**Team 0**

Diagram

Description automatically generated

Diagram

Description automatically generated

Diagram

Description automatically generated

**White Team**

Contains elements of *Compliance, Management, Analytics, Logistics.*

Responsibilities:

* Rule Drafting
* Organize Teams
* Make plans
* Follow up on progress

**Security Standards**

ISO27001 Controls (Annex A) – defines how to mange Information Security in a company

A.5 **Information security policies**   
How the policies are written and reviewed

A.6 **Organization of information security**   
How the responsibilities are assigned; also includes the controls for mobile devices and teleworking

A.7 **Human resources security**    
Controls prior to employment, during, and after the employment

A.8 **Asset management** – controls related to inventory of assets and acceptable use, also for information classification and media handling

A.9 **Access control** Controls for Access control policy, user access management, system and application access control, and user responsibilities

A.10 **Cryptography**Controls related to encryption and key management

A.11 **Physical and environmental security**   
Controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, clear desk and clear screen policy, etc.

A.12 **Operational security**   
Controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.

A.13 **Communications security** – controls related to network security, segregation, network services, transfer of information, messaging, etc.

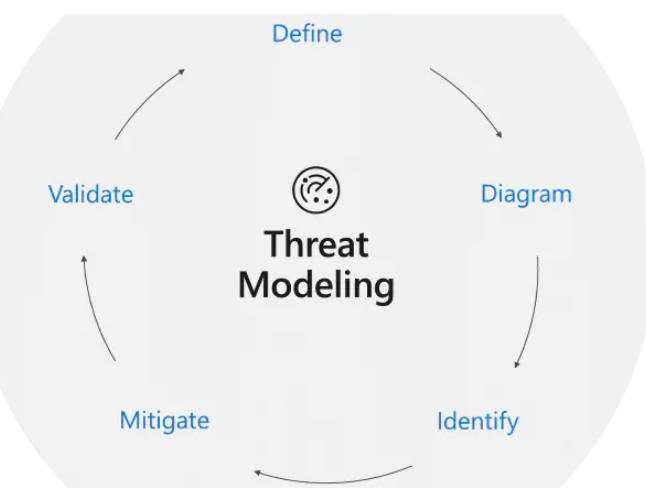
A.14 **System acquisition, development and maintenance**   
Controls defining security requirements and security in development and support processes

A.15 **Supplier relationships**Controls on what to include in agreements, and how to monitor the suppliers

A.16 **Information security incident management**   
Controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence

A.17 **Information security aspects of business continuity management** – Controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy

A.18 **Compliance**   
Controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security



**Threat Modeling**

process by which potential threats, such as structural vulnerabilities can be identified, enumerated, and prioritized. Purpose: provide defenders with a systematic analysis of probable attackers profile, most likely attack vectors, most desired assets

**Modeling Techniques**

* Find Security Bugs early
* Understand Security Requirements
* Engineer and Deliver Better Products
* Address Issues Other Techniques Wont

**Trust Boundaries**

* Boundaries to show who controls what
* Threats that cross those boundaries are likely important
* Different people control different things

