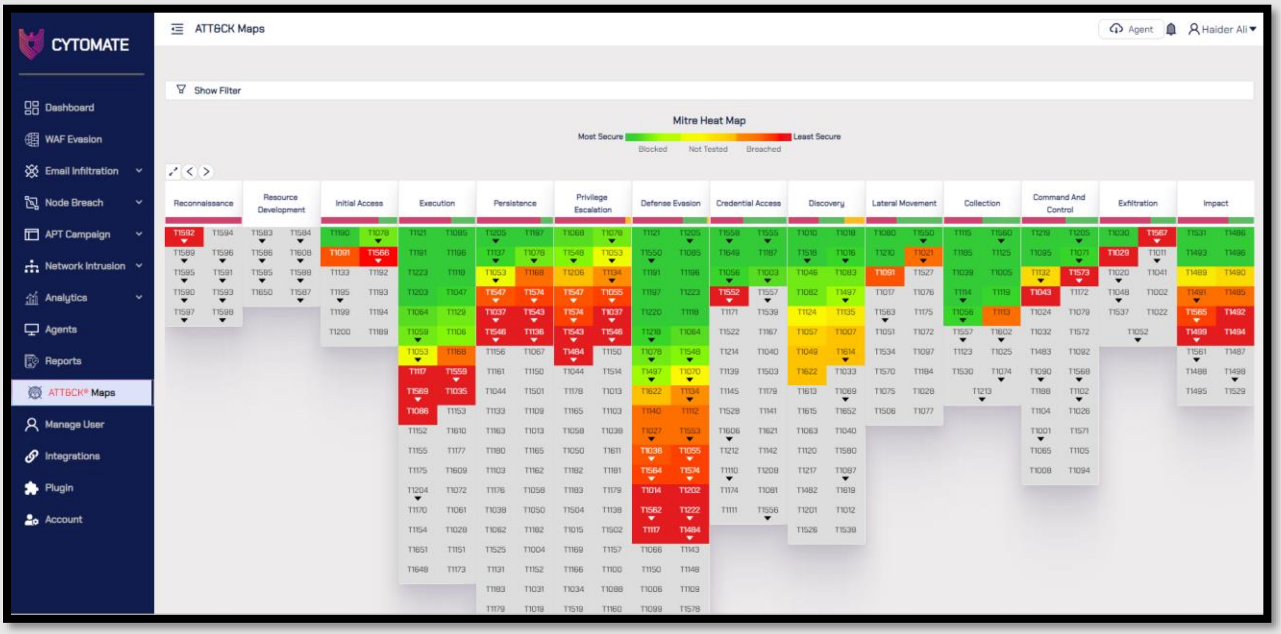
Tactics:
Defense Evasion (TA0005)

Techniques:
Process Injection (T1055.S005)

Description
This is a malware that injects malicious shellcode into legitimate processes using Callback Function

Exploit Attack Path

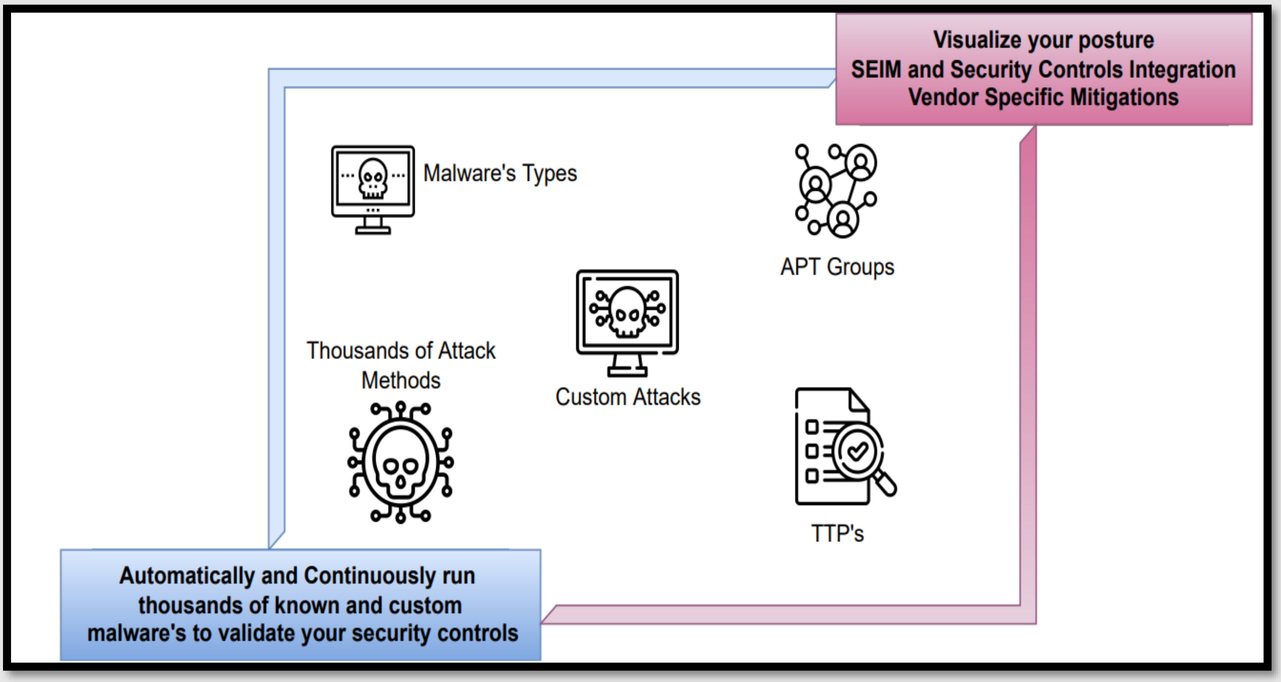
```
Step 1
File downloaded
C:\Users\DARKN3T\Downloads\java.exe

Step 2
Waiting five seconds for
file
C:\Users\DARKN3T\Downloads\java.exe

Step 3
File downloaded
C:\Users\DARKN3T\Downloads\Newtonsoft.Json.dll

Step 4
Waiting five seconds for
file
C:\Users\DARKN3T\Downloads\Newtonsoft.Json.dll

Step 5
File downloaded
C:\Users\DARKN3T\Downloads\golden-jerboa-from-hell.exe

Step 6
Waiting five seconds for
file
C:\Users\DARKN3T\Downloads\golden-jerboa-from-hell.exe

S
File downloa
C:\Users\DARK
utput.bin
```



ATT&CK Maps

Mitre Heat Map

Reconnaissance		Resource Development		Initial Access		Execution		Persistence		Privilege Escalation		Defense Evasion		Credential Access		Discovery		Lateral Movement		Collection		Command And Control		Exfiltration		Impact	
T1592	T1594	T1583	T1584	T1190	T1078	T1121	T1085	T1205	T1197	T1068	T1078	T1121	T1205	T1558	T1555	T1010	T1018	T1080	T1550	T1115	T1560	T1219	T1205	T1030	T1567	T1531	T1486
T1589	T1596	T1586	T1608	T1091	T1566	T1181	T1196	T1137	T1078	T1548	T1053	T1550	T1085	T1649	T1187	T1518	T1016	T1210	T1021	T1185	T1125	T1095	T1071	T1029	T1011	T1493	T1496
T1595	T1591	T1585	T1588	T1133	T1192	T1223	T1118	T1053	T1168	T1206	T1134	T1191	T1196	T1056	T1003	T1046	T1083	T1091	T1527	T1039	T1005	T1132	T1573	T1020	T1041	T1489	T1490
T1590	T1593	T1650	T1587	T1195	T1193	T1203	T1047	T1547	T1574	T1547	T1055	T1197	T1223	T1552	T1557	T1082	T1497	T1017	T1076	T1114	T1119	T1043	T1172	T1048	T1002	T1491	T1485
T1597	T1598			T1199	T1194	T1064	T1129	T1037	T1543	T1574	T1037	T1220	T1118	T1171	T1539	T1124	T1135	T1563	T1175	T1056	T1113	T1024	T1079	T1537	T1022	T1565	T1492
				T1200	T1189	T1059	T1106	T1546	T1138	T1543	T1546	T1218	T1064	T1522	T1167	T1057	T1007	T1051	T1072	T1557	T1602	T1032	T1572	T1052		T1499	T1494
						T1053	T1168	T1156	T1067	T1484	T1150	T1078	T1548	T1214	T1040	T1049	T1614	T1534	T1097	T1123	T1025	T1483	T1092			T1561	T1487
						T1117	T1559	T1161	T1150	T1044	T1514	T1497	T1070	T1139	T1503	T1622	T1033	T1570	T1184	T1530	T1074	T1090	T1568			T1488	T1498
						T1569	T1035	T1044	T1501	T1178	T1013	T1622	T1134	T1145	T1179	T1613	T1069	T1075	T1028	T1213		T1188	T1102			T1495	T1529
						T1086	T1153	T1133	T1109	T1165	T1103	T1140	T1112	T1528	T1141	T1615	T1652	T1506	T1077			T1104	T1026				
						T1152	T1610	T1163	T1013	T1058	T1038	T1027	T1553	T1606	T1621	T1063	T1040					T1001	T1571				
						T1155	T1177	T1180	T1165	T1050	T1611	T1036	T1055	T1212	T1142	T1120	T1580					T1065	T1105				
						T1175	T1609	T1103	T1162	T1182	T1181	T1564	T1574	T1110	T1208	T1217	T1087					T1008	T1094				
						T1204	T1072	T1176	T1058	T1183	T1179	T1014	T1202	T1174	T1081	T1482	T1619										
						T1170	T1061	T1038	T1050	T1504	T1138	T1562	T1222	T1111	T1556	T1201	T1012										
						T1154	T1028	T1062	T1182	T1015	T1502	T1117	T1484			T1526	T1538										
						T1651	T1151	T1525	T1004	T1169	T1157	T1066	T1143														
						T1648	T1173	T1131	T1152	T1166	T1100	T1150	T1148														
								T1183	T1031	T1034	T1088	T1006	T1109														
								T1179	T1019	T1519	T1160	T1099	T1578														



Visualize your posture
SEIM and Security Controls Integration
Vendor Specific Mitigations

Malware's Types

APT Groups

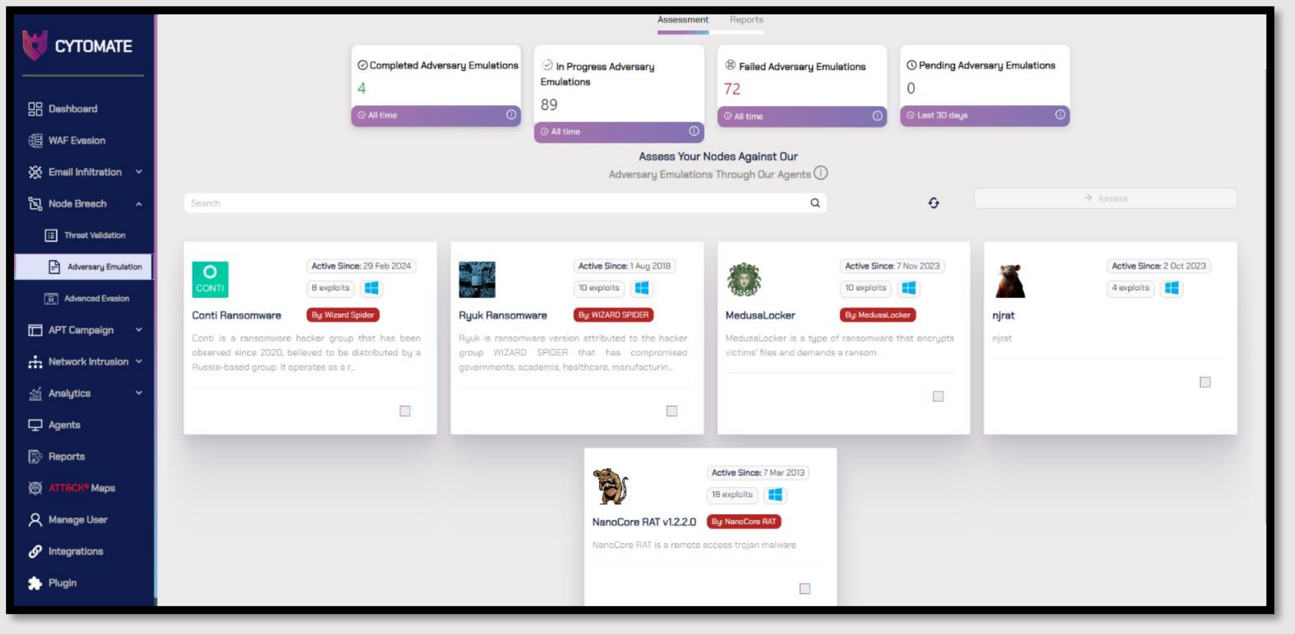
Custom Attacks

Thousands of Attack Methods

TTP's

Automatically and Continuously run thousands of known and custom malware's to validate your security controls

Cytomate Breach+ validates security posture against emerging threats by emulating the whole behavior of real-world APT campaign in sequence of test cases. In this feature, Cytomate is focused on Behavior code mirroring (BCM) approach. Cytomate reverse engineered the malware extract the TTP's and re-create same APT with sequence of exploits. Cytomate R&D team re-create extracted TTPs in the same manner with behavior code mirroring techniques and emulate all created TTPs in a sequence to provide TTP based insight about real world malware.



