OWASP 2025 GLOBAL AppSec

BARCELONA

CENTRE DE
CONVENCIONS
INTERNACIONAL DE
BARCELONA

OWASP 2025 GLOBAL AppSec | BARCELONA MAY 26-30

Pluggable DevSecOps for free, using community resources

Spyros Gasteratos

The OWASP superpower

The world’s best security resources: 200+ projects

- Maturity Standards, Controls frameworks
- Top 10s
- CheatSheets,
- Posture Management
- SBOMs, SCA
- WAFs

The drawback

- You can’t focus on everything at the same time
- Each team needs to do one thing very well
- But this creates the Dreaded Silos
- Silos require expensive manual work to unify

Manually connecting silos?
Think again!

Let’s Solve this
Because all of us are affected

Nice to meet you

- Spyros Gasteratos
  - OWASP Volunteer
  - OpenSource dev
  - Founder – smithy.security

Nice to meet you

- Spyros Gasteratos
  - OWASP Volunteer
  - OpenSource dev
  - Founder – smithy.security

Itinerary

- Problem Breakdown
- Information Unification
  - SARIF
  - OCSF
- Execution Unification
  - Rules of translation
  - Orchestration
  - Taming the Chaos
  - Workflows
- Scenario
- Future ideas
- Questions

Breakdown

- Unify information
- Unify execution
- Translate business processes to automated execution

Unify Information

- A singular way of representing that “something” is related to AppSec
- Open Source standards to the rescue
- SARIF
- OCSF

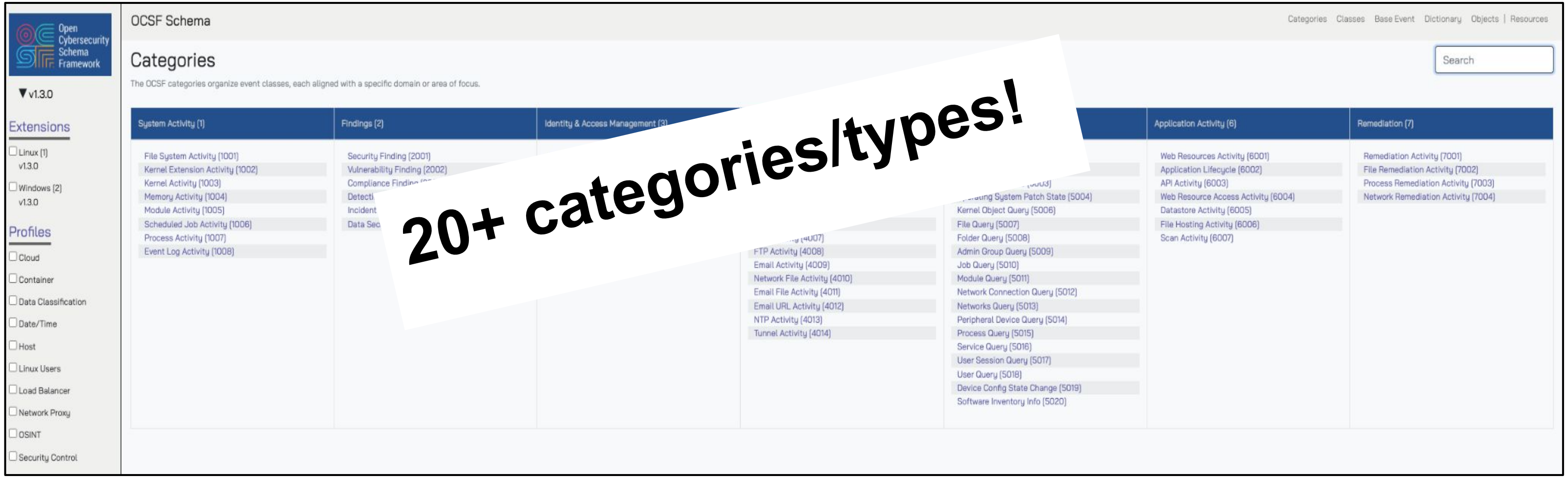
SARIF (Static Analysis Results Interchange Format)

- Open Source Standard for SAST
- Pros:
  - Vendors Support – Github
  - Human and machine readable – JSON
  - Supports evidence and traces
- Cons:
  - support MOSTLY SAST vendors
  - weak schemas
  - vendor dialects
  - a lot of arbitrary data fields

OCSF (Open Cybersecurity Schema Framework)

