Comtrade
Three-Sixty

Security Services

Comprehensive Solutions for Protecting Your Digital Assets

Contents

1.Penetration Testing

1.1. Infrastructure Penetration Testing Service

Our Infrastructure Penetration Testing Service is designed to rigorously challenge the security of your network and systems by simulating an attack from the perspective of both external and internal threats. This service targets your infrastructure to uncover vulnerabilities and configuration errors that could be exploited by attackers.

Benefits

- **Identify and Prioritize Security Risks:** Find out the gaps in your network and systems security setting before these are exploited by the malicious subjects.
- **Enhance Security Measures:** Understand your vulnerabilities and potential risks. Use this knowledge to strengthen your defense mechanisms.
- **Regulatory Compliance:** Make sure that your security measures comply with regulations, industry standards and data protection requirements to avoid financial and reputation damage.
- **Increased Stakeholder Confidence:** Build trust with clients, stakeholders, and internal teams by demonstrating your commitment to strict security standards.
- **Prevent Financial Loss:** Proactively identify and address security threats to avoid potential financial implications of data and system breaches.

Outputs

- **Detailed Vulnerability Report:** Detailed report of vulnerabilities exploited during testing, categorized by severity and impact.
- **Risk Assessment:** Assessment of potential business and operational impacts if the security gaps were to be exploited in a real-world scenario.
- **Remediation Guidelines:** Detailed explanation of steps required to remediate discovered vulnerabilities and prevent potential exploits.
- **Executive Summary:** A high-level summary highlighting critical risks and the potential business impacts of identified vulnerabilities.
- **Re-Test Option:** An option, to verify that vulnerabilities have been effectively resolved and to assess the improvements in your security posture.

1.2. Cloud Penetration Testing

Cloud Penetration Testing Service is designed to identify and address vulnerabilities in your cloud infrastructure. From public and private clouds to hybrid environments, our expert team employs advanced testing methodologies and techniques to simulate real-world attacks, making sure your cloud configurations, applications, and data are protected against potential breaches.

Benefits

- **Targeted Vulnerability Identification:** Identify weaknesses in your cloud infrastructure that could be exploited by cyber attackers, including improper configurations, inadequate access controls, and vulnerable cloud storage.
- **Improved Cloud Security Posture:** Improve your defense, understand your environment, components and their security status to better manage risks and prevent security incidents.
- **Compliance Assurance:** Make sure that your security measures comply with regulations, industry standards and data protection requirements to avoid financial and reputation damage.
- **Recommendation plan:** Get recommendations on how to improve your cloud security and measures based on industry standards, best practices and our vast penetration testing experience.

Outputs

- **Detailed Vulnerability Report:** Detailed report on each identified vulnerability within your cloud environment, classified by severity and potential impact.
- **Risk Assessment Documentation:** An analysis of the potential risks associated with each vulnerability, including the likelihood of exploitation and the potential impact and exploitation scenarios.
- **Remediation Guidelines:** Guidance and recommendations for addressing identified vulnerabilities. Outlining measures to secure your cloud environment against future threats, including short-term fixes and long-term security strategies.
- **Executive Summary:** A high-level summary highlighting critical risks, potential business impacts of identified vulnerabilities and strategic recommendations.

1.3. Application Penetration Testing Service Offering

Our Application Penetration Testing Service is designed to ensure that all your software applications including Web, Mobile and API are free from known vulnerabilities. This service emulates actual attack scenarios to expose the vulnerabilities that hackers might take advantage of. Our assessments (including but not limited to common and critical ones such as OWASP Top 10, OWASP Web and Mobile Security Testing Guides (WSTG, MSTG)) are intended to put your applications to the test under safe, managed conditions to help your business stay resilient against new forms of cyber threat.