Completed Adversary Emulations 4 All time

In Progress Adversary Emulations 89 All time

Failed Adversary Emulations 72 All time

Pending Adversary Emulations 0 Last 30 days

Assess Your Nodes Against Our Adversary Emulations Through Our Agents

Conti Ransomware — Active Since: 29 Feb 2024 — 8 exploits — By: Wizard Spider
Conti is a ransomware hacker group that has been observed since 2020, believed to be distributed by a Russia-based group. It operates as a r...

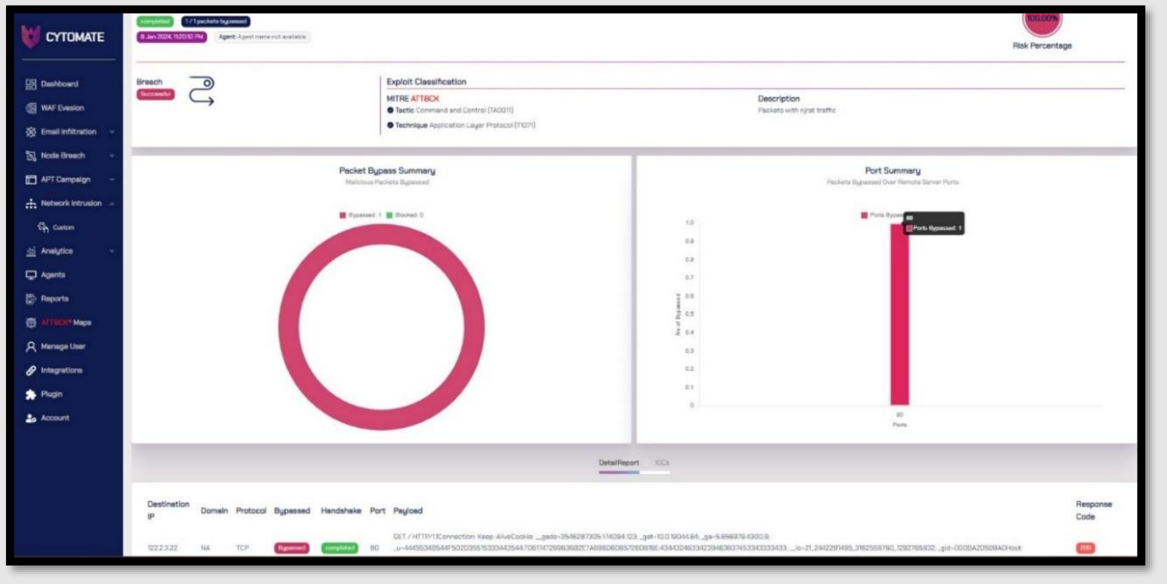
Ryuk Ransomware — Active Since: 1 Aug 2018 — 10 exploits — By: WIZARD SPIDER
Ryuk is ransomware version attributed to the hacker group WIZARD SPIDER that has compromised governments, academia, healthcare, manufacturin...

MedusaLocker — Active Since: 7 Nov 2023 — 10 exploits — By: MedusaLocker
MedusaLocker is a type of ransomware that encrypts victims' files and demands a ransom.

njrat — Active Since: 2 Oct 2023 — 4 exploits
njrat

NanoCore RAT v1.2.2.0 — Active Since: 7 Mar 2013 — 18 exploits — By: NanoCore RAT
NanoCore RAT is a remote access trojan malware

Breach+ performs attack path validation by emulating active directory exploits. This module covers attack paths that can be exploited by attackers to achieve their objective such as domain admin credential, domain persistence and data exfiltration. Breach+ executes advanced custom exploits to check misconfiguration, group policies and all active directory attacks. Breach+ provides detailed mitigations and system hardening based policies to stop active directory attacks.



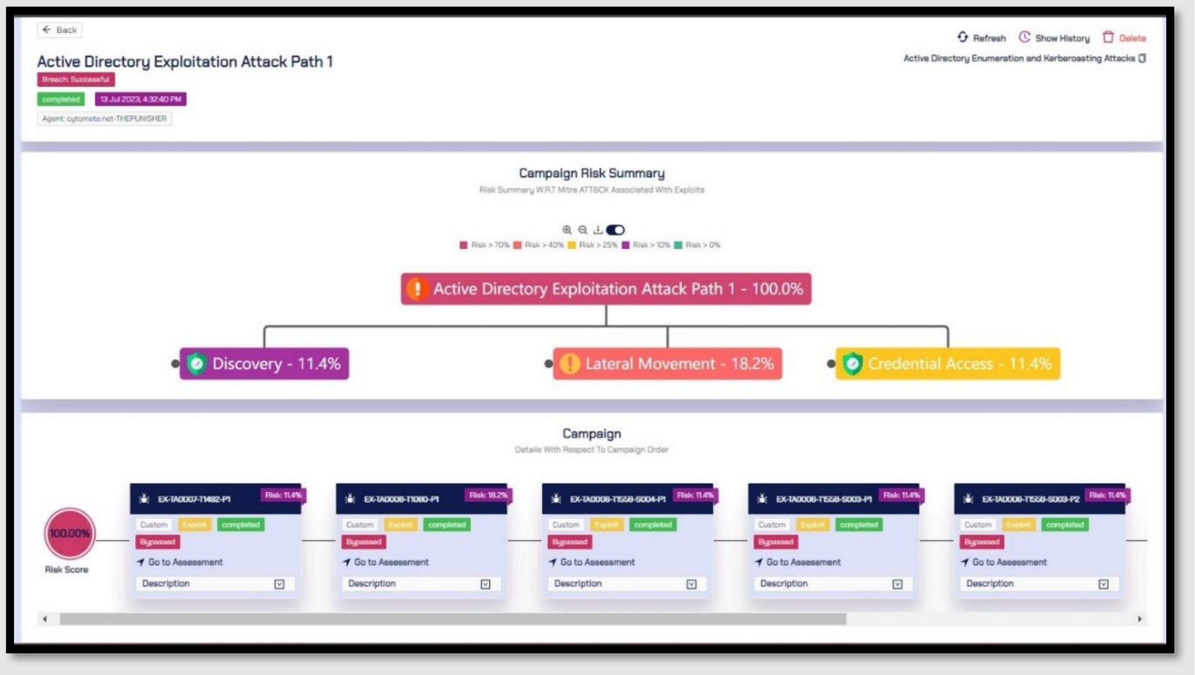
Agent: Agent name not available

Breach Successful

Exploit Classification
MITRE ATT&CK
- Tactic Command and Control (TA0011)
- Technique Application Layer Protocol (T1071)

Description
Packets with njrat traffic

Destination IP	Domain	Protocol	Bypassed	Handshake	Port	Payload	Response Code
122.2.3.22	NA	TCP	Bypassed	completed	80	GET / HTTP/1.1Connection: Keep-AliveCookie: __gads=3546287305.114094123; _gat=10.0.19044.64; _gs=5.656979.43009; __u=44455340544F502035515333443544706174728963682E7A696060657260616E4344324633423946363745334333433; __io=21_2442291495_3162559780_1292765932; _gid=0000A20509A0Host	200



Active Directory Exploitation Attack Path 1

Breach: Successful

completed 13 Jul 2023, 4:32:40 PM

Agent: cytomate.net-THEPUNISHER

Active Directory Enumeration and Kerberoasting Attacks

Campaign Risk Summary

Risk Summary W.R.T Mitre ATT&CK Associated With Exploits

Active Directory Exploitation Attack Path 1 - 100.0%

Discovery - 11.4%

Lateral Movement - 18.2%

Credential Access - 11.4%

Campaign

Details With Respect To Campaign Order

Risk Score 100.00%

EX-TA0007-T1482-P1	Risk: 11.4%	completed Bypassed
EX-TA0008-T1080-P1	Risk: 18.2%	completed Bypassed
EX-TA0006-T1558-S004-P1	Risk: 11.4%	completed Bypassed
EX-TA0006-T1558-S003-P1	Risk: 11.4%	completed Bypassed
EX-TA0006-T1558-S003-P2	Risk: 11.4%	completed Bypassed

Network Security Controls Validation

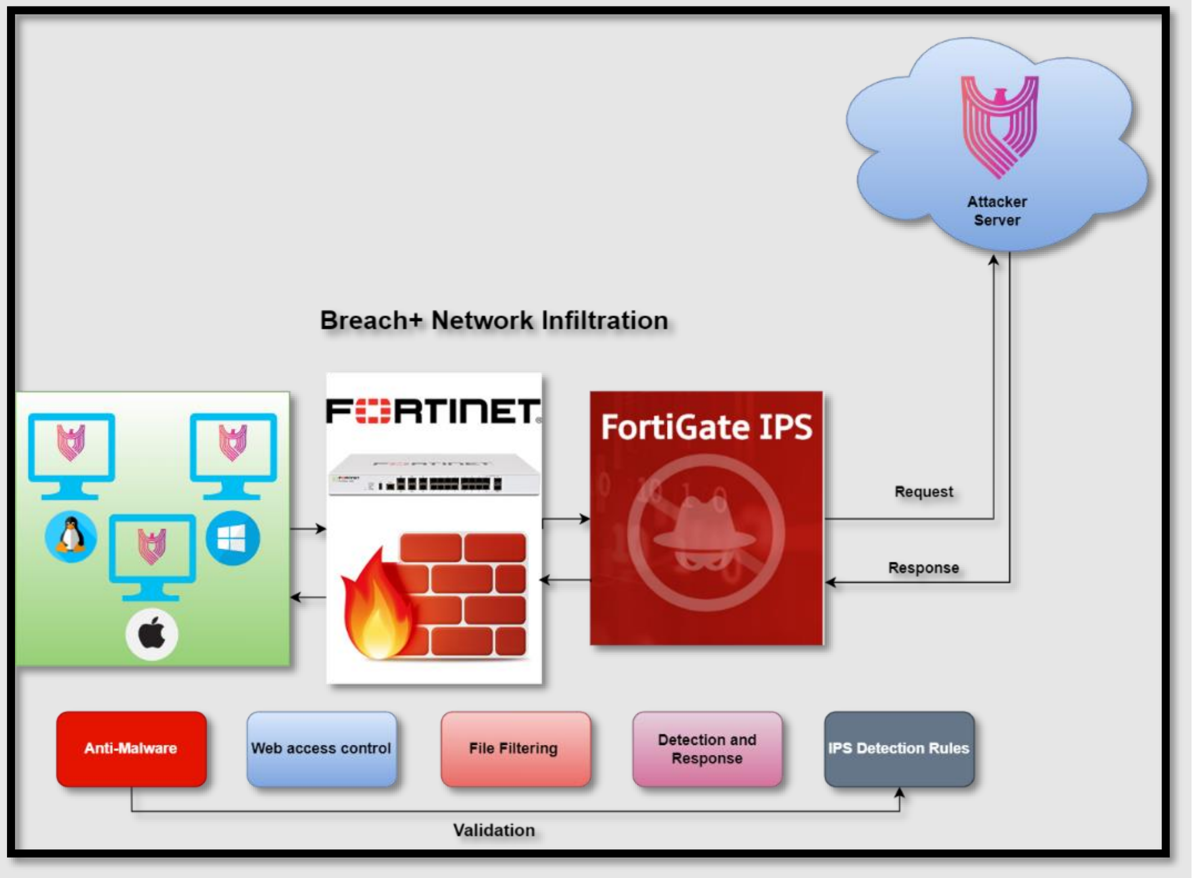
Cytomate's Breach+ Network Infiltration module is a sophisticated tool designed for enhancing cybersecurity measures, particularly focusing on the efficiency and effectiveness of network-deployed security controls. This module is tailored for organizations that have invested in next-generation firewalls (NGFWs) and other similar advanced security technologies. Here is a detailed explanation of its features and functionalities:

- **Performance Evaluation of Security Controls:** The primary function of this module is to assess the performance of security controls that have been deployed within a network. This is crucial for organizations to ensure that their investments in security technologies like NGFWs, IPS/IDS are yielding the desired protective outcomes.