- Security agnostic schemas
- Pros:
  - SAST++++
  - Schemas AND tools (JSON, Protobuf)
  - More expressive than SARIF
  - Extensible
- Cons:
  - Designed by committee
  - Tools STILL don’t map the same way
  - Steep learning curve
  - Footgun

OCSF



Open Cybersecurity Schema Framework

▼v1.3.0

Extensions

□ Linux (1) v1.3.0

□ Windows (2) v1.3.0

Profiles

□ Cloud

□ Container

□ Data Classification

□ Date/Time

□ Host

□ Linux Users

□ Load Balancer

□ Network Proxy

□ OSINT

□ Security Control

OCSF Schema

Categories | Classes | Base Event | Dictionary | Objects | Resources

Categories

Search

The OCSF categories organize event classes, each aligned with a specific domain or area of focus.

System Activity (1)

- File System Activity (1001)
- Kernel Extension Activity (1002)
- Kernel Activity (1003)
- Memory Activity (1004)
- Module Activity (1005)
- Scheduled Job Activity (1006)
- Process Activity (1007)
- Event Log Activity (1008)

Findings (2)

- Security Finding (2001)
- Vulnerability Finding (2002)
- Compliance Findin
- Detecti
- Incident
- Data Sec

Identity & Access Management (3)

- (4007)
- FTP Activity (4008)
- Email Activity (4009)
- Network File Activity (4010)
- Email File Activity (4011)
- Email URL Activity (4012)
- NTP Activity (4013)
- Tunnel Activity (4014)

- (5003)
- rating System Patch State (5004)
- Kernel Object Query (5006)
- File Query (5007)
- Folder Query (5008)
- Admin Group Query (5009)
- Job Query (5010)
- Module Query (5011)
- Network Connection Query (5012)
- Networks Query (5013)
- Peripheral Device Query (5014)
- Process Query (5015)
- Service Query (5016)
- User Session Query (5017)
- User Query (5018)
- Device Config State Change (5019)
- Software Inventory Info (5020)

Application Activity (6)

- Web Resources Activity (6001)
- Application Lifecycle (6002)
- API Activity (6003)
- Web Resource Access Activity (6004)
- Datastore Activity (6005)
- File Hosting Activity (6006)
- Scan Activity (6007)

Remediation (7)

- Remediation Activity (7001)
- File Remediation Activity (7002)
- Process Remediation Activity (7003)
- Network Remediation Activity (7004)

20+ categories/types!

Itinerary

- ~~Problem Breakdown~~
- ~~Information Unification~~
  - ~~SARIF~~
  - ~~OCSF~~
- Execution Unification
  - Rules of translation
  - Orchestration
  - Taming the Chaos
  - Workflows
- Scenario
- Future ideas
- Questions

OCSF is the Vocabulary – Where is the Grammar?

- SMITHY – SDK
- The only Open Source SDK for OCSF. – Golang – For now
- Plug n Play
- Focus on writing business logic
- Translate $tool -> OCSF
- Advanced capabilities

Orchestration Challenges

- Running security tools reliably not trivial
- Leveraging common knowledge is hard
- Not straightforward feedback loops

Taming the Chaos

- SMITHY – Workflows
- The Open Source AppSec workflow engine
- Orchestrate and Normalize
- Enrich and Filter
- Report
- Component Reusability and Registry