Benefits

- **Proactive Vulnerability Identification:** Identify security weaknesses in your applications before they are exploited by attackers, reducing potential risks to your business.
- **Enhanced Application Security:** Reinforce your applications against attacks by addressing and patching vulnerabilities uncovered during testing.
- **Compliance Assurance:** Make sure that your security measures comply with regulations, industry standards and data protection requirements to avoid financial and reputation damage.
- **Customer Confidence:** Proactively address application vulnerabilities to demonstrate your commitment to security.
- **Cost-effective Security:** Vulnerabilities discovered early in development cycle are quicker and cheaper to address.

Outputs

- **Vulnerability Report:** Detailed report of vulnerabilities exploited during testing, categorized by severity and impact.
- **Risk Assessment Documentation:** An analysis of the potential risks associated with each vulnerability, including the likelihood of exploitation and the potential business impact.
- **Remediation Guidelines:** Detailed explanation of steps required to remediate discovered vulnerabilities and prevent potential exploits.
- **Executive Summary:** A high-level summary highlighting critical risks and the potential business impacts of identified vulnerabilities.
- **Re-Test Option:** An option, to verify that vulnerabilities have been effectively resolved and to assess the improvements in your security posture.

1.4. Objective-Based Penetration Testing Service

Objective-Based Penetration Testing extends beyond vulnerability checks to involve an exploration based on specific objective for a given organization. This service reproduces realistic cybers threats that are designed to achieve objectives that may pose a significant threat to an organization's operations and its customers; for instance, gaining unauthorized access to customer databases, compromising a valuable corporate asset, or interfering with important organizational business processes. This results in tests being specific to your business needs and security threats, which provides a more straightforward understanding of your real threats and protection. Objective-Based Penetration Testing can include wide specter of objectives like Data Exfiltration, Access to Protected Networks, System Disruption, Social Engineering, Email Phishing, just to name a few.

Benefits

- **Goal-Oriented Approach:** Focus directly on real-world outcomes and threats that matter most to your business. Specter of possible
- **Enhanced Security Posture:** Detect and mitigate potential weak points that can result in critical security threats, with the aim of aligning protective mechanisms against specific categories of threats.
- **Resource Efficiency:** Focus security resources and efforts on the key assets and critical processes to increase the overall security efficiency and effectiveness.
- **Risk Management:** Understand your risks in relation to business goals to allow better planning and more informed decision-making.
- **Compliance Assurance:** Make sure that your security measures comply with regulations, industry standards and data protection requirements especially in most critical business areas.

Outputs

- **Objective Achievement Report:** Documented simulated attacks, business objectives achieved and exploited vulnerabilities/security gaps.
- **Detailed Vulnerability and Exploit Analysis:** Detailed report of vulnerabilities exploited during testing, categorized by severity and impact, and relations to your business objectives.
- **Remediation Strategies:** Set of remediations designed to protect your assets against exploited vulnerabilities.
- **Impact Analysis:** Assessment of potential business and operational impacts if the security gaps were to be exploited in a real-world scenario.
- **Executive Summary:** High-level report outlining critical findings, business impacts, and strategic recommendations.
- **Re-Testing Option:** Verification of implemented security measures designed to prevent exploited security gaps in first round of testing, to prove that original objectives cannot be achieved after implementation of additional measures.

1.5. Ransomware Penetration Testing

Ransomware Penetration Testing Service is specifically designed to protect your organization by simulating sophisticated ransomware attacks. This service tests the resilience of your networks, systems, and staff against ransomware tactics, techniques, and procedures, helping to identify vulnerabilities before they can be exploited. Our expert team uses controlled and ethical hacking techniques to mimic the behavior of actual ransomware, assessing how it spreads, encrypts, and communicates, without the risk of real data loss.

