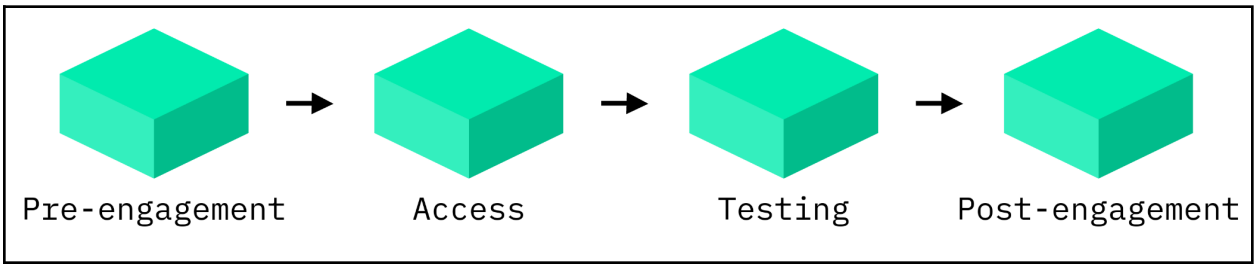
Forces Unseen

www.forcesunseen.com
contact@forcesunseen.com
+1 (312) 767-4029

Infrastructure Security Assessment Methodology



Pre-engagement

In this phase, Forces Unseen establishes the goals and scope of the engagement by gathering information about the target environment and client objectives.

Goals

Understanding the purpose and business function of the environment is essential to provide a comprehensive review. Functionality, data types, and associated risks should be enumerated at this stage.This is also the best time to share any pre-existing security concerns regarding the environment, recently released functionality, or particular classes of vulnerabilities.

Scoping

Understanding the scope will ensure that Forces Unseen is able to assess the environment adequately. This includes reviewing items such as:

- Hosting provider (e.g., AWS, Azure, GCP)
- Size of the environment and number of cloud resources in use
- Infrastructure-as-Code tools used (e.g., Kubernetes, Terraform)
- Container technologies
- CI/CD pipeline (e.g., GitHub actions, Jenkins)

Access

As a prerequisite to testing, Forces Unseen requires access to the environment. This will take place prior to the target start date of the engagement.

Some items the team may need include:

- Account credentials and cloud access keys (AWS/GCP/Azure)
- Infrastructure as Code definitions
- Documentation and diagrams
- Slack, email, or other communication channels

Testing

The majority of the apportioned time is spent in this phase. This is when tool-assisted manual security testing occurs. Forces Unseen will communicate with the client during this time in regards to access obstacles, critical vulnerabilities, and developer insight.

Tooling

Infrastructure-as-Code Static Analysis

Forces Unseen uses a combination of open source and in-house tools to scout for high-impact misconfigurations in Infrastructure as Code configurations. This includes Kubernetes, Terraform, Ansible, Docker, and other infrastructure orchestration utilities.

Validation of Automated Scan Results

Forces Unseen performs automated infrastructure and configuration scanning using ScoutSuite, tfsec, trivy, checkov, and other third-party and in-house tools. Forces Unseen validates these results to ensure only bona fide vulnerabilities are included in the report.

Manual Activities

Manual assessment of the infrastructure is crucial for discovering impactful security vulnerabilities. This involves understanding the architecture of the infrastructure and its business context. The

adversarial “tire-kicking” often leads to the identification of complex and critical vulnerabilities that would otherwise go undiscovered. The following list summarizes the key areas which are often focused on during an engagement:

Authentication and Authorization

Authentication, ACLs, and other policy and process configurations dictate the environment in cloud computing. Over time, these configurations tend to accumulate debts from the many “one-off” exceptions.

- Over-scoped IAM ACLs
- Unmanaged Inline Policies
- Disabled 2FA

Encryption and Secrets

Data encryption requirements and standards vary by category and context. Regulatory requirements often dictate minimum standards and practices. While encryption and data handling are often straightforward, nuances in implementation can result in unexpected or exploitable behavior.

- Persistent Data Encryption
- Transport Security
- Secrets Management
- Tenancy and Partitioning

Application and Data Processing

Infrastructure applications and data processing pipelines differ by environment. Testing ensures the principle of least privilege is implemented and that sensitive resources are not exposed within the environment.

- Service Exposure
- Cloud Data Storage ACLs
- Cloud Compute Applications

Post-engagement

Once the assessment is complete, the team delivers a report that will provide the information necessary to reproduce and remediate the identified vulnerabilities. This will be provided as a PDF document along with any accompanying materials referenced in the report.

We then schedule a readout of the report to review and answer any questions. Remediation testing can be scheduled once the vulnerabilities have been remediated.