



SOC - Security Operations Centre Framework Project



OWASP

The Open Web Application Security Project

<https://t.me/learningnets>



OWASP

The Open Web Application Security Project

- Modals & Strategies of SOC's
- Processes
- People & Skills



OWASP

The Open Web Application Security Project

- Centralized
- Distributed
- In-hose
- Constituency
- Managed
- Hybrid



OWASP

The Open Web Application Security Project

- One Team
- One Central Location
- Close to HQ
- Most Common
- Most Feasible
- 24x7



OWASP

The Open Web Application Security Project

- Multiple Teams
- May have Multiple sets of Dashboards
- Small Team in SOC & rest outside the SOC
- Follow the Sun vs 24x7



OWASP

The Open Web Application Security Project

- Within the organization
- **Pros:**
 - Dedicated staff
 - Knows environment better
 - Correlations between internal groups
 - Logs stored locally
- **Cons:**
 - Larger up-front investment
 - Pressure to show ROI
 - Hard to find competent staff



OWASP

The Open Web Application Security Project

- External SOC
 - UnManaged
 - No write access to security devices
 - Managed
 - Has write access to security devices



OWASP

The Open Web Application Security Project

- Active Access on Security Appliances as well
- **Pros:**
 - quick start with less Capex
 - reduced staff requirement including for managing Security Appliances
- **Cons:**
 - less environment knowledge
 - external data mishandling
 - external device mishandling
 - lack of archiving



- High level Centralized
- Focused Distributed
- **Pros:**
 - Sufficient Visibility across the environment
 - Quickest detection & Response Time
 - Reduced backlog
 - Intel sharing
- **Cons:**
 - Most costly
 - 3rd party handling



OWASP

The Open Web Application Security Project

- No authority
- Shared authority
- Full authority
- Situations of Containment
- Pre-agreements
- Reactive
- Proactive (pushing emergency patches)



OWASP

The Open Web Application Security Project

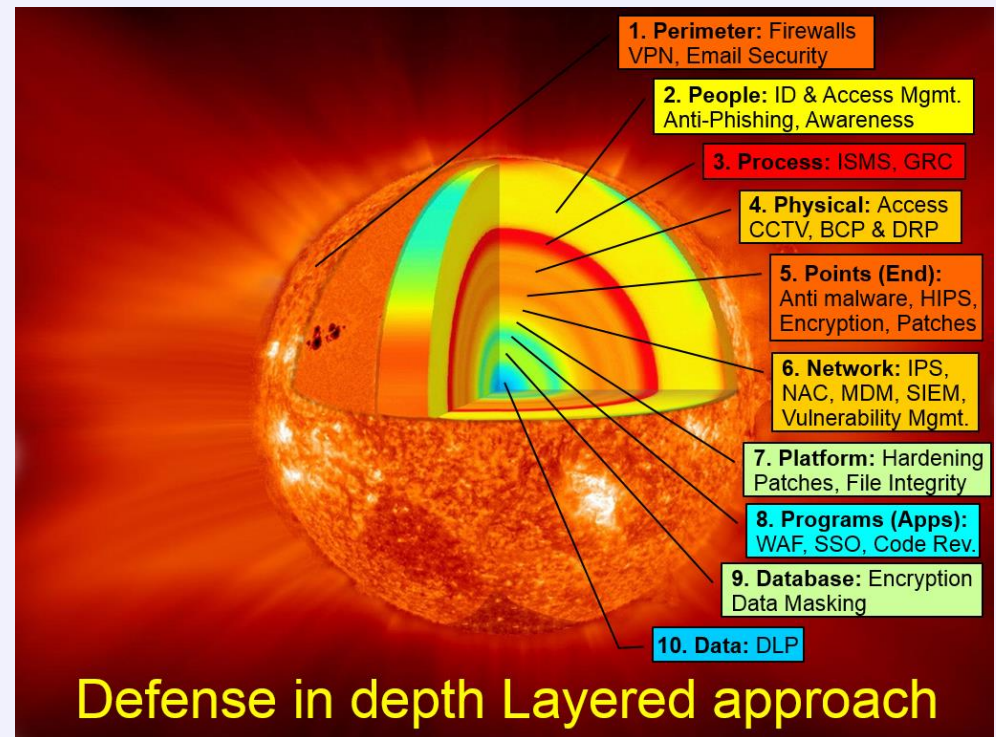
1. Monitoring and Detection
 - I. Identification
 - II. Correlation
 - III. Aggregation
 - IV. Retention
 - V. Scanning
 - VI. Monitoring
2. Incident response
 - I. Alerting
 - II. Incident management
 - III. Communication
3. Threat Intelligence
 - I. Threat hunting
 - II. Intelligence collection
 - III. Vulnerability management
4. Quality Assurance
 - I. Optimization
 - II. Tuning and Maintenance
 - III. Metrics



OWASP

The Open Web Application Security Project

- What, Where, How much
- Asset Management
- Risk Management
- Supported Devices
- Licenses, EPS
- Storage





OWASP

The Open Web Application Security Project

- Prime objective - Incident tracking
- Timestamp
- Time synchronization
- Real-time correlation
- Includes:
 - Filtering
 - Aggregation
 - De-duplication
- Custom Rules