Benefits

- **Proactive Vulnerability Identification:** Detect security vulnerabilities that ransomware might exploit, so that you reduce your risk of actually getting infected and losing your data.
- **Enhanced Incident Response:** Response helps your organization respond instantly and maintain business continuity even after an attack, reducing downtimes and recovery costs.
- **Employee Training:** Train employees to be resilient to strategic and realistic phishing attacks delivered by ransomware distributors while also increasing organizational vigilance and preparedness for such attacks.
- **Business Continuity Assurance:** Confirm that your backup and disaster recovery plans are effective and can maintain critical business functions, in the event of an attack.
- **Regulatory Compliance:** Make sure that your ransomware protection comply with regulations, industry standards and data protection requirements.

Outputs

- **Ransomware Simulation Report:** Descriptions of the simulated ransomware attack, including how it entered the organization, what it targeted, and what it did with the data, plus information about which security layers were bypassed.
- **Vulnerability and Impact Assessment:** Detailed findings of any vulnerabilities exploited during the test, categorized by severity level, and possible impact on operations and data.
- **Remediation Plan:** Plan containing actionable, prioritized, recommendations for improving your defenses against ransomware, both technically and strategically.
- **Training Summary:** An overview of employee response actions during the simulation, highlighting areas for improvement in human factors and response procedures.
- **Executive Summary:** A high-level summary highlighting critical vulnerabilities, potential business impacts, and recommendations for enhanced ransomware protection.

2.Security assessments

2.1. Cyber Maturity Assessment

Cyber Maturity Assessment is our service that helps you to determine the efficiency of your organization’s cybersecurity measures. This service involves a systematic evaluation of your security systems, policies, and practices, which helps in developing a clear picture of your security posture. This allows us to help you devise a robust plan for improvement that aligns with industry standards and best practices.

Benefits

- **Comprehensive Security Overview:** Get a detailed overview of your current cybersecurity posture and practices.
- **Identify Gaps and Vulnerabilities:** Discover weaknesses in your security measures that could be exploited by cyber threats.
- **Best Practices:** Get recommendations on how to improve your security processes and measures according to industry standards and best practices.
- **Risk Management:** Know your security risks and devise a prioritized plan to mitigate them.

Outputs

- **Maturity Assessment Report:** An assessment document that offers insights into the existing state of cyber security in your organization and the level of maturity within specific domains like governance, risk, assets, and events.
- **Gap Analysis:** Assessment of gaps in your security measures compared to industry standards and best practices.
- **Recommendation Plan:** A detailed plan how to address identified gaps to achieve desired maturity level.
- **Executive Summary:** Summary designed for senior management, highlighting key findings and strategic recommendations.

2.2.ICS/OT Cyber Security Assessment

Industrial Control Systems (ICS) and Operational Technology (OT) are critical components of the infrastructure that supports utilities, manufacturing, and essential services. However, these systems are increasingly targeted by cyber threats that can disrupt operations and cause significant economic and physical damage. Our ICS/OT Cyber Security Assessment Service is designed to address the unique challenges of securing industrial networks and devices. By comprehensively assessing the security posture of your ICS/OT environments, we identify vulnerabilities, assess risks, and provide actionable guidance to safeguard your critical infrastructure against cyber threats.

Benefits

- **Detailed Security Insights:** Gain a detailed understanding of your specific ICS/OT environment's security posture, tailored to the unique demands and vulnerabilities of industrial systems.
- **Risk Reduction:** Identify and address security vulnerabilities and deficiencies in your ICS/OT networks to help reduce risks of operational downtime and security incidents.
- **Regulatory Compliance:** Be compliant with industry regulations and standards -NERC CIP, IEC 62443 or ISO 27001- essential for keeping operational licenses and avoiding financial consequences.
- **Increased Resiliency:** Boost resilience to cyber threats with recommendations and strategic guidance designed to improve both cybersecurity and physical security.
- **Educate and Train the Employees:** Raise employee awareness about cyber security, vulnerabilities and safety procedures in ICS/OT environments.