- **Use of Packet Capture (PCAP) Replay:** A key feature of this module is its ability to replay traffic using PCAP. PCAP is a data packet capture format that records network traffic. The module replays this recorded traffic between a target and attacking assets.
- **Real-World Malware Traffic Simulation:** The traffic replayed is not just any traffic; it includes real-world malware traffic. This means the module simulates actual malicious traffic patterns and behaviors seen in real cyberattack scenarios. This provides a more realistic and challenging test environment for the network's security controls.
- **Comprehensive Testing of Inline Security:** By replaying whole PCAPs, the module thoroughly checks the inline security measures. 'Inline security' refers to security controls that are placed directly in the path of network traffic, actively analyzing, and making decisions about the traffic in real-time. This comprehensive testing is crucial for identifying any weaknesses or gaps in the security setup.
- **Detection and Prevention Analysis:** The module not only tests whether the in-line security controls can detect an attack but also if they can prevent it. This dual capability is essential for a robust security posture, as detection without prevention may not be sufficient to thwart sophisticated cyber threats.
- **Mitigation Recommendations and Prescriptive Guidance:** Post analysis, the module provides

clear mitigation recommendation options. This includes prescriptive guidance on how to improve the security posture. Such recommendations are crucial for organizations to understand the necessary steps needed to enhance their defenses against identified vulnerabilities.

- **Provision of IoCs and Vendor-Specific Mitigations:** Cytomate also provides Indicators of Compromise (IoCs) and vendor-specific mitigation **strategies and signatures**.



Security Configuration Review

1. Scope Definition:

Cytomate will define the scope of devices and systems to be reviewed, including routers, switches, endpoint devices, access points, and IDS/IPS systems OS Images, Firewalls rules and configurations, networks.

- **Access Control and Password Policies:** Cytomate will review and document existing access control lists (ACLs) on routers and switches, ensuring they follow the principle of least privilege.
- Cytomate will evaluate password policies on network devices, ensuring strong password requirements and regular password changes.
- **Endpoint Security Controls:** Cytomate will assess endpoint security settings, including firewall configurations, antivirus/antimalware presence, and host-based intrusion detection systems (HIDS).
- Cytomate will validate proper configuration of endpoint security solutions, such as malware detection, behavioral analysis, and application whitelisting.
- **IDS/IPS Detection Rules:** Cytomate will examine IDS/IPS detection rules for accuracy and relevance, ensuring they cover known attack vectors and vulnerabilities.
- **Firewall Rules:** Verify that firewall rules are up-to-date and aligned with the organization's needs.
- **OS Images:** Cytomate team will verify the Sidra Medicine using updated operating

systems and all systems are updated and patched.

- **Network Segmentation:** Cytomate team will verify that networks are segmented, and traffic is being forwarded within the allowed subnets. Cytomate will also test the isolated network segment and verify that these segments are not accessible from any unknown or unauthorized segment.

Automated Breach and Attack Simulation (Breach+):

- **Access Control and Password Policies**: Cytomate will utilize BAS tools to simulate attacks against ACLs and access controls, identifying potential misconfigurations or access leakage.
- Cytomate will test password policies by simulating brute-force attacks to assess their effectiveness.
- **Endpoint Security Controls**: Cytomate will run BAS scenarios to assess endpoint security controls, evaluating their ability to detect and prevent simulated attack attempts.
- Cytomate will test the response of host-based intrusion detection systems (HIDS) to various attack techniques.
- **IDS/IPS Detection Rules**: Cytomate will employ BAS tools to simulate attacks that should trigger IDS/IPS detection rules, validating their accuracy and responsiveness.
- Cytomate will identify false positives or false negatives in IDS/IPS detection rules.

Configuration Review

Active Directory Security Hygiene Review

Scope: Cytomate will review and assess the security of the Active Directory (AD) environment. It will focus on identifying potential vulnerabilities, ensuring adherence to best practices, and verifying the effectiveness of security controls.

Methodology

- **Access Control Review:** Evaluate user, group, and admin account permissions to ensure least privilege principles are followed.
- **Password Policies:** Assess the complexity and expiration policies to ensure they meet security standards.
- **Audit Policies:** Review logging and monitoring settings for AD-related events.
- **GPO Analysis:** Evaluate Group Policy Objects (GPOs) to ensure security settings are correctly configured and applied.
- **Patch Management:** Check the update status of AD servers to confirm they are up-to-date with security patches.

Security Tools Configuration Review

Scope

Cytomate will review to evaluate the security configuration of tools used within the organization. The focus will be on ensuring that these tools are optimally configured to protect against threats and comply with organizational security policies.

Methodology

- **Tool Inventory:** Identify and list all security tools currently deployed within the organization.
- **Configuration Assessment:** Review the settings and configurations of each tool to ensure they align with industry best practices.
- **Integration Checks:** Verify the integration of security tools with other systems, ensuring data flow and alerting mechanisms are properly configured.
- **Policy Alignment:** Ensure that the configuration of each tool supports the organization's security policies and objectives.
- **Performance Testing: Conduct tests to confirm that the tools are functioning as expected and can detect and mitigate threats.**

VPN Security Configuration Review

Scope

Cytomate will focus on evaluating the security configuration of the organization's VPN (Virtual Private Network) infrastructure. The goal is to ensure that remote access is secure, and that the VPN setup minimizes exposure to potential threats.

Methodology

- **Access Controls:** Review who has access to the VPN and ensure that access is granted based on role and necessity.
- **Authentication Methods:** Evaluate the strength and configuration of authentication mechanisms (e.g., multi-factor authentication, certificates).
- **Encryption Protocols:** Assess the encryption protocols in use to ensure data transmitted over the VPN is secure.
- **Logging and Monitoring:** Review logging configurations for VPN access and activities to ensure adequate monitoring and incident detection.
- **Patch and Update Status:** Verify that the VPN software and hardware are up-to-date with the latest security patches and updates.
- **Penetration Testing:** Conduct penetration testing to identify potential vulnerabilities within the VPN configuration.
- **Security Architecture Review:** Conduct security architecture review to identify weaknesses in VPN protocol.
- **Review Segregation of Network Zones:** Analyze the network architecture to ensure proper isolation between zones and adherence to security policies.
- **Review Identity and Network Access Controls:** Assess the implementation and effectiveness of identity management and access controls across the network.
- **Review Remote Access IT/OT Networks:** Evaluate the security measures and controls for remote access to IT and OT networks, ensuring secure and monitored connectivity.
- **Complete IT Network & IT/OT Interface:** Conduct a comprehensive review of the entire VPN network and its interface with OT systems to identify potential security gaps and integration risks.

Social Engineering

Gather Scoping Information: Identify the scope and collect the Publicly available information about victim.

- Identify and collect the information includes the targets (names, emails, phone numbers, departments, physical locations)
- Specify the type of information or systems that can be targeted.

Reconnaissance: Gather as much information as possible about the target.

- Passive Information Gathering:
- Public records and databases.
- Social media platforms.
- Open-source intelligence tools.
- Websites, blogs, and forums related to the target.
- Active Information Gathering:

- Sending non-malicious emails to gauge Responsiveness Calling the organization to collect information.

Threat Modelling: Understand the potential threats to the target.

- Identify potential threat actors and their motivations.
- Who might want to target the organization and why?
- What methods might they employ?
- What would be their desired outcome (e.g., data theft, financial gain, reputation damage)?

Vulnerability Analysis: Discover and identify weak points in the organization's human layer.

- Employees do not verify identities before giving out sensitive info.
- Susceptibility to phishing attempts.
- Weak policies regarding visitor access to physical locations (on-site).

Exploitation: Exploit the identified vulnerabilities and weak points to determine their real-world impact.

- Conducting phishing campaigns.
- Calling employees to extract sensitive information (pretexting).
- Trying to gain physical access to the premises (on-site).

Presentation and Reporting: Document the findings in a structured and understandable format.

- Successful and unsuccessful exploitation attempts.
- Methodology used.
- Vulnerabilities found.
- Recommendations for remediation.
- Highlight critical vulnerabilities.
- Awareness campaigns for phished users.
- Explain potential consequences.
- Advocate for resources or changes to address identified issues.

Compromise Assessment - Network Forensic Analysis

Scope

The purpose of this compromise assessment is to conduct a detailed forensic analysis of the network to identify any indicators of compromise (IOCs). The assessment focuses on detecting suspicious network activities, identifying lateral movement, discovering potential data exfiltration, and locating rogue devices on the network.

Methodology

- **Suspicious Network Activity Identification:**
  - **Traffic Analysis:** Monitor and analyze network traffic patterns to detect anomalies, such as unusual spikes in traffic, unexpected protocols, or communication with known malicious IP addresses.
  - **Log Review:** Examine firewall, router, and IDS/IPS logs for signs of unauthorized access, unusual connections, or failed login attempts.
  - **Protocol Analysis:** Use deep packet inspection (DPI) to scrutinize the content of network communications, identifying any suspicious or malicious payloads.
- **Lateral Movement Detection:**
  - **User Behavior Analysis:** Track user account activities to identify unusual patterns, such as logins from unexpected locations or times, which may indicate lateral movement within the network.
  - **Endpoint Communication Mapping:** Map out the communication paths between endpoints to identify unauthorized or unexpected connections between internal systems.

  - **Privilege Escalation Monitoring:** Look for signs of privilege escalation attempts, such as changes to user roles or the creation of new admin accounts.
- Data Exfiltration Identification:
  - **Outbound Traffic Monitoring:** Monitor for large or unexpected data transfers, especially to external IP addresses, which could indicate data exfiltration.
  - **Data Flow Analysis:** Trace the flow of sensitive data within the network to ensure it is not being routed to unauthorized destinations.
  - **DLP Integration:** Utilize Data Loss Prevention (DLP) tools to detect and block attempts to transfer sensitive data out of the network.
- Rogue Devices Identification:
  - **Network Scanning:** Perform active and passive scans of the network to identify any unauthorized devices connected to the network.
  - **MAC Address Filtering:** Check for devices with suspicious or unknown MAC addresses that do not match the organization's inventory.
  - **Wireless Network Monitoring:** Monitor wireless networks for unauthorized access points or devices attempting to connect to the network.

Compromise Assessment - Host Forensic Analysis

Scope

This compromise assessment's objective is to perform an in-depth forensic analysis of 1,500 endpoints covered by Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) systems. The focus will be on reviewing security logs and analyzing both ongoing and historical compromises. This assessment will help in identifying any indicators of compromise (IOCs), understanding the extent of any potential breaches, and ensuring that the endpoints are secure.

Methodology

- Security Log Review:
  - **Correlation and Analysis:** Use Security Information and Event Management (SIEM) tools to correlate logs from different sources, identifying suspicious patterns or activities.
  - **Event Focus:** Examine critical security events such as unauthorized access attempts, abnormal process execution, file modifications, and privilege escalation incidents.
- Ongoing and Past Compromise Analysis:
  - **Retrospective Analysis:** Analyze historical data captured by EDR and NDR systems to identify any previous compromises, focusing on indicators like file hashes, IP addresses, and domain names associated with known threats.
  - **Memory and Disk Forensics:** Perform memory and disk analysis on select endpoints to uncover hidden or persistent threats that might have evaded initial detection.
  - **Malware Analysis:** Utilize sandboxing and behavioral analysis to detect advanced or zero-day malware.
- Endpoint Coverage Verification:
  - **Coverage Check:** Ensure that all 1,500 endpoints are monitored by EDR and NDR solutions, verifying the active status and functionality of security agents.
  - **Proactive Threat Hunting:** Conduct threat hunting activities across all endpoints using IOCs and threat intelligence to identify potential compromises.
  - **Remediation Actions:** Confirm that any identified threats have been properly remediated, including isolating affected systems, and removing malware.

Tools

- **Forensic Tools:** EnCase, FTK (Forensic Toolkit), or Volatility, utilized for in-depth analysis of memory, disk images, and other forensic data.
- **Threat Intelligence Platforms:** Recorded Future, ThreatConnect, or MISP, used for gathering and analyzing threat intelligence and IOCs.
- **Sandboxing Tools:** Cuckoo Sandbox, FireEye Malware Analysis, or Hybrid Analysis, used to safely execute and analyze the behavior of suspicious files.

Source Code Review

Scope

The objective of this source code review is to identify and mitigate security vulnerabilities within the application codebase through Static Application Security Testing (SAST) and manual code analysis. The assessment will focus on exposing security flaws, such as coding errors, insecure practices, and potential vulnerabilities that could be exploited by attackers.

Methodology

- Static Application Security Testing (SAST):
  - **Automated Scanning:** Utilize SAST tools to automatically scan the codebase for common security vulnerabilities, including SQL injection, cross-site scripting (XSS), buffer overflows, and insecure coding practices.
  - **Rule Set Customization:** Customize the scanning rules to align with the specific coding standards and security requirements of the application.
  - **Report Analysis:** Analyze the SAST reports to identify false positives, prioritize findings based on risk level, and categorize vulnerabilities by type.
- Perform Code Analysis:
  - **Manual Code Review:** Conduct a manual review of critical code sections, especially those handling sensitive data, authentication, authorization, and external inputs, to identify complex or context-specific vulnerabilities that automated tools may miss.
  - **Coding Standards Compliance:** Verify that the code adheres to secure coding standards and best practices, such as OWASP Secure Coding Guidelines.
  - **Peer Review:** Implement peer review processes where developers examine each other’s code to catch potential issues and share knowledge about secure coding practices.
- Expose Security Flaws in Code:
  - **Vulnerability Identification:** Identify and document security flaws, such as logic errors, improper error handling, insecure use of cryptography, and hard-coded credentials.
  - **Threat Modeling:** Perform threat modeling to understand potential attack vectors and how identified vulnerabilities could be exploited in real-world scenarios.