Examples: Accounts, Network Interfaces, Different physical computers, VM’s

**STRIDE**

**S**poofing → Pretending to be someone you’re not *(Authenticity)*

**T**ampering → Modification *(Integrity)*

**R**epudiation → Claiming you didn’t do something

**I**nformation Disclosure → Exposing info to people who are not authorized to see it *(Confidentiality )*

**D**enial of Service → Prevent system from providing services *(Availability)*

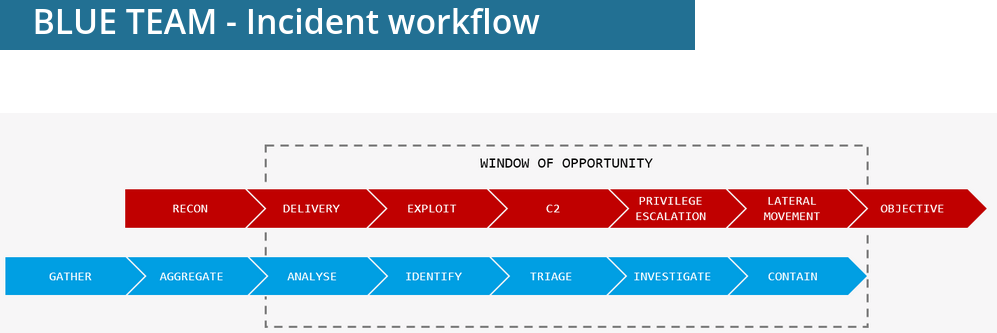
**E**levation of Privilege → When a program/user is able to do things they’re not supposed to *(Authorization)*

**What to do?**

* Mitigate
* Eliminate
* Transfer
* Accept

**Blue Team**

“Blue team is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify effectiveness of each security measure, an d make certain all security measures will continue to be effective after implementation”



Chart, pie chart

Description automatically generated

**Phase 1 – Preparation**

1. Identify and prioritize your assets

- *What would cost the company financially?*

*- What creates biggest disruption?*

*- What would cause biggest reputational damage?*

1. Identify potential risks

- *Risk Assessment*

1. Establish procedures

- *Forensic Analysis checklists*

*- Emergency contact communications checklists*

*- System backup and recovery checklists*

*- Security policy review checklists*

1. Assemble a response team

- *Multidisciplinary & clear about their role*

*- Not only IT-people*

1. Train your employees

**Phase 2 – Detection & Analysis**

1. **Detection**

- *Network Intrusion*

*- Detection System (NIDS/NIPS)*

*- Host Intrusion*

*- Detection System (HIDS/HIPS)*

Chart

Description automatically generated

***NIDS Tools***: Snort Suricata

***HIDS Tools***: Wazuh OSSEC

**Honeypots**

***Low Interaction:*** Emulate attractive services such as FTP and SMB, collection probes from attackers, not compromise-able but seems so

***High Interaction:*** Attackers can interact with it like a normal machine, collect forensic data in central repository, seems normal, hard to identify

**2. Analysis**

**DFIR**

Digital Forensics & IR is a multidisciplinary profession that focuses on identifying, investigating, and remediating computer network exploitation. Skill-set includes:

* Malware Triage (*IDA) –* Recognize/Analyze/Reverse-Engineer
* Log Analysis *(Security Onion*)
* Dev
* Network Forensics (*Wireshark, Snort, Suricata)*
* Intelligence Analysis (*Maltego, OSINT but more advanced)*
* Memory Forensics (*Volatility*)
* FS Forensics *(Autopsy, AccessData ForensicToolKit)*
* Soft Skills: Good communication skills, Teamwork, Lifelong learning

**FS Forensics**

Disk-to-Image, Disk-to-disk, Logical, Sparse

***Extraction***: Retrieving unstructured or deleted data. Deleted != gone, only removes it from disc contents table. Other hiding techniques include encryption, steganography, file obfuscation.

**Phase 3 – Containment, Eradication, Recovery**

Protect the Present:

* Lock Down Systems
* Analyze/Archive logs
* Repair/Rebuild systems
* Test systems

Protect the Future:

* Network Forensics
* Computer Forensics
* Log Analysis
* Root Cause Analysis

- **Identify** the fault

- Establish a **timeline**

- **Distinguish** between root cause and causal factors

**Phase 4: Post-Incident Review**

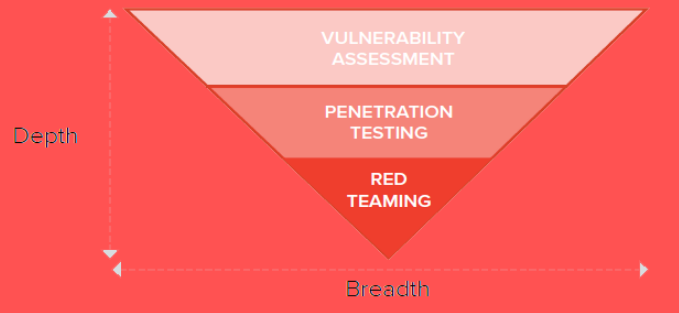
Investigation Status Report

* Discussed by IR Team
* Send to MGMT
* What all is given OK → Incident closed

**Phase 5: Update the Plan**

Hold a meeting with the IR Team and discuss what to improve

**Red Team**

****

**Project Initiation**

This describes the project, the target. The following operations are handled in this phase: *Scoping Meeting, Network/WebApp, WiFi, Physical, Social Engineering*, and also:

1. **Threat Modeling**
2. **Define Topics**
3. **Determine Schedule**
4. **Develop Attack Playbook**

**Recon Phase**

Includes Asset identification*,* and Social Engineering

1. **OSINT**

- Passive: No traffic to target  
- Semi-passive  
- Active: Enumeration, vulnerability scanning, unpublished directories,   
 reconnaissance

1. **Covert Observation**

- Physical security inspections  
- Wireless scanning  
- Dumpster diving/HUMINT

1. **Foot-printing**

- External information gathering  
- information gathering from external perspective  
- Port Scanning, Banner Grabbing, SNMP Sweeps, DNS Bruteforce, etc.  
- External: DNS lookups, WHOIS, DNS bruting  
- Internal: AD mapping, Port scanning,

1. **Identifying Protection Mechanisms**

- Network Based protections  
- Host based protections  
- Application Level protections  
- Storage protections  
- User Protections

**Compromise Target**

1. **Scanning**
2. **Penetrate Network and/or applications**
3. **Obtain credentials**
4. **Lateral Movement**
5. **Obtain trophies**

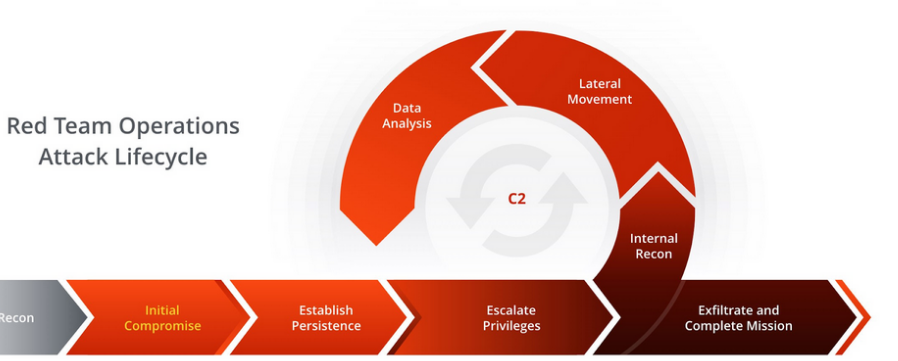
**Security Improvements**

1. **Share findings/weaknesses**
2. **Discuss improvements**
3. **Provide remediation guidance**

**Vulnerability Analysis**

Process of discovering flaws in systems and applications. Types: Active: automated application scans, banner grabbing, network scans. Passive: metadata analysis and traffic monitoring.

* Vulnerability identification
* Results analysis
* Risk Assessment
* Remediation & Implementation



**Post Exploitation**

**Purpose:** to determine the value of the machine compromised and to maintain control of the machine for later use. Value is determined by the sensitivity of the data stored on it, and the machines usefulness in further compromising the network

* Infrastructure Analysis
* Pilaging
* Data Exfiltration
* Persistence & Cleanup

**Reporting**

Technical Report includes: *Title, Description, Reproduction, Attack Vector/Payload, Exploitability, Impact, Recommendation(Optional), References (optional*

**Yellow Team**

1. Input Sanitization

2. Don't trust the client

3. Update your shit

**OWASP**

Proactie Controls

***C1: Define Security Requirements***

* OWASP Application Security Verification Standards (ASVS) = Statement of needed security functionality
* Misuse cases ↔ User stories
* Verifiable

***C2: Leverage Security Frameworks and Libraries***

* User libraries and frameworks from trusted sources
* Maintain inventory catalog
* Proactively keep up-to-fate
* Encapsulate library and expose only required behavior