Outputs

- **Security Assessment Report:** In-depth report detailing vulnerabilities, and how effectively our existing security controls are mitigating them.
- **Risk Analysis and Prioritization –** A list of risks derived from vulnerabilities, with consideration to potential safety/reliability/compliance impacts
- **Tailored Remediation Strategies:** Recommendations to address discovered risks and how they apply within your ICS/OT environment.
- **Compliance Analysis:** Review of the existing regulatory compliance gaps against recommended standards and guidelines.
- **Security Roadmap:** A blueprint for both immediate and long-term strategies to enhance the level of cybersecurity in your ICS/OT environment.
- **Training and Awareness Program:** A program to elevate employee cyber security awareness, threats, and protection.

3. DevSecOps

Secure your applications by employing industry best security practices in your software development process.

Integrate security checks into every step of your development cycle from earliest stages to neutralize vulnerabilities during development process to improve your application security posture and resilience.

DevSecOps Benefits:

- Proactive approach to application security reduces the risks of security breaches and data leaks.
- Integrates seamlessly into your development process and Incorporates industry best standards.
- Security by design from earliest development stages.
- Discover and remediate vulnerabilities before your application is affected.
- Reduces costs and time required to fix potential vulnerabilities.
- Helps you achieve regulatory and industry compliance.

3.1. Development Process Assessment

Gain insight into your company's software development process and security measures. People, Processes and Technology are evaluated to assess current state and identify gaps and recommended improvements needed to develop roadmap to enhance software development practices, security posture and vulnerabilities management. The results of the assessment will help you understand how to achieve better delivery times, reduced costs and a lower number of vulnerabilities in your software.

Benefits

- Gain insight into your software development practices and culture
- Identify areas which need improvements
- Learn about possible improvements, industry standards and tools that can help you elevate your software development
- Build a plan to strengthen your security posture and software development process

Activities

- Initial meeting with stakeholders
- Interviews with key personnel
- Review process/tools/environments
- Review and fine tune assessment findings
- Assessment presentation

Prerequisites

- Availability of key personnel for interviews during the assessment
- Access to development tools and environments

Output

Assessment report including:

- Documented Key security gaps and risks:
  - Practices and standards
  - Communication and processes
  - Recommended tools
- Roadmap to implement recommended improvements.

3.2.Build & Deploy

Enhance your traditional development process by introducing CI/CD pipeline built on the best industry standards. This allows you to gain control of your development lifecycle, configuration management and deployment, while preparing ground for implementation of security measures and continuous security improvements.

Prerequisites

- Build scripts and tools
  - pre-existing build scripts for individual application/component
  - make scripts (npm package.js scripts, maven pom files, etc.)
  - application tests (suits, scripts) to execute in pipeline
  - pre-existing container build scripts (docker files and dependencies)
- Availability of appointed Developer/Admins peers

Output

- Documentation specifying installed infrastructure, CI/CD, Configuration, Jobs
- Handover/Onboarding to engineers

Benefits

- Fully functional implementation and configuration of CI/CD pipeline and tools, ready to build your application
- Configuration management automation
- Automatic test execution
- Deployment control and automation.

Activities

Setup infrastructure:

- Jenkins/ Git (Hub/Lab) actions

- **Configuration:**
  - Jenkins/GitHub (Jobs, plugins, ...)
  - Code Repositories
  - WebHooks
  - Pipeline to use the existing Container registry
- Build automation (include one of: Maven, Gradle, Make, Go, Gcc)
- QA Automation Tool setup & Triggering (includes only run predefined tests prepared by Dev/QA engineers)
- Containerization scripts triggering
- Deployment configuration (Dev, Test, Prod)

Technical Description

- On-prem (local)
  - CI/CD
    - Jenkins or
    - Git (Hub/Lab) actions
  - Container registry
    - Local Open-source registry tool or
    - Hosted registry services (Docker Hub, GitHub registry, AWS ECR)
- Cloud (AWS)
  - CI/CD:
    - Jenkins
    - Git (Hub/Lab) actions

3.3. Security

3.3.1. Essential Security (SAST & DAST)

Identify critical vulnerabilities (like OWASP Top 10 and SANS 25) in the initial stages of development by analyzing source code and quickly resolve issues without breaking builds or passing on vulnerabilities to the final release of the application.