  - **Remediation Guidance:** Provide actionable recommendations for fixing identified vulnerabilities, including code snippets, best practices, and reference materials to guide developers in secure coding.

Tools

- SAST Tools:
  - **SonarQube:** A popular open-source platform for continuous inspection of code quality and security, capable of identifying vulnerabilities, bugs, and code smells.
  - **Checkmarx:** A widely used SAST solution that provides in-depth analysis of the codebase to detect and remediate security vulnerabilities.
  - **ESLint (for JavaScript):** A static analysis tool for identifying problematic patterns in JavaScript code, including security flaws.

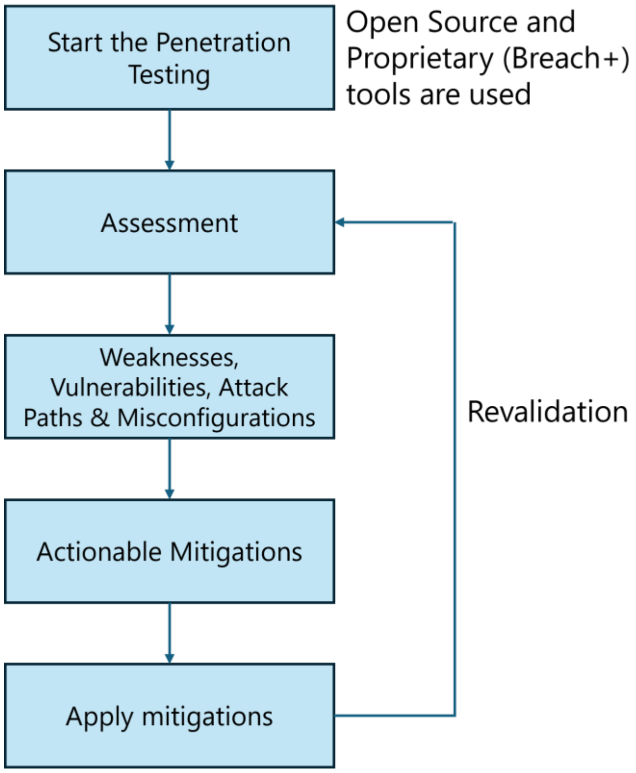
- Manual Code Review Tools:
  - **CodeCollaborator:** A tool that facilitates peer review of code changes, helping teams to collaborate on identifying and fixing security issues.
  - **GitHub Code Scanning:** Integrated security features in GitHub that allow for inline comments and suggestions during pull request reviews.
  - **Crucible:** A code review tool that helps developers catch defects and discuss code in a collaborative environment.

- Vulnerability Databases:
  - **OWASP Dependency-Check:** An open-source tool that identifies project dependencies and checks if there are any known, publicly disclosed vulnerabilities.
  - **CVE Details:** A database that provides information on publicly disclosed vulnerabilities and how they can be mitigated.

Tools/Softwares	Purpose
Nmap	Network mapping tool for identifying open ports and live hosts
Metasploit	Framework for developing and executing exploits
Nessus	Vulnerability scanner for identifying security flaws
Burp Suite	Web application security testing tool for analyzing traffic
Wireshark / TCPDump /Ettercap	Network protocol analyzer for monitoring network traffic
Aircrack-ng	Wireless network security tool for cracking WEP and WPA keys
Hydra	Network login cracker for testing password security
Kali Linux	Penetration testing operating system with a range of built-in tools
Nipper	A network infrastructure parser and security scanner that can be used for identifying vulnerabilities in SCADA systems.
Custom Exploits, Scripts	Team of exploit developer custom OT network-based test cases and custom script to exploit vulnerabilities.
Racid	External Attack Surface Management Tool for discovering and testing external assets including dark web monitoring, leak credentials, external infrastructure.
Breach+	Breach & Attack Simulation tool to automate network, endpoint and email security testing tool developed by Cytomate.
SonarQube	Source code review

Phase 4

Re-Validation Scan (Post assessment & verification test)


Start the Penetration Testing
Open Source and Proprietary (Breach+) tools are used
Assessment
Weaknesses, Vulnerabilities, Attack Paths & Misconfigurations
Actionable Mitigations
Apply mitigations
Revalidation

This process involves a detailed examination and validation of previously identified vulnerabilities within a system or network. By conducting a confirmatory scan, security professionals can verify that these vulnerabilities have been adequately addressed and remediated. It also helps in identifying any new or overlooked vulnerabilities that might have emerged since the last assessment.

Project Management

Deliverables

Cytomate will provide the following deliverables.

- Results Presentation
- Initial Technical Report
- Final Technical Report
- Executive Summary Report
- Remediation Plan

Reports

For each phase of the assessment, Cytomate will provide separate technical reports that will include the following sections:

- Detailed approach, tools, techniques, and methods used for the assessment, and a Risk Assessment Matrix adheres to international best practices and aligned to the assessment phases and in-scope assets.
- Identification of vulnerabilities/weaknesses, affected assets, observations, Risk Rating (High, Moderate, Low), level of exploitation, detailed Risks, and recommendations that align with standards, best practices, and regulations.
- Name of the vulnerability, Date of the discovery, Score based on CVE (Common Vulnerabilities and Exposures) databases.
- A detailed description of the vulnerability and affected systems
- Details of the process to fix/mitigate the vulnerability.
- POC (proof of concept) of the vulnerability for the system

Executive Summary Reports

- An English executive summary report that will provide an overview of the assessment purpose, objectives, approach, and high-level summary.
- List of all identified issues under each activity with maturity levels.

Follow-up Report:

We will provide a detailed report that lists the status of remediation for each revalidation.

Communication Plan

Cytomate will conduct **weekly update meetings** with the **QAPCO** team to discuss the ongoing progress of the project. These reports will include an overview of the overall project status, summaries of activities performed during the previous week, outlines of planned activities for the upcoming week, any required actions, and key findings. This regular communication ensures that the **QAPCO** team remains fully informed and can promptly address any emerging issues or requirements.

Stakeholders:

Stakeholder identification:

The first step in stakeholder management is identifying the key stakeholders involved in or impacted by the VAPT project from both sides.
Above mentioned list is stakeholders involved from Cytomate.

Employee Name	Designation	Company	Contact
Dr. Masoom Alam	Chief Technology Officer	Cytomate	mmalam@cytomate.net
Bilel Souaid	Chief Operating Officer	Cytomate	bilel@cytomate.net
Fraz Ahmad	Senior Cybersecurity Engineer	Cytomate	fraz@cytomate.net
Ijlal Haider	Pentest Lead	Cytomate	Ijlal.haider@cytomate.net
Zabi Ullah	Pentester	Cytomate	zabiullah@cytomate.net

Stakeholder meetings:

- **Kick-off Meeting**: Introduce the project scope, timeline, and testing methodology to all stakeholders.
- **Mid-Project Review**: Discuss preliminary findings and assess if additional testing is needed.
- **Final Meeting**: Present the executive summary, detailed findings, and remediation plan.

Project Timeline

Man-Days Requirements

Activity/Services	Man-Days	Deliverables
Stage 1: External Penetration Testing	20	Detailed technical report, mitigations, excel summary report
Stage 2: Internal Penetration Testing	40	Detailed technical report, mitigations, excel summary report

Stage 3: External Web Application	7	Detailed technical report, mitigations, excel summary report
Stage 4: Email Gateway Security Controls Validation	3	Detailed technical report, mitigations
Stage 5: Endpoint Security Controls Validation	7	Detailed technical report, vendor specific detection rules (Sigma, Yara), mitigations
Stage 6: Network Security Controls Validation	6	Detailed technical report, IOCs, Threat intel sharing (STIX2.1)
Stage 7: Security Architecture Review	7	Detailed technical audit report
Stage 8: Configuration review	7	Detailed technical audit report
Stage 9: Social Engineering	6	Assessment report, training
Stage 10: Compromise Assessment - Network Forensic Analysis	10	Detailed technical report, recovery strategies
Stage 11: Compromise Assessment - Host Forensic Analysis	14	Detailed technical report, recovery strategies
Stage 12: Source Code review	7	Detailed technical report, mitigations
Revalidation	7	Detailed technical report
Reporting	6	Detailed technical full report, executive summary report
Total	147	

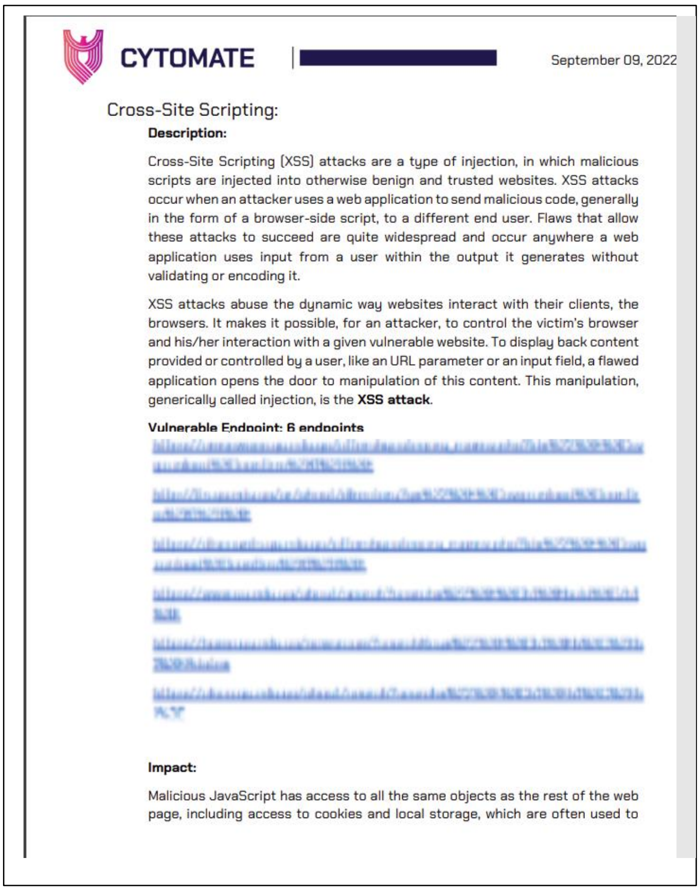
Detailed Timeline for each activity

Activities	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12
Onboarding and Deployment (VAPT & BAS)	■	■										
External Penetration Testing		■	■	■								
Internal Penetration Testing				■	■	■	■	■				
External Web Application		■	■									
Email Gateway Security Controls Validation			■	■								
Endpoint Security Controls Validation				■	■							
Network Security Controls Validation					■	■						
Security Architecture Review							■	■				
Configuration review								■	■			
Social Engineering								■	■			
Compromise Assessment - Network Forensic Analysis									■	■	■	
Compromise Assessment - Host Forensic Analysis									■	■	■	
Source Code review								■	■			
Reporting											■	■
Revalidation												■

References Point of Contacts

No.	Client Reference	Contact Person	Position	Phone
1	Dukhan Bank	Mahmoud Alsalakhi	CTO	5582 1986
2	SSB	Ahmed Al Naimi	Cybersecurity Director	66653999
3	Aljazeera	Ahmed Azzawe	Head of Infosec	5577 3391
4	QOC	Rasheed Al Nahlawi	Info Security consultant	33609241
5	Sidra Medicine	Tariq Abu Saqri	Senior Architect – Enterprise Architecture Solutions	55252010
6	HBKU	Mohammed Alhinndi	CIO	6634 7331
7	QDB	Mr. Dipu	System Engineer	66999018

Technical Report Template and Visual Dashboard



Cross-Site Scripting:

Description:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser-side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

XSS attacks abuse the dynamic way websites interact with their clients, the browsers. It makes it possible, for an attacker, to control the victim's browser and his/her interaction with a given vulnerable website. To display back content provided or controlled by a user, like an URL parameter or an input field, a flawed application opens the door to manipulation of this content. This manipulation, generically called injection, is the **XSS attack**.

