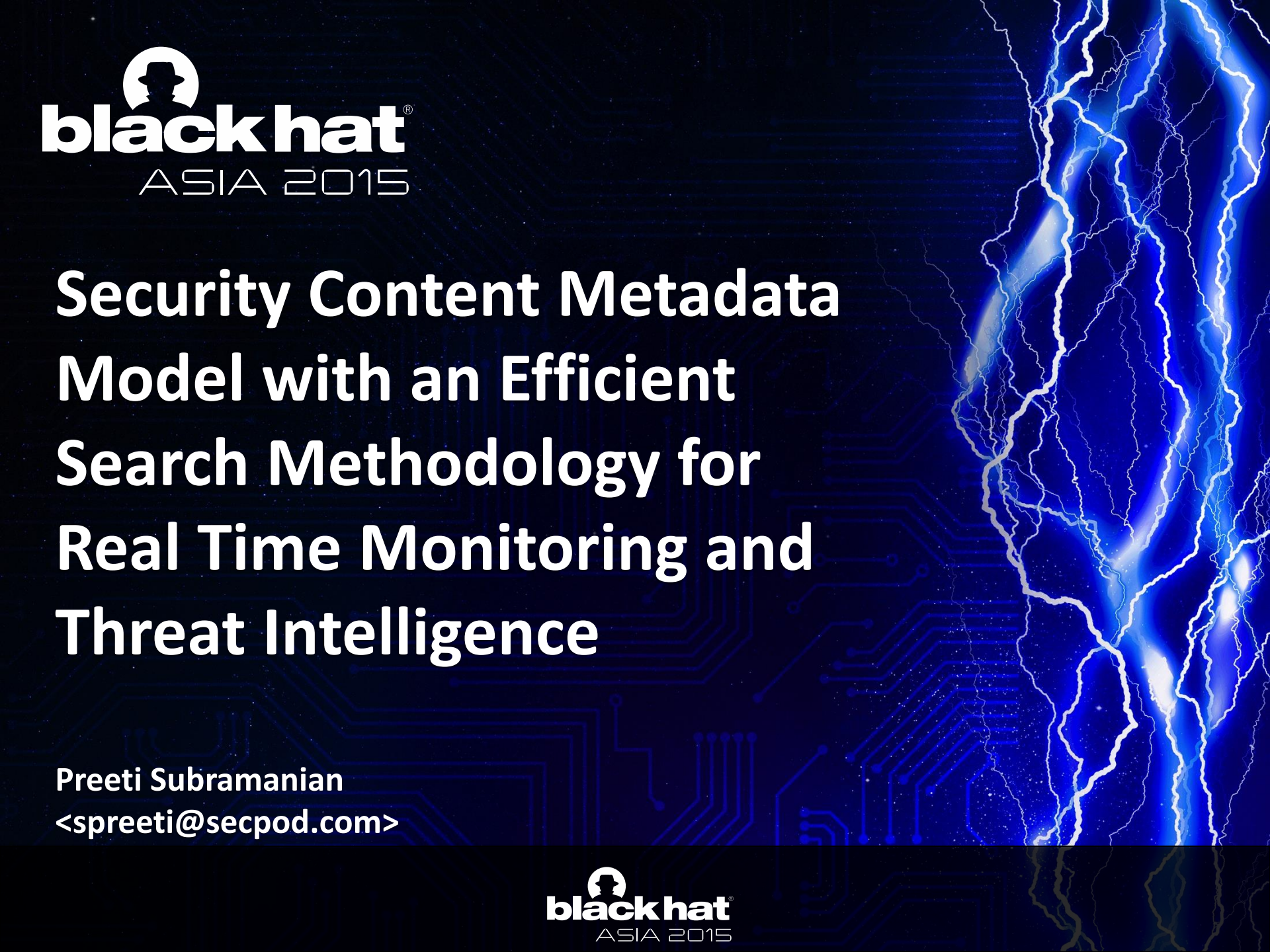


Security Content Metadata Model with an Efficient Search Methodology for Real Time Monitoring and Threat Intelligence

Preeti Subramanian
<spreeti@secpod.com>

black hat
ASIA 2015

Who am I?