Taming the Chaos

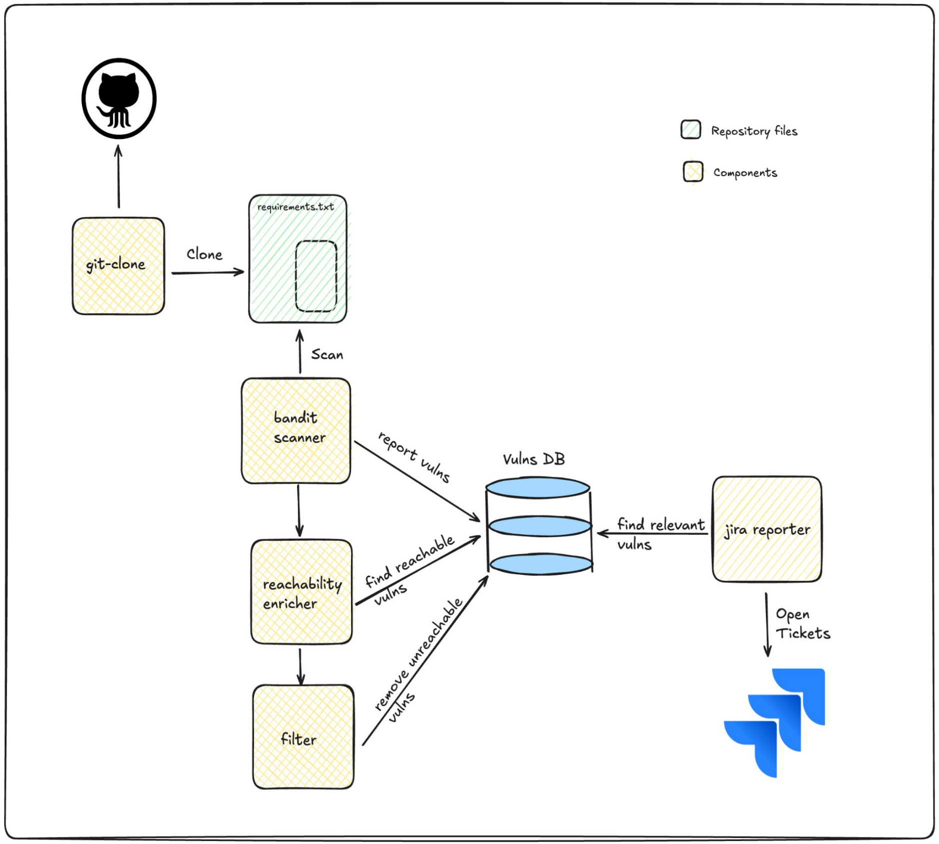
- Standardise tools execution and implementation
- Automatic instrumentation:
  - Metrics
  - Logs
  - Traces
  - panic handling
- Centralized AppSec Datalake

Not impacting on production CI pipelines

Workflows

- Define component execution order and configuration

- Configurable via yaml or CLI



Itinerary

- ~~Problem Breakdown~~
- ~~Information Unification~~
  - ~~SARIF~~
  - ~~OCSF~~
- Execution Unification
  - Rules of translation
  - Orchestration
  - Taming the Chaos
  - Workflows
- Scenario
- Future ideas
- Questions

Scenario: Sole AppSec in new Org

- No team
- No budget
- Not doomed – just feed off the land – use existing resources and orchestrate

A complete AppSec programme

- Strategy
- Controls
- Observability
- Data Centralization and understanding
- Culture and Awareness

Strategy

- SAMM
- Lightweight
- Verbose enough with levels
- Easy to follow questionnaire
- Automated tracking? – Smithy

A complete AppSec programme

- ~~Strategy~~
- Controls
- Observability
- Data Centralization and understanding
- Culture and Awareness

Controls

- ASVS and/or DSOMM
- Checklist for secure design and automation
- How do we know who is failing ASVS controls?

A complete AppSec programme

- ~~Strategy~~
- ~~Controls~~
- Observability
- Data Centralization and understanding
- Culture and Awareness

Observability

- Running tools has never been easier
- DepScan, CDXGen, Syft and SAST or DAST
- Routing findings where they should live.
  - Jira/Linear
  - Slack/Discord
  - DefectDojo/Any ASPM out that door
  - Dependency Track

A complete AppSec programme

- ~~Strategy~~
- ~~Controls~~
- ~~Observability~~
- Data Centralization and understanding
- Culture and Awareness

Data Centralization and understanding

- Reprioritisation and false positives?
- Filters!

A complete AppSec programme

- ~~Strategy~~
- ~~Controls~~
- ~~Observability~~
- ~~Data Centralization and understanding~~
- Culture and Awareness

Culture and Awareness

- Custom Training
- Agile Advice

More automation ideas

- Threat modeling (semi-generated) STRIDE-GPT, Threat Dragon, or PyTM
- Run on events.

Pitfalls

- Not using open standards and SDKs
- Raw Data dumping in human - focused fields
- Not being strict about original tool info – less is more
- Relying only on AI mappings

Closing

- Standing on the shoulders of giants
- The community power – tools and resources waiting to be put together.
- If you publish code or docs, thank you.

To Recap

- Community resources FTW!
- Dirty Scripts and manual orchestration doesn’t scale
- **Interoperability**: The only way to do security is Open Standards
- **Short Feedback loops**: Fast and flexible integrations
- Smithy can help you

Thank you for your attention and support

Slides:

Smithy – give us a star?: https://github.com/smithy-security/smithy

Thank you