Vulnerable Endpoint: 6 endpoints

[redacted]

[redacted]

[redacted]

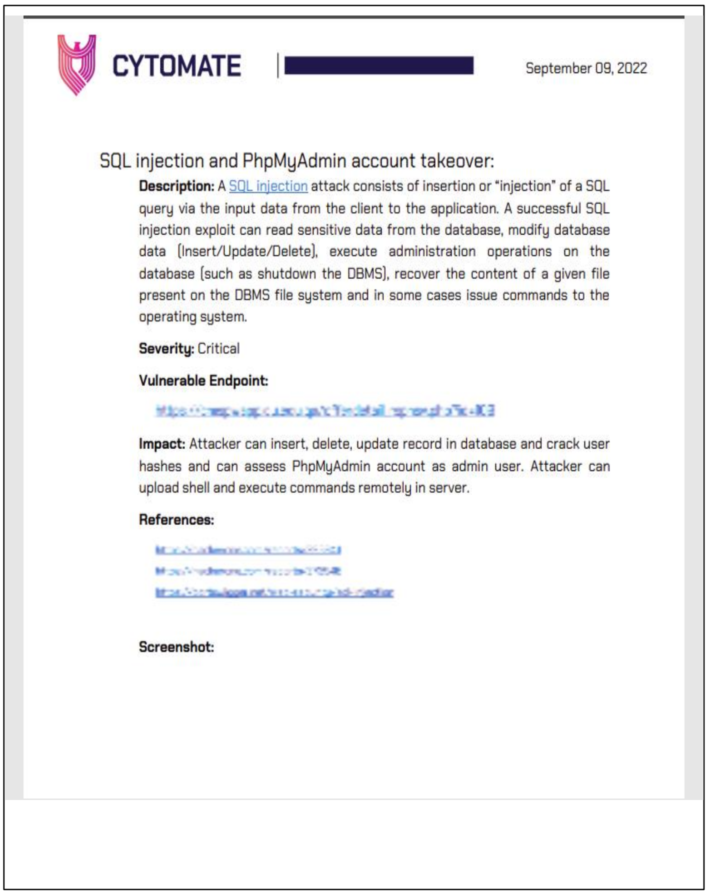
[redacted]

[redacted]

[redacted]

Impact:

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to



SQL injection and PhpMyAdmin account takeover:

Description: A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

Severity: Critical

Vulnerable Endpoint:

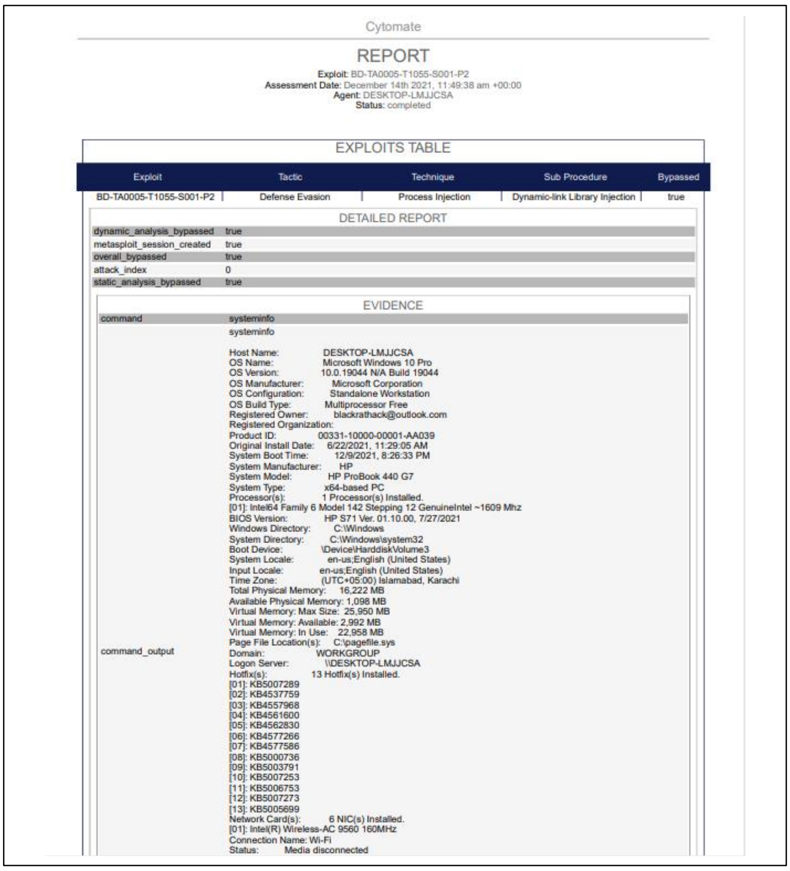
[redacted]

Impact: Attacker can insert, delete, update record in database and crack user hashes and can assess PhpMyAdmin account as admin user. Attacker can upload shell and execute commands remotely in server.

References:

[redacted]

Screenshot:



Cytomate

REPORT

Exploit: BD-TA0005-T1055-S001-P2
Assessment Date: December 14th 2021, 11:49:38 am +00:00
Agent: DESKTOP-LMJJCSA
Status: completed

EXPLOITS TABLE

Exploit	Tactic	Technique	Sub Procedure	Bypassed
BD-TA0005-T1055-S001-P2	Defense Evasion	Process Injection	Dynamic-link Library Injection	true

DETAILED REPORT

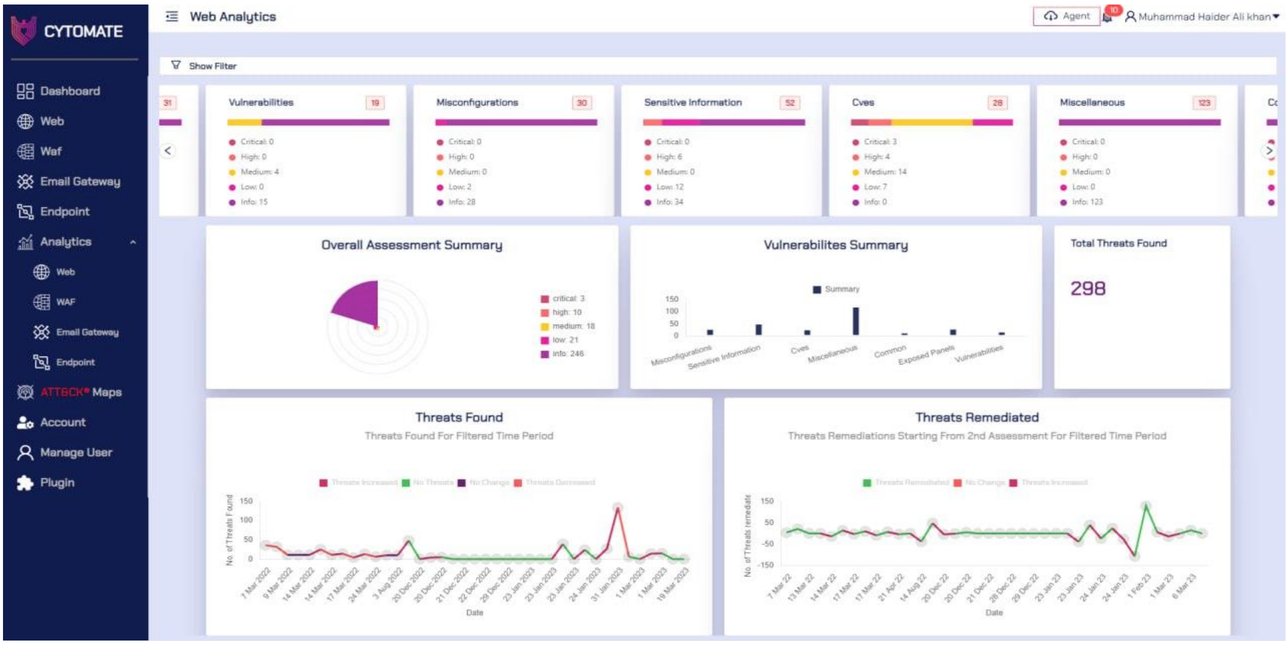
dynamic_analysis_bypassed	true
metasploit_session_created	true
overall_bypassed	true
attack_index	0
static_analysis_bypassed	true

EVIDENCE

command	systeminfo

command_output

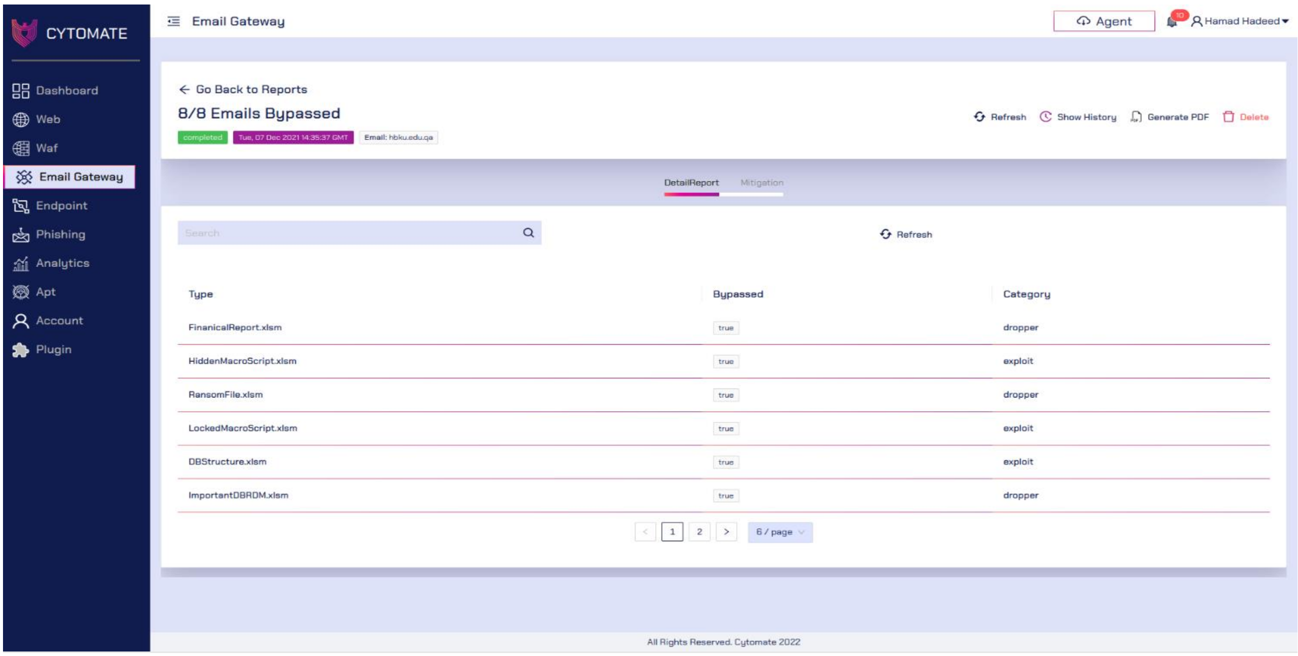
```
systeminfo

Host Name:                 DESKTOP-LMJJCSA
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          blackrathack@outlook.com
Registered Organization:
Product ID:                00331-10000-00001-AA039
Original Install Date:     6/22/2021, 11:29:05 AM
System Boot Time:          12/9/2021, 8:26:33 PM
System Manufacturer:       HP
System Model:              HP ProBook 440 G7
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 12 GenuineIntel ~1609 Mhz
BIOS Version:              HP S71 Ver. 01.10.00, 7/27/2021
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:00) Islamabad, Karachi
Total Physical Memory:     16,222 MB
Available Physical Memory: 1,098 MB
Virtual Memory: Max Size:  25,950 MB
Virtual Memory: Available: 2,992 MB
Virtual Memory: In Use:    22,958 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-LMJJCSA
Hotfix(s):                 13 Hotfix(s) Installed.
                           [01]: KB5007289
                           [02]: KB4537759
                           [03]: KB4557968
                           [04]: KB4561600
                           [05]: KB4562830
                           [06]: KB4577266
                           [07]: KB4577586
                           [08]: KB5000736
                           [09]: KB5003791
                           [10]: KB5007253
                           [11]: KB5006753
                           [12]: KB5007273
                           [13]: KB5005699
Network Card(s):           6 NIC(s) Installed.
                           [01]: Intel(R) Wireless-AC 9560 160MHz
                                 Connection Name: Wi-Fi
                                 Status:          Media disconnected
```



Vulnerabilities 19	Misconfigurations 30	Sensitive Information 52	Cves 28	Miscellaneous 123
Critical: 0	Critical: 0	Critical: 0	Critical: 3	Critical: 0
High: 0	High: 0	High: 6	High: 4	High: 0
Medium: 4	Medium: 0	Medium: 0	Medium: 14	Medium: 0
Low: 0	Low: 2	Low: 12	Low: 7	Low: 0
Info: 15	Info: 28	Info: 34	Info: 0	Info: 123

