INTERMEDIATE LEVEL

Advanced Misconfigurations

1. Cloud Infrastructure Vulnerabilities

- **Improper S3 bucket permissions: Public access to sensitive storage**
- **Excessive IAM permissions: Over-privileged accounts and roles**
- **Unprotected cloud storage: Missing encryption at rest**
- **Unmanaged cloud assets: Shadow IT and forgotten resources**
- **Insecure API gateways: Missing authentication/authorization controls**
- **Misconfigured virtual networks: Improper network segmentation**

2. Complex Web Security Misconfigurations

- **Inadequate CORS configurations: Too permissive cross-origin policies**
- **JWT implementation flaws: Missing signature validation, weak algorithms**
- **Insecure deserialization: Improperly configured deserializers without validation**
- **WebSocket security issues: Missing authentication or encryption**
- **OAuth/OIDC implementation errors: Improper redirect validation, token handling**
- **API security gaps: Missing rate limiting, input validation, or authentication**

3. Database and Data Storage Misconfigurations

- **Exposed database interfaces: Admin consoles accessible from public networks**
- **Excessive database permissions: Accounts with more privileges than necessary**
- **Missing data encryption: Sensitive data stored in plaintext**
- **Default database settings: Default ports, credentials, or configuration values**
- **Improper backup security: Unencrypted or publicly accessible backups**

4. Network Security Misconfigurations

- **Firewall rule issues: Overly permissive or conflicting rules**
- **Misconfigured WAF settings: Bypassed security controls or false positives**
- **TLS/SSL implementation flaws: Weak cipher suites, outdated protocols**
- **VPN misconfigurations: Split tunneling issues, excessive access grants**
- **Insecure network segmentation: Missing controls between environments**

Intermediate Detection Methods

1. Specialized Testing

- **Configuration scanners: Tools like ScoutSuite for cloud environments**

- **SAST/DAST tools: Static and dynamic application security testing**
- **Infrastructure as Code scanners: Tools like Checkov, tfsec**
- **Container security scanners: Tools like Trivy, Clair**
- **Compliance benchmarks: CIS benchmarks for various systems**

2. Advanced Analysis Techniques

- **Security architecture reviews**
- **Threat modeling sessions to identify potential misconfigurations**
- **Code-assisted security reviews**
- **Cloud security posture assessment**
- **Network penetration testing**

3. Monitoring and Validation

- **Configuration baseline monitoring: Detecting drift from secure baselines**
- **Log analysis: Identifying unusual access patterns**
- **Network traffic analysis: Detecting unexpected communications**
- **Vulnerability trend analysis: Identifying recurring misconfiguration patterns**

Intermediate Prevention Strategies

1. Security Engineering Practices

- **Defense in depth: Multiple security layers to protect against single failures**
- **Principle of least privilege: Minimize access rights to only what's necessary**
- **Infrastructure as Code: Version-controlled, tested infrastructure configuration**
- **Immutable infrastructure: Replace rather than modify running systems**
- **DevSecOps integration: Security checks in CI/CD pipelines**

2. Comprehensive Hardening Approaches

- **Environment-specific security configurations**
- **Component isolation using containers and micro-segmentation**
- **Third-party dependency security review process**
- **Secure configuration templates and golden images**
- **Role-based access control for all systems**

3. Advanced Security Controls

- **Multi-factor authentication for all admin interfaces**
- **Just-in-time access provisioning**

- **Service mesh security configuration**
- **API gateway security controls**
- **Web application firewall with custom rules**