Further improve your application security by employing dynamic testing methods to detect runtime issues by simulating cyber-attacks. Simulate real life scenarios in a realistic environment to find potential exploits in your application, which could not be detected by static analysis alone. Application is tested from outsiders/attackers' perspective, mimicking their behavior and techniques, covering wide specter of vulnerabilities. Apply proactive approach to reduce the probability of security breaches and the corresponding costs of mitigation. Track all the security issues in an organized to help developers remediate these issues promptly and release applications with minimal problems.

Benefits

- Security assessment of source code
- Identification of security vulnerabilities during development
- Dynamic security testing of application
- Identification of security vulnerabilities in runtime environment
- Automatic issue severity assessment, allowing you to focus on most important issues first
- Security testing automation and integration in development process
- Security issues tracking and management
- Recommendations for fixing security issues

Activities

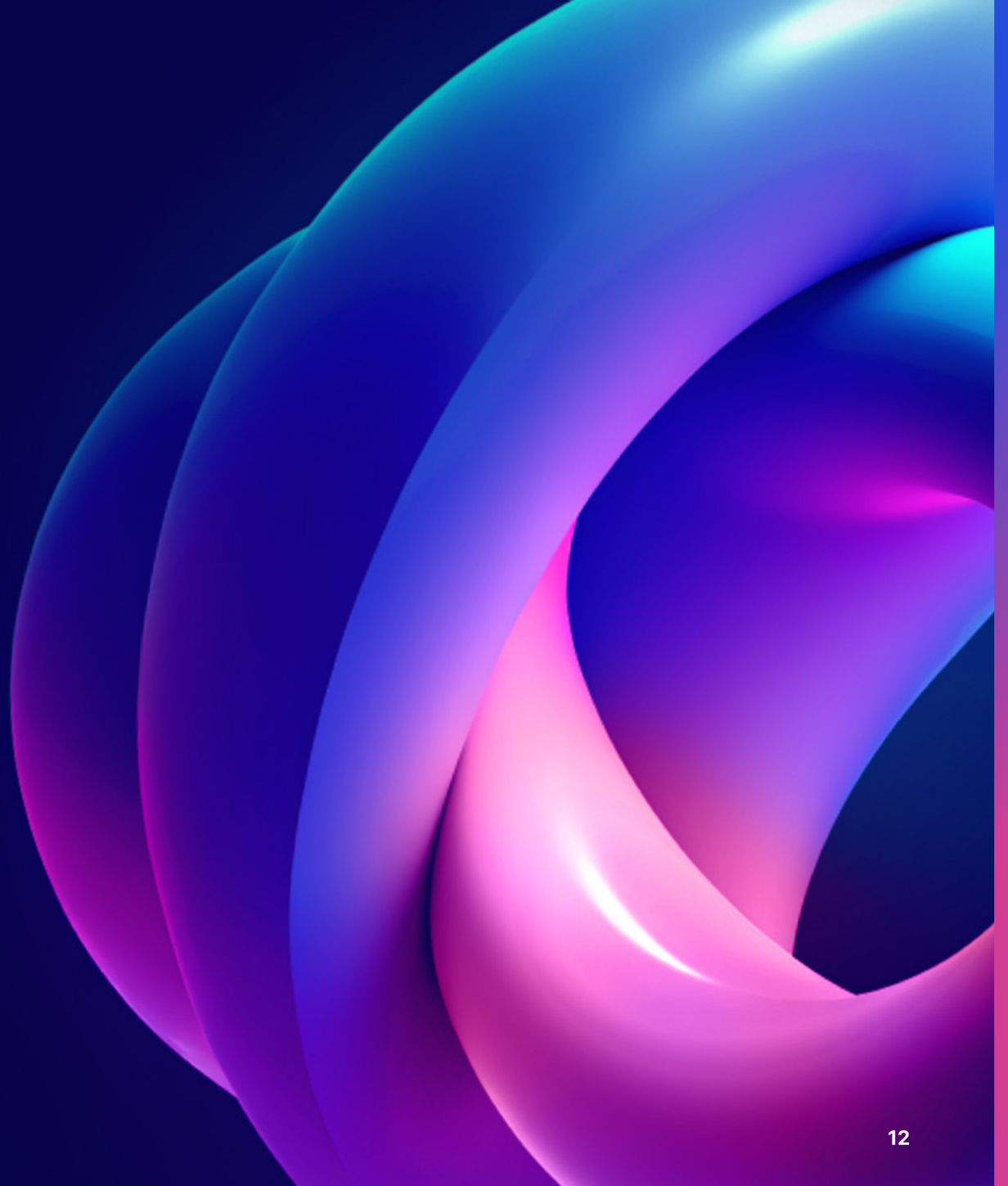
- Setup Infrastructure:
  - Sonarqube
  - OWASP ZAP
- Configure ZAP Scan to match the customers services, like specifying frameworks and DB if it is applicable.
- Configure SonarQube reporting to match the needs of client infrastructure.