Total Threats Found

298

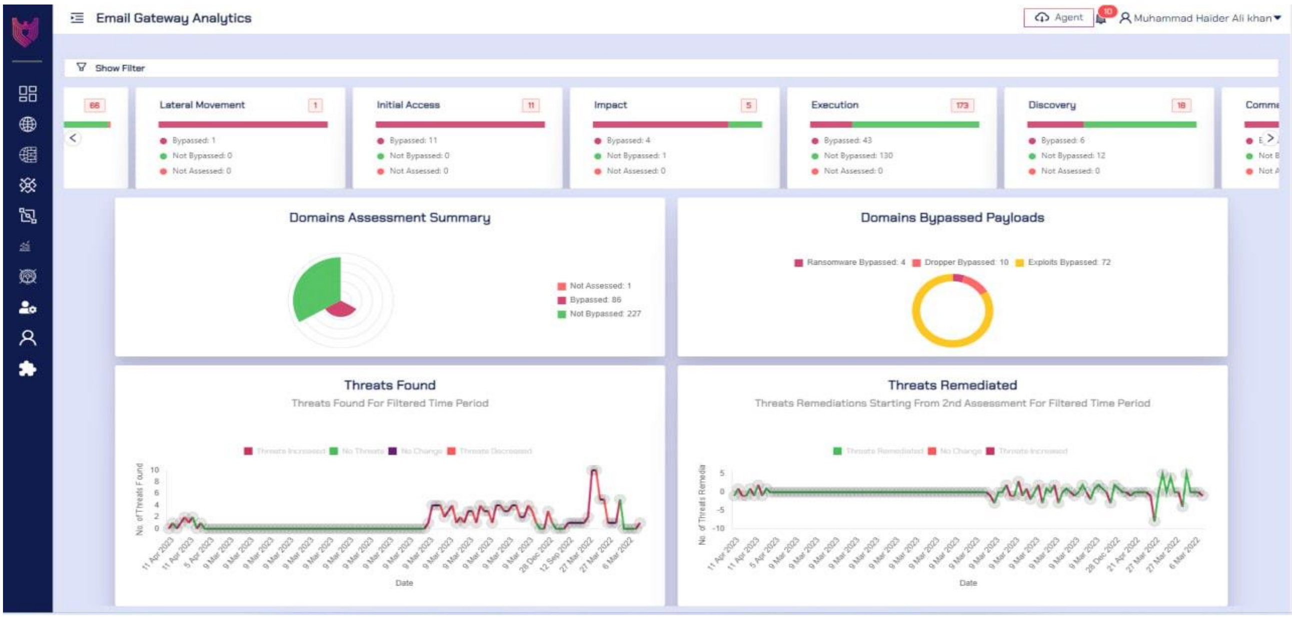


8/8 Emails Bypassed

completed Tue, 07 Dec 2021 14:35:37 GMT Email: hbku.edu.qa

Type	Bypassed	Category
FinanicalReport.xlsm	true	dropper
HiddenMacroScript.xlsm	true	exploit
RansomFile.xlsm	true	dropper
LockedMacroScript.xlsm	true	exploit
DBStructure.xlsm	true	exploit
ImportantDBRDM.xlsm	true	dropper

All Rights Reserved. Cytomate 2022



List of Employees

Name	Experience	Certifications	Field	Qualification
Dr. Masoom Alam	17+ Years	2 US Patents and 50+ Publications	Chief Technology Officer and Project Manager for this assessment	Ph.D. in Security Engineering
Fraz Ahmed	5 Years	Certified Cyber Security by ISC2, Practical Ethical Hacking, Mobile Application Penetration Testing, Cyber Security Foundation Professional, Pen tester Lab	Senior Cyber Security Engineer	Ongoing Master in Cybersecurity from HBKU
Ijlal Haider	5+ Years	Mobile Application Penetration Testing by TCM Security, Certified AppSec Practitioner by the SEC Group.	Cyber Security Engineer	B.S in Software Engineering
Usman Sikander	5 Years	PJPT (TCM), CEH (Certified Ethical Hacking) PFTP, API Penetration Testing, Foundations of Operationalizing MITRE ATT&CK, HCIA-Security Huawei, Cyber Security Foundation Certiprof, CCNA Routing and Switching Eduonix, OPSWAT EMAIL Security Associate, OPSWAT	Sr. Offensive Security Researcher	Master’s in cyber security

		Endpoint Associate, OPSWAT Network security Associate, OPSWAT web and WAF protection		
Zabi Ullah	3+ Years	Windows Penetration Testing Essentials, Ethical Hacking, Web Hacking/ Penetration Testing, Cyber Security Foundation Professional Certificate - CSFPC™	Cyber Security Engineer	Master of Science in Information Security

Note: This Proposal is valid for 120 days only (starting from 05/09/2024).

سايتوميت للحلول والخدمات ★ CYTOMATE SOLUTIONS AND SERVICES
س.ت ١٦٠٣٢١ ص.ب ١٧٨٢٩
الدوحة - قطر
Doha Qatar
C.R.No.. 160321, P.O. Box. 17829

Dr. Masoom Alam (Chief Technology Officer)

Appendix A: CVs of Key Personnel

Biographical Details

Name	Fraz Ahmad
Position in the Firm	Cyber Security Engineer
No. of Years' Experience	4+

Qualification Details: Educational/Professional/Training Record

Description	Year Obtained	Accreditation Body
Master of Science, Cyber Security	2024	Hamad Bin Khalifa University, Qatar
Bachelor of Science, Software Engineering	2022	COMSATS University, Pakistan
Mobile Application Penetration Testing	2022	TCM Security
Practical Ethical Hacking	2022	TCM Security
Cyber Security Foundation Professional Certificate	2021	CertProf
TensorFlow in Practice Specialization	2020	DeepLearning.AI
Deep Learning Specialization	2020	DeepLearning.AI

Employment Record

Employer	Period	Role Held
Cytomate Solutions and Service – Qatar	Jul 2020 - Present	Operations Team Lead & Cyber Security Engineer
Cyber Security Lab – Comsats University – Pakistan	2019 - 2021	Undergraduate Research Assistant
7 Star Internet Kallar Syedan – Pakistan	2021 - Present	Head of Internet Service Provider

Specialist Knowledge - Experience, Competencies and Skills

Fraz's specialist knowledge, competencies and skills include the following:

- ✓ Software Development
- ✓ SDLC (Software Development Life Cycle)
- ✓ Microservices Architecture (Docker, Kubernetes, Azure)
- ✓ OWASP, MITRE
- ✓ API Security
- ✓ Mobile application penetration testing
- ✓ Web application penetration testing
- ✓ Open-source threat intelligence (OSINT)
- ✓ Network Forensics
- ✓ Network Security
- ✓ Attack Surface Management
- ✓ Bug Hunter

Fraz is skilled and versatile professional with a strong background in Cyber Security and Software Development, additionally having hands-on experience of Microservices architecture, including proficiency in Docker, and Kubernetes. He has successfully implemented security solutions and led penetration testing campaigns/exercises.

Fraz led the penetration testing exercises from Cytomate for big organizations in Qatar, such as the Amiri diwan, and some top critical organizations testing during FIFA world cup. He has found many critical bugs in organization from black-box perspective which helped organizations to improve their security posture.

He also has hand on experience in projects life cycle and Software Development different methodologies, which led him to collaborate in research and development team who build innovative solutions like BAS (breach and attack simulation) and ASM (Attack surface management),

He has experience in comprehensive problem-solving, creative troubleshooting, and DevOps. Accomplished with effective collaboration skills, team building capabilities and leadership in diverse and multifaceted situations.

Biographical Details	
Name	Muhammad Ijlal Haider Zaidi
Position in Firm	Cyber Security Engineer
Role	Cyber Security Engineer
No. of Years' Experience	5+

Qualification Details: Educational/Professional/Training Record		
Description	Year Obtained	Accreditation Body
Mobile Application Penetration Testing	2023	TCM Security
Certified AppSec Practitioner	2023	The SEC Group

Employment Record		
Employer	Period	Role Held
Cytomate Solutions and Service – Qatar	Jan 2024 - Present	Penetration Tester Lead
Evamp&Saanga - Pakistan	2021 – 2023	Cyber Security Specialist, Cyber Security Lead
CydeaTech – Pakistan	2019-2021	Cyber Security Analyst

Specialist Knowledge - Experience, Competencies and Skills

Ijlal's specialist knowledge, competencies and skills include the following:

- ✓ SDLC (Software Development Life Cycle)
- ✓ Microservices Architecture (Docker, AWS)
- ✓ OWASP, MITRE, ISO, NIST
- ✓ API Security
- ✓ Mobile application penetration testing
- ✓ Web application penetration testing
- ✓ Open-source threat intelligence (OSINT)
- ✓ Network Forensics
- ✓ Network Security
- ✓ Red Team
- ✓ Blue Team
- ✓ Purple Team

Ijlal is skilled and versatile professional with a strong background in Cyber Security and Software Development, additionally having hands-on experience of Red Teaming, including Application Security, and Network Security. He has successfully implemented security solutions and led penetration testing campaigns/exercises.

Ijlal has vast experience with FinTech and Selfcare applications working on projects like MobilyPay, Maroctel, Salam DMS, Ufone BSMS, Jazz World, Ericsson Connected Recycling, Ericsson Wallet Platform etc.

He also has hand on experience of Penetration Testing and Vulnerability Assessment methodologies, such as PTES, OWASP, OSSTMM and ATT&CK. He has also participated in BlackHat MEA for 2023 securing 50th position worldwide.

He has experience in comprehensive problem-solving, creative troubleshooting, and Linux Administration. Accomplished with effective collaboration skills, team building capabilities and leadership in diverse and multifaceted situations.

Biographical Details

Name	**Usman Sikander**
Position in Firm	Cyber Security Engineer
Role	Security Consultant
No. of Years' Experience	3+

Qualification Details: Educational/Professional/Training Record

Description	Year Obtained	Accreditation Body
MS in Information Security	2022	COMSATS University, Pakistan
BS in Information Technology	2020	Arid Agriculture University, Pakistan
Practical Junior Penetration Tester (PJPT) Practical Malware Analysis & Triage Practical Ethical Hacking	2023	TCM Security
API Penetration Security	2023	APIsec
OPSWAT Email Security Associate OPSWAT Endpoint Compliance Associate OPSWAT Network Security Associate OPSWAT web and waf protection	2022	OPSWAT Academy
Certified Ethical Hacker	2022	PFTP
Cyber Security Foundation	2021	CertiProf
CompTIA Network+	2021	LinkedIn

CCNA Routing and Switching	2021	Eduonix
Foundations of Operationalizing MITRE ATT&CK	2021	AttackIQ
Huawei Certified ICT Associate of Security	2020	Huawei

Employment Record

Employer	Period	Role Held
Cytomate Solutions and Service – Qatar	May 2020 - Present	Senior Cyber Security Engineer
Medium	July 2020 – Present	Cyber security content Writer
COMSATS University, Pakistan	Nov 2020 – Jun 2021	Graduate Research Associate
HEC Pakistan	Nov 2020 - Jun 2021	HEC project: T-Eye: Threat Intelligence Platform
Network Administrator	Jan 2020 – Jan 2021	FIVERR

Specialist Knowledge - Experience, Competencies and Skills

Usman's specialist knowledge, competencies and skills include the following:

- ✓ Adversary Research and Emulation
- ✓ Offensive Security
- ✓ Malware Development (Linux & Windows)
- ✓ Malware TTPs Extraction (Analysis)
- ✓ Active Directory Exploitation
- ✓ Red Teaming
- ✓ Penetration Testing
- ✓ Web API Testing
- ✓ ICS/SCADA Attack Simulations
- ✓ Network Security
- ✓ Honeypot Deployment
- ✓ SIEM (Qradar, Azure Sentinel, Wazuh)
- ✓ Team building skills.
- ✓ C++, PowerShell, Batch Scripting, C#

Experienced cyber security engineer with a demonstrated history of working in offensive security. Usman passion lies in identifying and exploiting security gaps through advanced persistent threat (APT) emulations and simulations.

Usman has a proven track record of developing undetected exploits across all MITRE ATT&CK tactics, leveraging his proficiency in automating exploit processes, and conducting comprehensive endpoint simulations with security controls.

Usman commitment to excellence extends to researching new techniques and analysing real-world samples TTPs, enabling him to stay at the forefront of emerging cyber threats and techniques. Usman adept at recreating Tactics, Techniques, and Procedures (TTPs) to assess and enhance organizations' security controls effectively.

Usman led the Red Team Operations in Cytomate, and he has hands-on experience in OT penetration testing, with a unique ability to conduct attack simulations on various ICS/SCADA protocols, including Modbus, Modbus+, ModbusRTU, DNP3, S7 Siemens, and BACnet.

He specialized in crafting Stage 0 and 1 exploit, cleverly bypassing AV/EDR using both user-land API and kernel calls. Additionally, he created specific implants aligned with MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) to enhance purple teaming exercises.

Usman quick-learning abilities have allowed him to consistently deliver innovative and effective solutions, making him a valuable asset to any cybersecurity team.

