



OWASP  
**AppSec Europe**  
London 2nd-6th July 2018

# Regular to Enterprise-Ready Apps with Cybersecurity APIs

For Cloud, Apps, Services and Infrastructure

Ovidiu CICAL – [ovidiu.cical@gmail.com](mailto:ovidiu.cical@gmail.com)





## What's going to happen in the upcoming minutes?

- ✓ Present some API Categories
- ✓ Available Open Source, Free and Paid solutions
- ✓ Dive into
  - Vulnerability Scanning & Web Apps Security
  - Threat Intrusion Detection & Prevention
  - Data Loss Prevention APIs – DLP
- ✓ Short demo of popular Open Source Slack & Dropbox alternatives
- ✓ Q&A



## Why APIs? Self-protecting apps; they know the data

### Security of data at its source

Advanced data security, data loss prevention, data classification, user behavior, vulnerability awareness etc.

Can be added to:

-  Desktop application
-  Web applications
-  Mobile apps
-  Servers or Infrastructure
-  Cloud
-  IoT devices

### No more proprietary formats

No better perspective than the one collected from the software generating and using it.

It knows:

- The format
- The content
- The importance
- Its origin and the destination

# Cybersecurity API Categories

Quite a few...





## API Categories

- Identity and Access Management - IAM
- Web Applications / Web Services Security
- Vulnerability Scanning APIs
- Threat Intrusion/Detection, Behavior Anomaly Detection
- Data Loss Prevention – DLP
- Endpoint Security
- Containerized Environments Security
- Public, Private and Hybrid Cloud Infrastructure Security
- many more...

## Vulnerability Scanning

---

- OWASP Vulnerability Scanning Tools List
- OWASP Zed Attack Proxy (ZAP) - Free
- <https://pentest-tools.com> - Freemium
- Burp Suite
- Accunetix Free
- Qualys FreeScan
- SUCURI Free
- UpGuard Web Scan, Tenable, Rapid7 ...

## Threat detection/prevention

---

- AlienVault Open Source SIEM (OSSIM)
- Suricata Intrusion Detection/Prevention
- OSSEC
- OPSWAT
- Snort IPS
- Security Onion
- Fail2ban ...

## IAM APIs

---

- OpenIAM – Community Edition
- Keycloak – Open Source
- Soffid – Open Source
- OneLogin, OKTA
- Amazon AWS
- Google IAM
- Microsoft AD ...

## Web Apps/Code Security

---

- OWASP – Follow Top 10 lists
- OWASP SonarQube – 20+ languages
- OWASP Orizon – Mostly Java
- Bandit – Python code analysis - Free
- w3af.org, Kali Linux + Nikto
- Contrast Security, Kiuwan, Puma Sec
- Fortify - HP...

## Infrastructure/Cloud/Server Security

---

- Let's Encrypt free SSL Certificates - Free
- Qualys SSL Labs (server, browser tests) - Free
- CloudStack - Free
- Kali Linux
- Metasploit
- HPE ConvergedSystem
- ...

## Container Security

---

- Peekr from Aqua Security
- Platform9
- Twistlock
- Red Hat Atomic Scan
- Clair from CoreOS
- ...

# Vulnerability Scanning & Web Apps Security

Know your weaknesses





## Vulnerability Scanning & Web Apps/Code Security



OWASP ZAP



Burp Suite



Nikto

The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools.

Graphical tool for testing Web application security, written in Java and developed by PortSwigger

Leading web vulnerability scanner used by Fortune 500 companies as the most advanced SQL injection and XSS black box scanning technology.

The leading product for Continuous Code Quality.

Webserver scanner for potentially dangerous files, outdated versions of servers, etc.

### Features:

- Identify the very latest vulnerabilities
- Cutting-edge scanning technology
- Intercept Proxy
- Brute Force
- Fuzzer
- Automated Scanner
- REST API

### Features:

- Automated Crawl & Scan
- Details about vulnerabilities
- Intercept browser traffic
- Burp Extender API

### Features:

- Vulnerability Scanner
- High detection rate
- Lowest false-positives
- Network security
- Wordpress checks
- Manual testing tools

### Features:

- 20+ languages - Java, Javascript, C#, C/C++, Python, PHP, COBOL, Swift/Obj-C...
- Continuous inspection
- Detect tricky issues
- DevOps Integration