OWASP

The Open Web Application Security Project

- Normalization
- Storage Usage
- Evidence preservation
- Deduplication



OWASP

The Open Web Application Security Project

- Active data for analysis
- Archived data
- Investigation
- Compliance requirements
- Storage Capacity Management
- Access especially Admin



OWASP

The Open Web Application Security Project

- Subscription to other SoCs
- Automated
- Manual Advisories
- Collections
 - IOC, IOA, TTP
- Analysis & Assessment
- Applicability
- Distribution
- Creation
- External Feed
- OSINT



- Network Mapping (size, shape, makeup, and perimeter interfaces)
 - Automated & Manual
- Vulnerabilities
- Passive Fingerprinting (to avoid disruptions due to scanning)
- Correlation of events related to Vulnerable Services



OWASP

The Open Web Application Security Project

- Real-time
- Network Monitoring - Net Flows
- Perimeter
- Configuration
- Critical Files changes
- Privileged use
- IDS/IPS
- 24/7 Shift Schedules
- Follow the sun
- UBA/UEBA



OWASP

The Open Web Application Security Project

- For Prompt Action
- Focused teams involvement
- Rules building
- Actions against alerts
- Ticketing system integration
- Workflow management



OWASP

The Open Web Application Security Project

- a) Detection
- b) Analysis
- c) Prioritization
- d) Response
- e) Containment
- f) Eradication
- g) Recovery
- h) Forensic Investigation
- i) Learning



OWASP

The Open Web Application Security Project

- What, Where, How much
- IDS/IPS, SIEM, log management tools, AV
- Misuse or signature-based detection
- Anomaly detection
- IOCs, IOAs & TTP



OWASP

The Open Web Application Security Project

- Who, what, when, where, and why of an intrusion
- Must be time constrained
- How to limit damage
- How to recover
- Malware Implant (Reversing)
 - De-compilation (Static code)
 - Detonation (thru runtime execution)
- Documented
- Recommendation for further action



OWASP

The Open Web Application Security Project

- Based on Impact
- For Example:
 - Level 1 Incidents that could cause significant harm
 - Level 2 Compromise of or unauthorized access to noncritical systems or information
 - Level 3 Situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel



- Action to deter, block, or cut off
- Eradication/ Remediation
- Manual
- Automated
- Active
- Passive
- On-site & Remote
- E.g. firewall blocks, DNS black holes, IP blocks, patch deployment, and account deactivation.
- Creation of signature



OWASP

The Open Web Application Security Project

- 1st Action
- Isolation of incident so it doesn't spread & cause further damage
- Disconnection of affected devices from Network & Internet
- Short term & long term containment Strategies
- **Questions to address**
 - What's been done to contain the breach short term?
 - What's been done to contain the breach long term?
 - Has discovered malware been quarantined from the environment?
 - What sort of backups are in place?



OWASP

The Open Web Application Security Project

- Eliminate the root cause of incident
- E.g. removal of Malware
- Complete removal of malware
- **Questions to address**
 - Have malware been securely removed?
 - Has the system be hardened, patched, and updates applied?
 - Can the system be re-imaged?



- to a known good state
- Based on priority
- Need of Evidence Preservation
- Systems up and running again without the fear of another breach
- **Questions to address:**
 - When systems can be returned to production?
 - Have systems been patched, hardened and tested?
 - Can the system be restored from a trusted back-up?
 - How long will the affected systems be monitored and what will you look for when monitoring?
 - What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc)



OWASP

The Open Web Application Security Project

- Unearthing ground truth of an incident
- Establishing a detailed timeline of events
- Gathering and storing artifacts e.g. storage media
- For legal proceedings
- Jurisdiction
- Documenting chain of custody
- bit-by-bit copies of evidence



OWASP

The Open Web Application Security Project

- Root cause analysis
- Preventive controls to avoid reoccurrence
- Post incident meeting with all Team members
- Documented
- what worked well, and were there some holes
- Custom Signature Creation, Validation and Distribution
- **Questions to address:**
 - What changes need to be made to the security?
 - How should employee be trained differently?
 - What weakness did the breach exploit?
 - How will you ensure a similar breach doesn't happen again?



OWASP

The Open Web Application Security Project

- KPIs
- SLA
- MTTD
- MTTR
- E.g.:
 - Response Time
 - No of Incidents
 - Pro Active – Lead Time to Patch Vulnerabilities
 - No of False Positives



OWASP

The Open Web Application Security Project

- Within SOC
- Internal
- External
- Alternative Channels
- Call centre, Email messages, Phone calls, Walk-in reports
- SOC website
- Cyber tip feeds (from other SOCs)
- SOC can't afford to miss tips
- Post incident communication



OWASP

The Open Web Application Security Project

- Segregation of Duties
- Access to Admins
- Artificial Intelligence is not a substitute
- SOC Analyst
- Incident Handler
- SOC Expert
- SOC Manager



OWASP

The Open Web Application Security Project



For more information, queries, feedback and updates:

[OWASP Security Operations Center \(SOC\) Framework Project](#)

<https://t.me/learningnets>