He wrote blogs on different tactics and techniques to bypass next generation EDR solutions and anti-virus. In those blogs, He explained the windows API structure and how to bypass EDR user mode hooks by using direct and indirect syscalls.
https://medium.com/@merasor07

Biographical Details	
Name	**Zabi Ullah**
Position in Firm	Cyber Security Engineer
Role	Security Consultant, Penetration Tester, Product Lead
No. of Years' Experience	4+

Qualification Details: Educational/Professional/Training Record		
Description	Year Obtained	Accreditation Body
MS Information Security	2021	COMSATS University Islamabad
BS Software Engineering	2019	National University of Modern Languages, Islamabad
F.Sc. in Pre-Engineering	2014	Punjab College of Information

		Technology
Junior Penetration Testing (EJPT)	2023	INE (EC-Council)
Windows Penetration Testing Essentials	2023	EC-Council
Ethical Hacking	2022	Askills
Web Hacking/ Penetration Testing	2022	Udemy
Cyber Security Foundation Professional Certificate	2021	CertiProf

Employment Record

Employer	Period	Role Held
Cytomate Solutions and Service – Qatar	Oct 2020 - Present	Cyber Security Engineer
Cyber Security Lab, Comsats University	June 2020 – Sep 2020	Cyber security Researcher
Fabulous Technologies	Jun 2020 – Sep 2020	Senior Web Developer (Remote)
Funtash Technologies	Nov 2019 – May 2020	Web Team Lead
Emerging Pixel Software & Web Solutions	Dec 2018 – Sep 2019	Web Developer

Specialist Knowledge - Experience, Competencies and Skills

Zabi’s specialist knowledge, competencies and skills include the following:

- ✓ Phishing Campaigns
- ✓ AI-Security Product Development
- ✓ Malware Development
- ✓ Penetration Testing
- ✓ Red Teaming
- ✓ Cyber Threat Hunting
- ✓ Full Stack Developer
- ✓ Research and Development
- ✓ Technical Writer / Requirement Gathering Skills
- ✓ SDLC (Software Development Life Cycle)
- ✓ Project Management

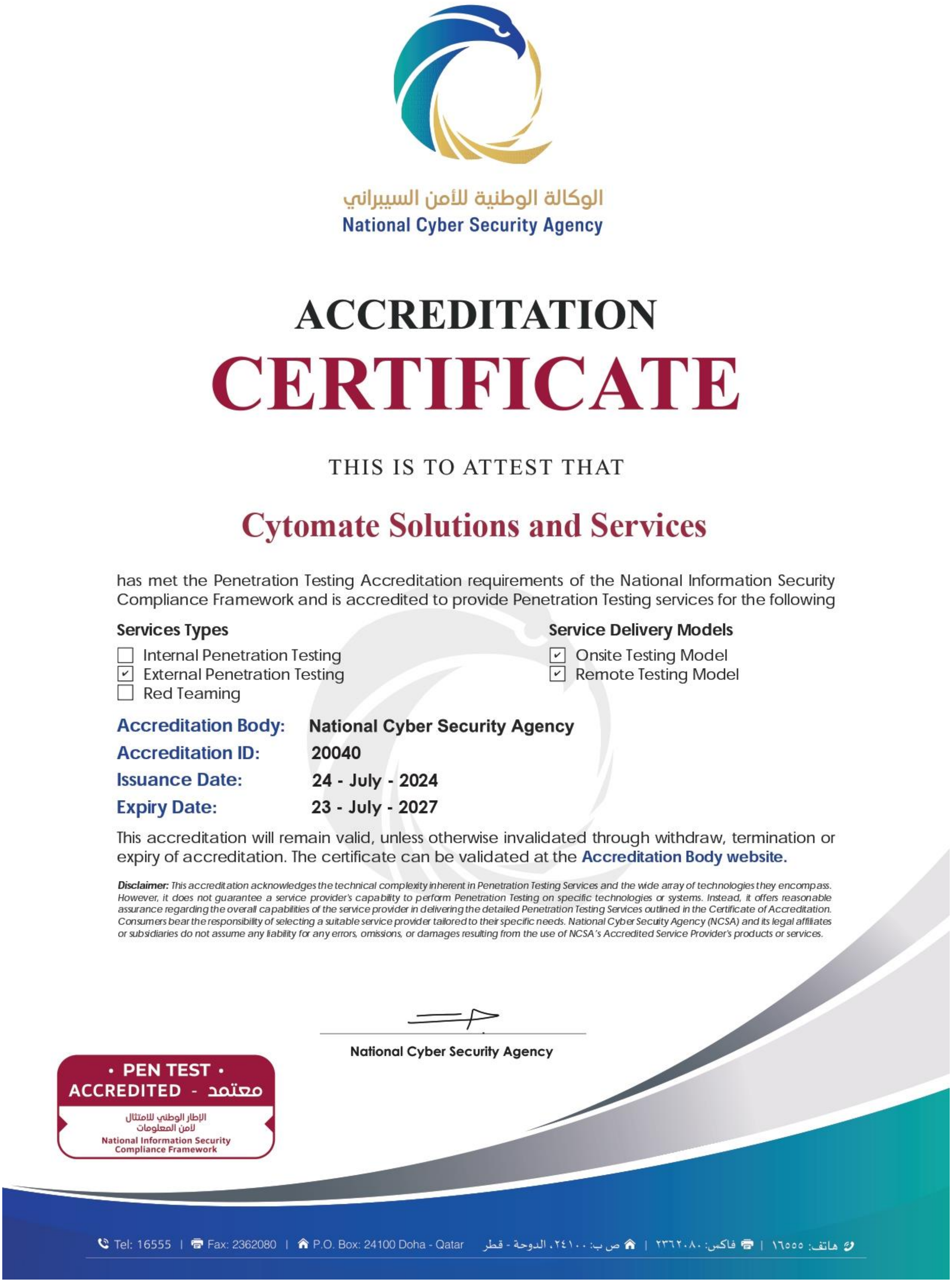
Zabi is a dynamic professional whose diverse skillset and extensive expertise form a comprehensive understanding of the cybersecurity landscape. With a keen eye for detail, Zabi adeptly devises and executes phishing campaigns, strengthening defenses against social engineering threats by simulating real-world attack scenarios.

An AI visionary, He has proficiency in AI-driven security product development empowers organizations with advanced threat detection solutions. His mastery extends to both offensive and defensive strategies, evident in his ability to develop and analyze malware behavior, contributing to cybersecurity readiness in an ever-evolving digital world.

Zabi's talents further span penetration testing, where he identifies vulnerabilities and recommends effective mitigations. His skill in orchestrating complex attack simulations through red teaming provides crucial insights into security readiness. As a full stack developer, Zabi seamlessly integrates security measures throughout the software development lifecycle. He also has hands on experience in projects life cycle and software development different methodologies. Hisham has delivered many end-to-end projects.

With a passion for innovation, Zabi conducts research that anticipates emerging threats. His effective communication and technical writing capabilities ensure clear documentation of intricate concepts and best practices. Deeply ingrained in the software development lifecycle, Zabi's understanding ensures the integration of robust security measures at every stage, yielding resilient software products.

Appendix B: Compliance Assurance



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

ACCREDITATION

CERTIFICATE

THIS IS TO ATTEST THAT

Cytomate Solutions and Services

has met the Penetration Testing Accreditation requirements of the National Information Security Compliance Framework and is accredited to provide Penetration Testing services for the following

Services Types

- □ Internal Penetration Testing
- ☑ External Penetration Testing
- □ Red Teaming

Service Delivery Models

- ☑ Onsite Testing Model
- ☑ Remote Testing Model

Accreditation Body:	National Cyber Security Agency
Accreditation ID:	20040
Issuance Date:	24 - July - 2024
Expiry Date:	23 - July - 2027

This accreditation will remain valid, unless otherwise invalidated through withdraw, termination or expiry of accreditation. The certificate can be validated at the **Accreditation Body website.**

Disclaimer: *This accreditation acknowledges the technical complexity inherent in Penetration Testing Services and the wide array of technologies they encompass. However, it does not guarantee a service provider's capability to perform Penetration Testing on specific technologies or systems. Instead, it offers reasonable assurance regarding the overall capabilities of the service provider in delivering the detailed Penetration Testing Services outlined in the Certificate of Accreditation. Consumers bear the responsibility of selecting a suitable service provider tailored to their specific needs. National Cyber Secuity Agency (NCSA) and its legal affiliates or subsidiaries do not assume any liability for any errors, omissions, or damages resulting from the use of NCSA's Accredited Service Provider's products or services.*

National Cyber Security Agency

• PEN TEST •
ACCREDITED - معتمد
الإطار الوطني للامتثال لأمن المعلومات
National Information Security Compliance Framework

☎ Tel: 16555 | Fax: 2362080 | P.O. Box: 24100 Doha - Qatar | هاتف: ١٦٥٥٥ | فاكس: ٢٣٦٢٠٨٠ | ص ب: ٢٤١٠٠، الدوحة - قطر

Appendix C: Approach to Confidentiality and Data Protection

This policy defines the mandatory minimum information security requirements based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise.
- assure a secure and stable information technology (IT) environment.
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure.
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions and vital government functions; compromise data; and result in legal and regulatory non-compliance.

2. Authority:

CYTOMATE SOLUTIONS AND SERVICES

3. Information Risk Management

- Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.
- Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
- Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.
- Risk assessment results, and the decisions made based on these results, must be documented.

4. Information Classification and Handling

- All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.
- All information assets must have an information owner established within the lines of business.
- Information must be properly managed from its creation, through authorized use, to proper disposal.
- All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.
- An information asset must be classified based on the highest level necessitated by its individual data elements.
- If the entity is unable to determine the confidentiality classification of information or the information is personal identifying information (PII) the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
- Merging of information which creates a new information asset or situations that create the

potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.

- All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
- The entity must communicate the requirements for secure handling of information to its workforce.
- A written or electronic inventory of all information assets must be maintained.
- Content made available to the general public must be reviewed according to a process that will be defined and approved by the entity. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- PPI must not be made available without appropriate safeguards approved by the entity.

5. IT Assets Management

- All IT hardware and software assets must be assigned to a designated business unit or individual.
- Entities are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.
- Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

6. Personnel Security

- The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific entity sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by the entity.
- An entity must require its workforce to abide by the Acceptable Use of Information Technology Resources Policy, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.
- All job positions must be evaluated by the to determine whether they require access to sensitive information and/or sensitive information technology assets.
- For those job positions requiring access to sensitive information and sensitive information technology assets, entities must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the entity to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the entity.
- A process must be established within the entity to repeat or review suitability determinations periodically and upon change of job duties or position.
- Entities are responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

7. Cyber Incident Management

- Entities must have an incident response plan, consistent standards, to effectively respond to security incidents.
- All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the Security Operations Center directly.
- The Security Operations Center must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

8. Physical and Environmental Security

- Entities must have an incident response plan, consistent standards, to effectively respond to security incidents.
- All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the Security Operations Center directly.
- The Security Operations Center must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

9. Account Management and Access Control

- All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT).
- Except as described in the, Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.
- Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.
- Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.
- Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.
- Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.
- Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.
- Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).
- Access privileges will be granted in accordance with the user’s job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with entity

missions and business functions (i.e., least privilege).

- Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).
- Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that user activities may be monitored and the user should have no expectation of privacy.
- Advance approval for any remote access connection must be provided by the entity. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.
- All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.
- Working from a remote location must be authorized by management and practices which assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

10. Third-party Security Management

- Risk Assessment: Conduct risk assessments of third-party service providers.
- Security Requirements: Include security requirements in contracts with third parties.
- Monitoring and Review: Regularly monitor third-party compliance with security requirements and conduct periodic reviews.
- Incident Reporting: Require third parties to report security incidents affecting the Service Provider’s information assets.

Appendix D: Communication and Reporting Strategy

1. OVERARCHING PRINCIPLES:

1.1. Confidentiality: Ensure that only authorized individuals can access the information.

1.2. Integrity: Ensure that the information is reliable and accurate and remains unaltered during transit.

1.3. Availability: Ensure that authorized users can access the information when they need it.

2. SECURE CHANNELS OF COMMUNICATION:

Secure Email Communication Setup

- **Choose a Secure Email Provider:** Select an email provider known for strong security measures. Providers like ProtonMail or Tutanota offer end-to-end encryption.
- **Create Dedicated Accounts:** Set up new email accounts specifically for the engagement to avoid mixing with routine business communications.
- **Enable Two-Factor Authentication (2FA):** Activate 2FA for an additional layer of security. This typically involves a secondary code sent to a phone or generated by an app.
- **Use Encryption:** Ensure that all emails are encrypted. If your email provider supports it, encryption will be automatic. Otherwise, use PGP (Pretty Good Privacy) for encrypting the content of the emails.
- **Secure Password Practices:** Use strong, unique passwords for each account. Consider using a password manager.
- **Test the Setup:** Send a test email to confirm that both parties can send and receive encrypted emails successfully.

3. SHARING OF VULNERABILITY DATA:

3.1. Encrypted Reports: All vulnerability reports will be encrypted using strong encryption algorithms (e.g., AES-256) and shared securely.

3.2. Password Protection: Reports and critical data will be password-protected. Passwords will be communicated via a separate channel (e.g., a voice call).