### Features:

- 6700+ dangerous files/programs
- 1250+ outdated servers versions
- SSL Support
- Template engine for custom reporting






# Threat Intrusion Detection & Prevention

Know your traffic



## Threat Intrusion Detection & Prevention

		
<p>Suricata is a free and open source, mature, fast and robust network threat detection engine.</p>	<p>Open source intrusion &amp; prevention system offered by Cisco. Capable of real-time traffic analysis and packet logging on IP networks.</p>	<p>AlienVault OSSIM:  The World's Most Widely Used Open Source SIEM</p>
<p>Features:</p> <ul style="list-style-type: none"> <li>✓ IDS / IPS API</li> <li>✓ High Performance</li> <li>✓ Automatic protocol detection</li> <li>✓ Industry standard outputs</li> <li>✓ YAML &amp; JSON Web API</li> </ul>	<p>Features:</p> <ul style="list-style-type: none"> <li>✓ Most widely deployed IDS in the world</li> <li>✓ 600,000+ Registered users</li> <li>✓ Real-time traffic analysis</li> <li>✓ Protocol analysis</li> <li>✓ Content searching/matching</li> </ul>	<p>Features:</p> <ul style="list-style-type: none"> <li>✓ Asset discovery</li> <li>✓ Vulnerability assessment</li> <li>✓ Intrusion detection</li> <li>✓ Behavioural monitoring</li> <li>✓ SIEM event correlation</li> <li>✓ JSON Web API</li> </ul>

# Data Loss Prevention (DLP) APIs

Know your data





## Data Loss Prevention DLP APIs – Free Solutions

### MyDLP



#### Pro:

- ✓ Open Source
- ✓ DLP API
- ✓ Data Discovery
- ✓ Remote Storage (CIFS, SMB, NFS, FTP etc.)
- ✓ AD Integration
- ✓ Self-hosted

#### Cons:

- Rarely updated
- Small community

### Dhound







#### Pro:

- ✓ Free for 1 Server
- ✓ More than DLP
- ✓ DLP API
- ✓ Threat Discovery
- ✓ Intrusion Detection
- ✓ Alerting

#### Cons:

- Not a pure DLP API Solution
- Move to Enterprise edition for more features

## Data Loss Prevention DLP APIs - Vendors

<p>Google Cloud DLP API</p> 	<p>Amazon Macie – DLP</p> 	<p>Microsoft Office 365 DLP</p> 	<p>Sensitivity.io</p> 	<p>Nucleuz CloudLock Symantec etc.</p>
<p>Pro:</p> <ul style="list-style-type: none"> <li>✓ Classify, Discover and Report</li> <li>✓ Redact it</li> <li>✓ Replace/Mask it</li> </ul>	<p>Pro:</p> <ul style="list-style-type: none"> <li>✓ Data visibility</li> <li>✓ Automation with advanced ML</li> <li>✓ Alerting</li> </ul>	<p>Pro:</p> <ul style="list-style-type: none"> <li>✓ Office 365 data visibility</li> <li>✓ Covers all of Office 365 apps</li> </ul>	<p>Pro:</p> <ul style="list-style-type: none"> <li>✓ Works <b>fully offline</b></li> <li>✓ Windows, Mac, Linux</li> <li>✓ Cloud API (SaaS)</li> <li>✓ Redact/Mask/Classify</li> <li>✓ Always Up2Date Policies</li> </ul>	<p>Pro:</p> <ul style="list-style-type: none"> <li>✓ Specific for apps</li> <li>✓ Office suite plugins</li> <li>✓ Outlook plugins</li> <li>✓ Windows support</li> </ul>
<p>Cons:</p> <ul style="list-style-type: none"> <li>○ Works only Online, using Google Cloud infrastructure and processing power</li> <li>○ Costly with high usage</li> </ul>	<p>Cons:</p> <ul style="list-style-type: none"> <li>○ AWS S3 only, no API</li> <li>○ High cost when classifying large datasets</li> </ul>	<p>Cons:</p> <ul style="list-style-type: none"> <li>○ Work with Office 365 online and offline</li> <li>○ Cannot be used by external apps or services</li> </ul>	<p>Cons:</p> <ul style="list-style-type: none"> <li>○ No free edition</li> </ul>	<p>Cons:</p> <ul style="list-style-type: none"> <li>○ Small set of apps supported</li> <li>○ Cannot be used by external services</li> </ul>