Output

- SonarQube and OWASP ZAP reports where each issue is described with possible solutions for developers.
- Documentation specifying installed security infrastructure, tools, configuration, reports
- Handover/Onboarding to engineers

Technical Description

- SonarQube is used to identify vulnerabilities early for automated scans and to generate actionable reports for proactive security enhancements, following well established security standards as CWE Top 25, and OWASP Top 10.
- OWASP ZAP uncovers live vulnerabilities, automate security testing in operational environments, and provides detailed insights for targeted security improvements following security issue standard.



3.3.2. Enhanced Security (SAST, DAST & IAST)

Additionally, SAST and DAST approaches employ advanced security testing techniques, combining static and dynamic approaches, to cover an even wider vulnerabilities range. Combination of static and dynamic techniques allows more accurate vulnerability detection and a more efficient remediation process, by pinpointing vulnerabilities in the source code and suggesting their remediation to help development and security teams triage test results. This approach not only prevents security breaches in wide range of cases, but additionally reduces time and cost related to fixing those issues discovered during development process by providing precise information on their location and possible remediations.

Output

- SonarQube, OWASP ZAP and Contrast's Security reports where each issue is described with a viable solution for developers.
- Documentation specifying installed security infrastructure, tools, configuration, reports
- Handover/Onboarding to engineers

Benefits

- Included benefits from Essential Security

Additional:

- Combine Static and Dynamic security testing of application to cover even wider specter of vulnerabilities.
- Identification of security vulnerabilities in runtime environment and their location in the code
- Automatic issue severity assessment, allowing you to focus on the most important issues first.
- Recommendations for fixing security issues

Activities

- Setup Infrastructure:
  - Sonarqube
  - OWASP ZAP
  - Contrast Security Community Edition IAST
- Configure ZAP Scan to match the customer services, like specifying frameworks and DB if it is applicable.
- Configure SonarQube reporting to match the needs of client infrastructure.
- Configure Contrast Security Community Edition so it can access internal service data and services endpoints.

Technical Description

- SonarQube is used to identify vulnerabilities early for automated scans and to generate actionable reports for proactive security enhancements, following well established security standards as CWE Top 25, and OWASP Top 10.
- OWASP ZAP uncovers live vulnerabilities, automate security testing in operational environments, and provides detailed insights for targeted security improvements following OWASP Top Ten security issue standard.
- Contrast Security's IAST tool enables real-time application monitoring and identifies vulnerabilities through interactive testing. This approach ensures continuous security assessments and enhances overall code security by aligning with compliance standards such as PCI-DSS, GDPR, and HIPAA.