***C3: Secure Database Access***

* Secure Queries
* Secure configuration
* Secure authentication
* Secure communication

***C4: Encode and Escape Data***

* Encoding: < becomes &lt
* Escaping: \”

***C5: Validate All Inputs***

* Logicallyy correct inputs (eg correct date format)

***C6: Implement Digital Identity***

* Level 1:Passwords
* Level 2: MFA
* Level 3: Cryptographic Based Authentication
* Session management

***C7: Enforce Access Controls***

* Deny by default
* Principle of Least privilege
* Log

***C8: Protect Data Everywhere***

* Encrypt in transit
* Encrypt @ rest
* Key/Secrets management

***C9: Implement Security Logging an Monitoring***

***C10: Handle All errors and Exceptions***

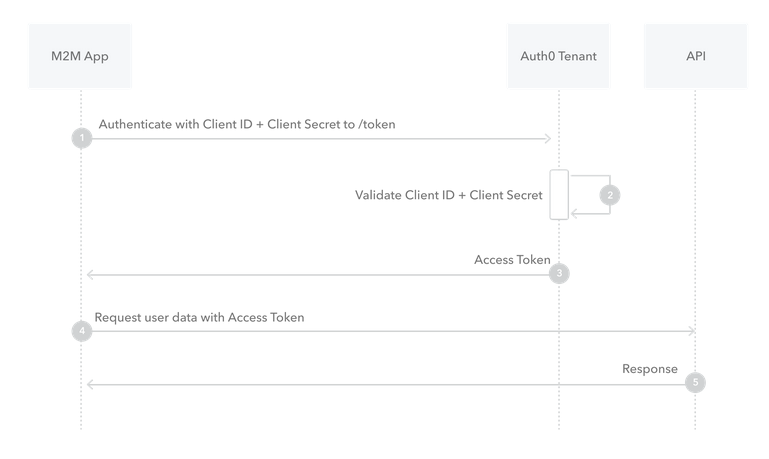
**OWASP top 10**

* Injection
* Broken Authentication
* Sensitive Data Exposure
* XML External Entities
* Broken Access Controls
* Security Misconfiguration
* XSS
* Insecure Deserialization
* Using Components with known vulns
* Insufficient Logging & Monitoring

**Oauth**

Client credentials

The Client Credentials Flow (defined in [OAuth 2.0 RFC 6749, section 4.4](https://tools.ietf.org/html/rfc6749" \l "section-4.4)) involves an application exchanging its application credentials, such as client ID and client secret, for an access token.

This flow is best suited for Machine-to-Machine (M2M) applications, such as CLIs, daemons, or backend services, because the system must authenticate and authorize the application instead of a user.

Here's a high-level overview of the OAuth process:

1. Client registration: The client (third-party application) registers itself with the authorization server and obtains a client identifier and a client secret. This registration step establishes trust between the client and the authorization server.
2. Authorization request: The client initiates the OAuth flow by redirecting the user (resource owner) to the authorization server. The request includes the client identifier, the desired scope of access, and a redirect URL to return the user after authentication.
3. User authentication and consent: The user is redirected to the authorization server's authentication page, where they enter their credentials to authenticate themselves. After successful authentication, the authorization server presents the user with a consent screen that explains the requested permissions and asks for their approval to grant access to the client.
4. Authorization grant: If the user consents, the authorization server issues an authorization grant (usually in the form of an access token) to the client. The authorization grant represents the user's consent to access their protected resources.
5. Access token request: The client sends a request to the authorization server, providing the authorization grant and its client credentials (client identifier and client secret).
6. Access token issuance: The authorization server validates the request and, if valid, issues an access token to the client. The access token is a credential that allows the client to access the protected resources on behalf of the user.
7. Resource access: The client includes the access token in subsequent requests to the resource server. The resource server verifies the access token's validity and permissions. If valid, the resource server provides the requested resources to the client.

OAuth is designed to be secure and allows users to control the level of access granted to third-party applications. It eliminates the need for sharing sensitive credentials and provides a standardized way for users to authorize application access to their resources.