## DLP APIs – What do I get?

- ✓ Minimal development effort -> a few days
- ✓ Build POCs or Production ready solutions in days
- ✓ Leverage many pre-built policies to detect and control sensitive data

Hundreds of out-of-the-box policies for

- **Email** (ovidiu.cical@gmail.com)
- **Credit Card** (Mastercard, VISA, Amex, JCB, etc.)
- **IBAN** (GB29NWBK60161331926819)
- **SSN** Social Security Number (UK, US, JP +20 more)
- **Passport** (10+ Countries)
- **Driver's License**
- **Health Insurance Number**
- **ID Card** (40+ Countries)
- **Phone Number**
- **Tax ID**
- Foreign Registration Number
- **Address**
- Dates
- Custom Dictionaries
- Custom Regexprs
- Office Files
- Graphic Files
- Media Files
- Archive Files
- Programming Files
- Other File types

- ✓ Compliance for HIPAA, PCI DSS, GDPR, FISMA, SOX, FERPA, GLBA, etc.
- ✓ Always up-to-date Compliance and Predefined Protection Profiles



## Examples Text Processing using an API

### Redaction - removal

Redaction removes text where it matches sensitive data

Hi Carlos, can you please have your credit card sent at `carlos.doe@greatest.com`? I tried registering with my SSN `849-12-1958` and this card `5500-0001-6268-3365`

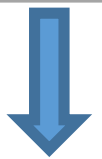


Hi Carlos, can you please have your credit card sent at `*****@*****`? I tried registering with my SSN `**-**-****` and this card `****-****-****-****`

### Masking

Apply full or partial masking on found threats

...credit card sent at `carlos.doe@greatest.com`. I tried registering with my SSN `849-12-1958` and this card `5500-0001-6268-3365`



...credit card sent at `ca****.***@gr*****.com`. I tried registering with my SSN `**-**-1958` and this card `****-****-****-3365`

### Tokenization (Encryption)

Apply tokens on found threat and make the data unreadable without the key

...credit card sent at `carlos.doe@greatest.com`. I registered with my SSN `849-12-1958` and this card `5500-0001-6268-3365`



`text.Tokenize("91e8e0985d8d0cc3")`

...credit card sent at `6Z2B!2^3*6bT_938Bx`. I registered with my SSN `kh[?eK+7S:8x6!]A` and this card `p958|*6|465A-e_8|X`

### Identification removal

Remove identifying information

Details	Contact
Call at 541-754-3010	543-754-3010
Email: <a href="mailto:ovidiu@sensitivity.io">ovidiu@sensitivity.io</a>	121-614-9554
CNP: 1871123070077 (invalid)	346-184-5748
IBAN: GB82WEST12345698765432	129-443-4986
MASTERCARD: 5500-0001-6268-3365	628-788-2474



Details	Contact
Call at <code>**1-**-4-3010</code>	<code>**3-**-4-3010</code>
Email: <code>ov****@se*****.io</code>	<code>**1-**-4-9554</code>
CNP: 1871123070077	<code>**6-**-4-5748</code>
IBAN: <code>**82**ST**34**9876****</code>	<code>**9-**-3-4986</code>
MASTERCARD: <code>****-****-****-3365</code>	<code>**8-**-8-2474</code>

## Examples automatic remediation actions

- ✓ Report to a logging or SIEM solution
- ✓ Block the data
- ✓ Quarantine it to a safe location
- ✓ Encrypt it using company keys or PKI
- ✓ Inform the user about the sensitive content
- ✓ Allow with justification - by a manager
- ✓ Reroute content to be later inspected and approved
- ✓ Delete it from the source or in transit

## Key features of DLP Cybersecurity APIs



### Compliance with InfoSec regulations

Protection profiles for compliance with UK DPA, PCIDSS, HIPAA, GDPR, FISMA, GLBA, and many more!



### Baked-in DLP

Add DLP capabilities into any app – mobile, desktop or cloud-based and even infrastructure and servers.

### UK DPA

The Data Protection Act 2018 controls how your personal information is used by organizations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

### HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a set of standards created to safeguard protected health information (PHI) by regulating healthcare providers.

### GDPR

The EU General Data Protection Regulation (GDPR) is designed to protect the privacy of EU residents. With Cybersecurity APIs policies, you can cover an important part of the audit, tracking and reporting of transferred data outside the company.