3.3. Avoidance of Descriptive Metadata: Ensure that filenames, subjects, or metadata do not reveal sensitive or indicative information about the contents.

4. INFORMATION RETENTION & DESTRUCTION:

4.1. Retention Policy: Maintain client-related communication and data only for the period necessary or as dictated by contractual obligations.

4.2. Secure Deletion: After the retention period, data will be securely deleted using tools that overwrite data multiple times, ensuring it cannot be easily recovered.

5. INCIDENT RESPONSE FOR COMMUNICATION BREACHES:

5.1. Immediate Notification: In the event of a suspected breach, the client will be notified immediately.

5.2. Investigation & Report: A thorough investigation will be conducted, and a detailed report of the breach, its impact, and remediation measures will be shared with the client.

5.3. Corrective Actions: Necessary actions will be taken to prevent a recurrence, and the communication procedure may be updated accordingly.

6. CLIENT RESPONSIBILITIES:

6.1. Secure Endpoint: Ensure that devices used to access and store information are secured,

patched, and free from malware.
6.2. Awareness & Training: Ensure that all stakeholders are aware of the secure communication protocols and adhere to them.
6.3. Feedback & Reporting: Inform **Cytomate** immediately if any anomalies, suspected breaches, or vulnerabilities in the communication process are identified.

Appendix E: Previous reports

Outlined below are summaries of the comprehensive VAPT reports delivered to our clients. These reports provide detailed insights into the vulnerabilities identified during the assessments, as well as the mitigation strategies recommended and implemented. These findings are taken from the executive report submitted to the client after the completion of the project.

Hadoop

Summary of findings

Risk Level	Critical	High	Medium	Low
No. of Vulnerabilities	0	21	46	33

Key Findings

Cytomate discovered the following **high-risk** vulnerabilities:

- **Missing Authentication:** the Apache Hadoop and Apache Solr application lacks proper authentication mechanisms, allowing users to access sensitive functionalities or data without requiring authentication.
- **Unrestricted shares**: The remote NFS server is exporting one or more shares without restricting access.
- **Possible Leak of Configuration Details:** Elasticsearch versions before 6.4.1 or 5.6.12 have an information disclosure issue where the _cluster/settings API can leak sensitive configuration details like passwords, tokens, or usernames to authenticated users.

These flaws could lead to serious breaches of confidentiality and integrity if they are exploited. Unauthorized access to personal identity information would be gained by adversaries.

Recommendations

Cytomate proposed the following recommendations:

- Configure and enable robust authentication mechanisms and implement role-based access control (RBAC) or attribute-based access control (ABAC) to enforce granular access controls based on user roles, permissions, or attributes.
- Upgrade the current installed version of Elastic Search

Cerner

Summary of findings

Risk Level	Critical	High	Medium	Low
No. of Vulnerabilities	5	34	21	4

Key Findings

Cytomate discovered the following **Critical** level risk vulnerabilities:

- **Oracle Java SE Vulnerability Detected**: The remote host is running Oracle Java SE versions 17.0.2 and 18, or Oracle GraalVM Enterprise Edition versions 20.3.5, 21.3.1, and 22.0.0.2. This critical vulnerability allows unauthenticated attackers with network access to

compromise data integrity and access within Oracle Java SE or Oracle GraalVM Enterprise Edition.
- **End of Support for Microsoft Windows Server 2012**: Microsoft Windows Server 2012 is no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor.
- **Missing Security Update of Windows Server 2012**: The remote Windows host lacks security update 5032249, rendering it vulnerable to multiple critical vulnerabilities, including remote code execution and security feature bypass. The identified vulnerabilities pose significant risks to the organization's IT infrastructure and data security.
- **Critical SMB shares improper authorization**: Shared Message Block (SMB) shares lack appropriate access controls, potentially allowing unauthorized users to access sensitive data and resources on the network.

Recommendations

Cytomate proposed the following recommendations:

- Upgrade to a version of Microsoft Windows that is currently supported.
- Apply Security Update 5032249 or Cumulative Update 5031419
- Configure share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.
- Review SMB share permissions, not to able for all users.

Appendix F: Risks Management & Mitigation Strategy

This Risk and Issue Management Plan establishes a structured approach to managing risks within a project lifecycle. It is designed to address risks in project scope, methodology, technology, or objectives, ensuring that each risk is monitored, managed, and mitigated, thus maintaining project integrity and alignment with strategic goals.

Risk Management Strategy

Risk Identification

The Project Manager has overall responsibility for managing project risk. Project team members may be assigned specific areas of responsibility for reporting to the project manager.

Throughout all phases of the project, a specific topic of discussion will be risk identification. The intent is to instruct the project team in the need for risk awareness, identification, documentation and communication.

Risk awareness requires that every project team member be aware of what constitutes a risk to the project, and being sensitive to specific events or factors that could potentially impact the project in a positive or negative way.

Risk identification consists of determining which risks are likely to affect the project and documenting the characteristics of each. Risk communication involves bringing risk factors or events to the attention of the project manager and project team.

It is the project manager's responsibility to assist the project team and other stakeholders with risk identification, and to document the known and potential risks. Updates to the risk documentation will occur as risk factors change. Risk management will be a topic of discussion during the regularly scheduled project meetings.

The project team will discuss any new risk factors or events, and these will be reviewed with the project manager. The project manager will determine if any of the newly identified risk factors or events warrant further evaluation. Those that do will undergo risk quantification and risk response development, as appropriate, and the action item will be closed.

Risk Analysis

To effectively prioritize and allocate resources in the event of risk event, identified risks are assessed according to two factors: the likelihood that risk will occur and the impact value of risk on the project. The higher the score, the greater the danger the risk poses to the project. Below is the Risk Analysis table based on Impact and Probability.

		Impact Value				
		Low	Minor	Moderate	Major	Critical
Likelihood	Almost certain	Low	Medium	High	Critical	Critical

		Impact Value				
		Low	Minor	Moderate	Major	Critical
	High	Low	Medium	High	High	Critical
	Medium	Low	Medium	Medium	High	High
	Low	Low	Low	Medium	Medium	Medium
	Almost Impossible	Low	Low	Low	Low	Low

Risk Response

Risk response includes two main tasks: (i) planning how to respond to risks and (ii) executing and monitoring action plans for responding to risks. There are four main types of risk response:

1. **Avoid**: Change the Project Plan and Schedule to avoid the risk completely. For instance, it can be done changing the scope.
2. **Accept**: Document and communicate the risk, but do not plan to take action.
3. **Transfer**: Transfer the risk to another party through insurance or contracting out.
4. **Mitigate**: Take action to reduce the probability and impact of a risk to a reasonable threshold. There are two types of risk mitigation activities:

    − **Prevention**: These are activities the team can do before the risk occurs to reduce its probability and impact, such as taking early action, close monitoring.

    − **Contingency**: These are activities the team can do once the risk occurs to reduce its impact. These activities can be written in a Contingency Plan. Having a contingency plan in place forces the project team to think in advance as to a course of action if a risk event takes place.

    • Identify the contingency plan tasks (or steps) that can be performed to implement the mitigation strategy.
    • Identify the necessary resources such as money, equipment and labor.
    • Develop a contingency plan schedule.
    • Define emergency notification and escalation procedures, if appropriate.
    • Develop contingency plan training materials, if appropriate.
    • Review and update contingency plans if necessary.

The below table provides concise outline of Cytomate's response protocol based on the risk evaluation.

Critical	Unacceptable	Must be given immediate Executive attention
High	Active management	Must have considerable management to reduce to as low as reasonably practicable
Medium	Tolerable	Risks should be managed and monitored to reduce to as low as reasonably practicable

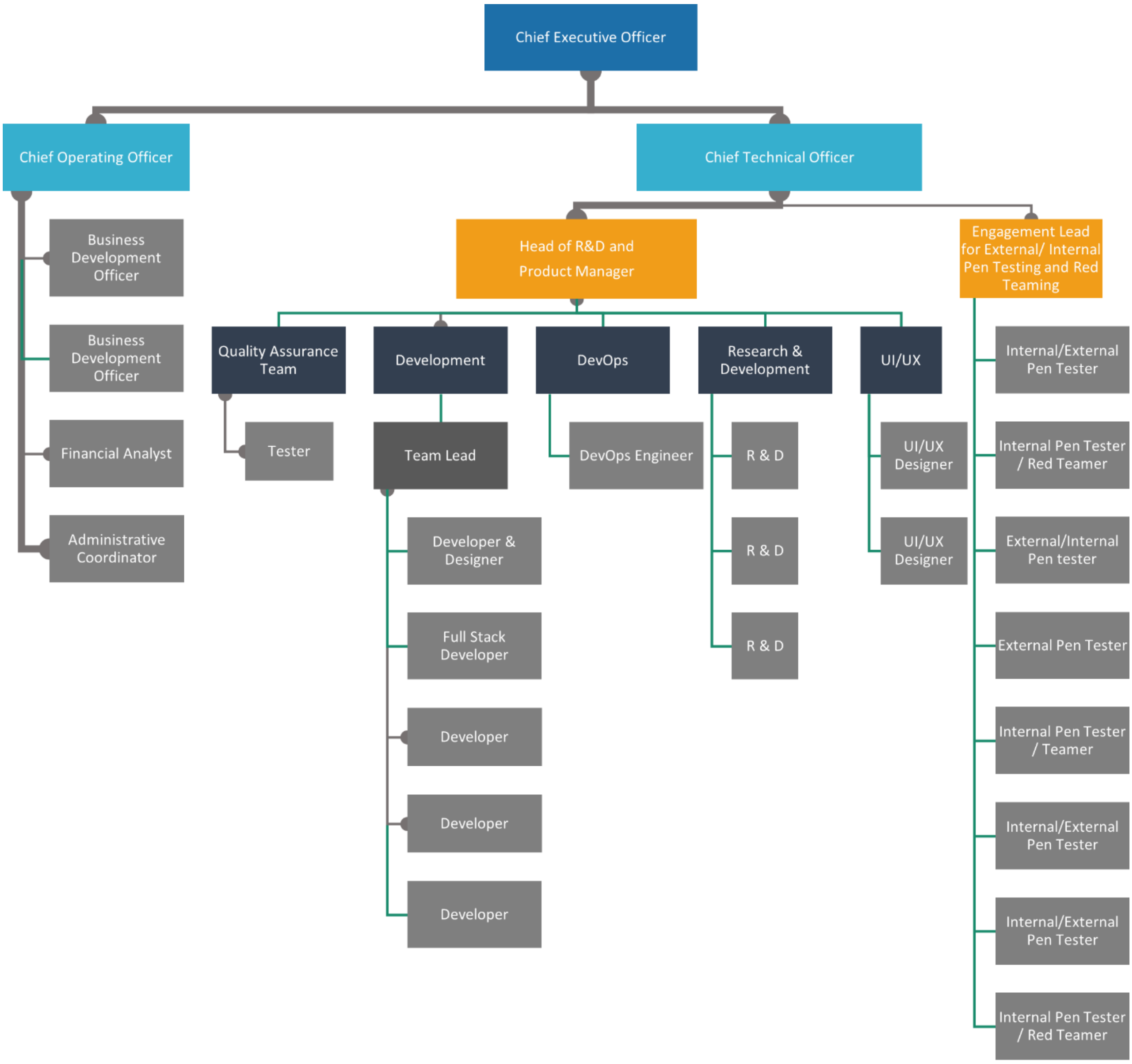
Low	No action required	Manage and monitor with normal operational management practices

Tracking and Reporting

As project activities are conducted and completed, risk factors and events will be monitored to determine if in fact trigger events have occurred that would indicate the risk is now a reality. Based on trigger events that have been documented during the risk analysis and mitigation processes, the project team or project managers will have the authority to enact contingency plans as deemed appropriate. Day to day risk mitigation activities will be enacted and directed by the project managers.

Risk management is an ongoing activity that will continue throughout the life of the project. This process includes continued activities of risk identification, risk assessment, planning for newly identified risks, monitoring trigger conditions and contingency plans, and risk reporting on a regular basis. Project status reporting contains a section on risk management, where new risks are presented along with any status changes of existing risks.

Appendix G: Organizational Chart



Chief Executive Officer
Chief Operating Officer
Chief Technical Officer
Business Development Officer
Business Development Officer
Financial Analyst
Administrative Coordinator
Head of R&D and Product Manager
Engagement Lead for External/ Internal Pen Testing and Red Teaming
Quality Assurance Team
Development
DevOps
Research & Development
UI/UX
Tester
Team Lead
DevOps Engineer
R & D
R & D
R & D
UI/UX Designer
UI/UX Designer
Developer & Designer
Full Stack Developer
Developer
Developer
Developer
Internal/External Pen Tester
Internal Pen Tester / Red Teamer
External/Internal Pen tester
External Pen Tester
Internal Pen Tester / Teamer
Internal/External Pen Tester
Internal/External Pen Tester
Internal Pen Tester / Red Teamer