3.3.3. Advanced Security

The advanced security package is our ultimate security solution including SAST, DAST, IAST tools with an addition of critical tools like Linters and Trivy image scan into the development pipeline, ensuring unparalleled code quality and security. Linters provide an initial layer of defense by enforcing coding standards and identifying syntax errors that could lead to vulnerabilities, while Trivy scans for known vulnerabilities in images and its dependencies, ensuring that the software is free from exploitable flaws.

As an addition, this package introduces SAST and DAST quality gate that stops insecure code from progressing further in the CI/CD pipeline, significantly reducing the risk of security breaches and enhancing the overall security posture by ensuring that only thoroughly filtered and secure code is deployed to your production environment.

Dynamic scans are configured to periodically check production code for vulnerabilities in ever-evolving security landscapes and alert if new vulnerabilities have been discovered in the application.

This approach is key to maintaining a high standard of security while optimizing the efficiency of the development process.

Benefits

- Included benefits from Enhanced Security

Additional:

- Image security scanning (Trivy)
- Linter (Pre-commit hook)
- Dynamic scans to proactively monitor threat situations in production.

Activities

- Setup Infrastructure:
  - Sonarqube
  - OWASP ZAP
  - Contrast Security Community Edition IAST
  - Image scanner (Trivy)
  - Pre-build checker (Linter)
- Configure ZAP Scan to match the customers services, like specifying frameworks and DB if it is applicable.
- Configure SonarQube reporting to match the needs of client infrastructure.
- Configure Contrast Security Community Edition so it can access internal service data and services endpoints.
- Create pre-build check configuration (plugins and configuration for activated plugins).
- Set up Trivy by selecting target image repositories, defining vulnerability severity thresholds, and scheduling regular scans to ensure continuous security monitoring and reporting.
- Setup and configure Sonarqube and OWASP ZAP QualityGate
- Setup production dynamic scans and alerting

Output

- Documentation specifying installed security infrastructure, tools, configuration, reports
- Handover/Onboarding to engineers

Technical Description

- SonarQube is used to identify vulnerabilities early for automated scans and to generate actionable reports for proactive security enhancements, following well established security standards as PCI DSS, CWE Top 25, and OWASP Top 10.
- OWASP ZAP uncovers live vulnerabilities, automate security testing in operational environments, and provides detailed insights for targeted security improvements following OWASP Top Ten security issue standard.
- Contrast Security's IAST tool enables real-time application monitoring and identifies vulnerabilities through interactive testing. This approach ensures continuous security assessments and enhances overall code security by aligning with compliance standards such as PCI-DSS, GDPR, and HIPAA
- Git hook Linter scripts are run on every commit ensuring superior code quality at the earliest stage of CI/CD pipeline by following generally established coding standards depending on the programming language (e.g. PEP 8, PSR, ESLint, Java Coding Conventions)
- Trivy is a pre-build image scanning tool that detects vulnerabilities in dependencies at the earliest stages of development
- Quality Gates are based on various metrics and rules that assess code against predefined standards as mentioned in SAST, DAST and IAST tools

3.4.Managed service

Have your CI/CD and security infrastructure maintained, monitored and updated on a regular basis by our team of skilled engineers. Keep your CI/CD up and running to allow your teams to develop your applications without disruptions.

Activities

- Update CI/CD instances/plugins
- Regularity patch Infrastructure and dependencies
  - Jenkins instance (update versions)
  - Jenkins plugins (update versions)
  - Docker registry (re-build existing Dockerfile if we need to change some cert or versions)
  - Monitoring software (update versions)
  - Security tool set (update versions)
- Review current pipeline and optimize Jobs if required
- Review current monitoring and update dashboards, triggers and alerts
- Backup Jenkins (instance and jobs), monitoring (dashboards and alerts), security reports

Benefits

- CI/CD and security infrastructure monitored to run and allow your teams uninterrupted development
- Regular updates and patches

Output

- Upgrades and maintenance
- Regular activity report
- Documentation about versioning and future patching

Comtrade
Three-Sixty

info@comtrade360.com
+1 617-546-7400
comtrade360.com