### PCI-DSS

The Payment Card Industry Data Security Standard is a set of security standards designed to ensure that ALL companies that store, process or transmit cardholder data and/or sensitive authentication data maintain a secure environment.



## Use Cases for DLP Cybersecurity APIs



### Mobile Apps

Protect your mobile apps against data leakage and theft and stay compliant using mobile DLP SDKs (iOS or Android) or by leveraging cloud-based DLP API.



### Online backup, sync & file sharing

Make sure all data stored in your backup and file sharing solution is compliant with security policies and industry regulations. Scan and detect policy violations.



### Content inspection - Compliance

Data in e-mail, cloud file sharing, web browser, cloud services and other apps or services can be scanned to detect confidential information and further actions can be taken to prevent data breaches.



### Discovery and data classification (for DPO)

Deploy powerful sensitive data scanners to your cloud apps, discover and monitor content for threats and get instant alerts when your valuable data oversteps your protection policies.

## Example app with DLP Cybersecurity APIs - Slack

- ✓ Slack will get more acceptance in the enterprise space
- ✓ Needs security features such as Vulnerability Scanning, Encryption, Discovery of sensitive data and DLP capabilities

Possible solutions to get there:

- Cumbersome and complicated OEM (costly, huge integration effort)
- In-house development (thousands of hours)
- Outsource to specialized company – costly, had to manage
- ✓ ... or Cybersecurity APIs

 slack + Cybersecurity APIs = DLP Enterprise-ready in 3-7 days development time



## Request

```
1
2 // Create new sensitivity.io HTTP(s) Client
3 sensitivityioClient := utils.NewSIOClient()
4
5 // Set client options
6 sensitivityioClient.AuthKey = "2a3bfe54a162466fba13ec1ac3b001a5"
7 sensitivityioClient.AccountId = "974df9c4cdc25b30"
8 sensitivityioClient.ProjectId = "f9c4cdc2"
9 sensitivityioClient.AppId = "b6fded054928cad8"
10 sensitivityioClient.PrepareHeaders()
11
12 // Prepare file for upload
13 file, _ := utils.ReadFile("/path/to/confidential_file.txt")
14
15 // Send file to sensitivity.io Cloud Engine
16 if resp, err := sensitivityioClient.PostFiles(&UploadData{
17     InContext: true, // scan X chars of context
18     ContextSize: 100, // context set to 100 chars around
19     StopAtFirst: false, // stop scan if threat is found
20     StopAt: 10, // stop when threshold is reached
21     Files: file, // file content
22     MaskResult: "random", // mask random results
23     Surrounding: 20, // display text around found threat
24 }); err != nil {
25     http.Error(w, err.Error(), http.StatusForbidden)
26 } else {
27     resp.PrepareResponse()
28     // Print JSON Response
29     w.Write([]byte(model.ThreatResultsToJson(resp)))
30 }
31
```

## Response

```
1
2 {
3     "threat_results": [
4         {
5             "total": 4,
6             "elapsed": 92867,
7             "elapsed_text": "0.093ms",
8             "threat_index": 65,
9             "threats": [
10                {
11                    "type_name": "phone-number/us",
12                    "type_id": 52,
13                    "matched_text": "+1 888 271 9349",
14                    "surrounding": "...her a call at +1 888 271 9349, but no lat...",
15                },
16                {
17                    "type_name": "credit-card/mastercard",
18                    "type_id": 14,
19                    "matched_text": "****-****-****-5100",
20                    "surrounding": "..company CC ****-****-****-5100, make sure Bri...",
21                },
22                {
23                    "type_name": "e-mail",
24                    "type_id": 11,
25                    "matched_text": "ov****@do****.io",
26                    "surrounding": "...unable at ov****@do****.io. Call me lat...",
27                },
28                {
29                    "type_name": "ssn/us",
30                    "type_id": 15,
31                    "matched_text": "721-12-1234",
32                    "surrounding": "...this ssn 721-12-1234 allows creating...",
33                }
34            ]
35        }
36    ]
37 }
```



## Works everywhere

Plug into any application



On any operating system



On your favorite cloud platform



## Examples



**Mattermost**



nextcloud

# Thank you!

Ovidiu CICAL – [ovidiu.cical@gmail.com](mailto:ovidiu.cical@gmail.com)