Preeti Subramanian

from

working as Software Architect at secpod

Roadmap

Issues in datasets used by security products

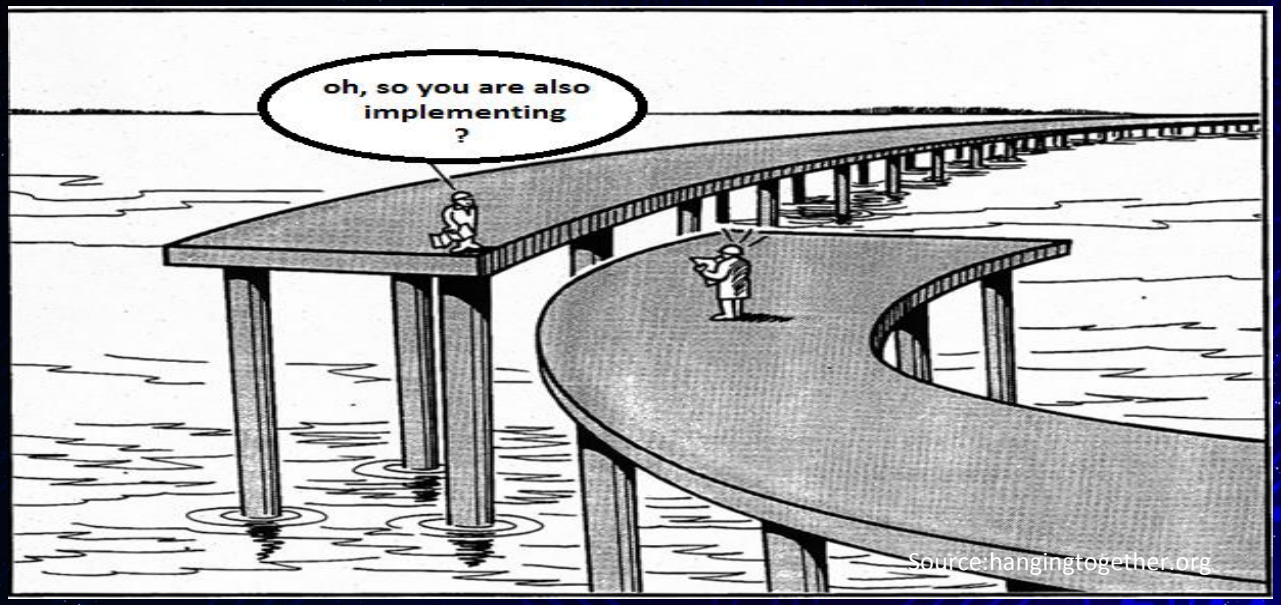
SCAP and other standards

What is Metadata Model?

How to use this metadata?

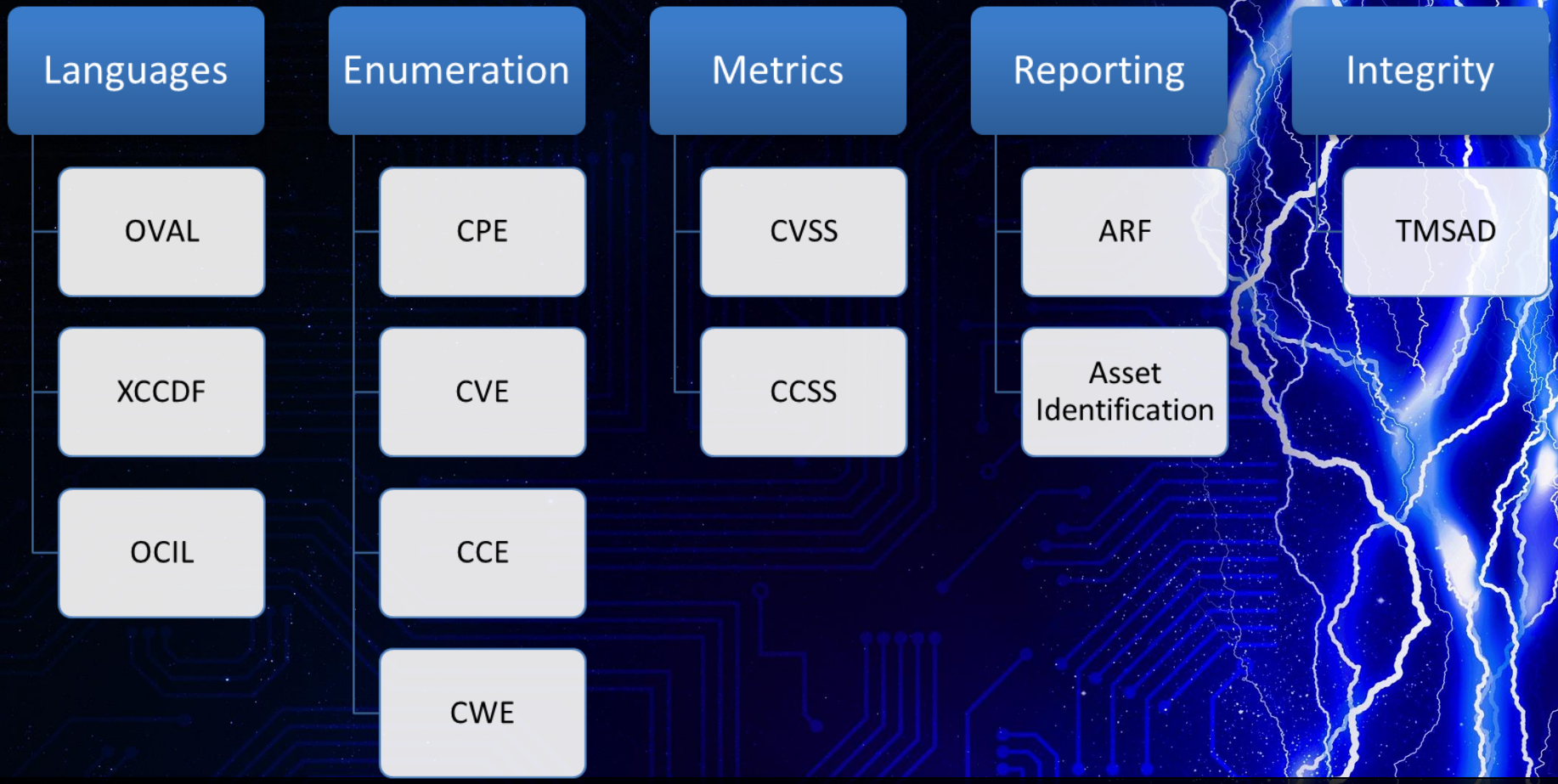
Real Time Monitoring and Threat Intelligence

Why is there a lack of commonality or inter-relationship between data sets of different security products?

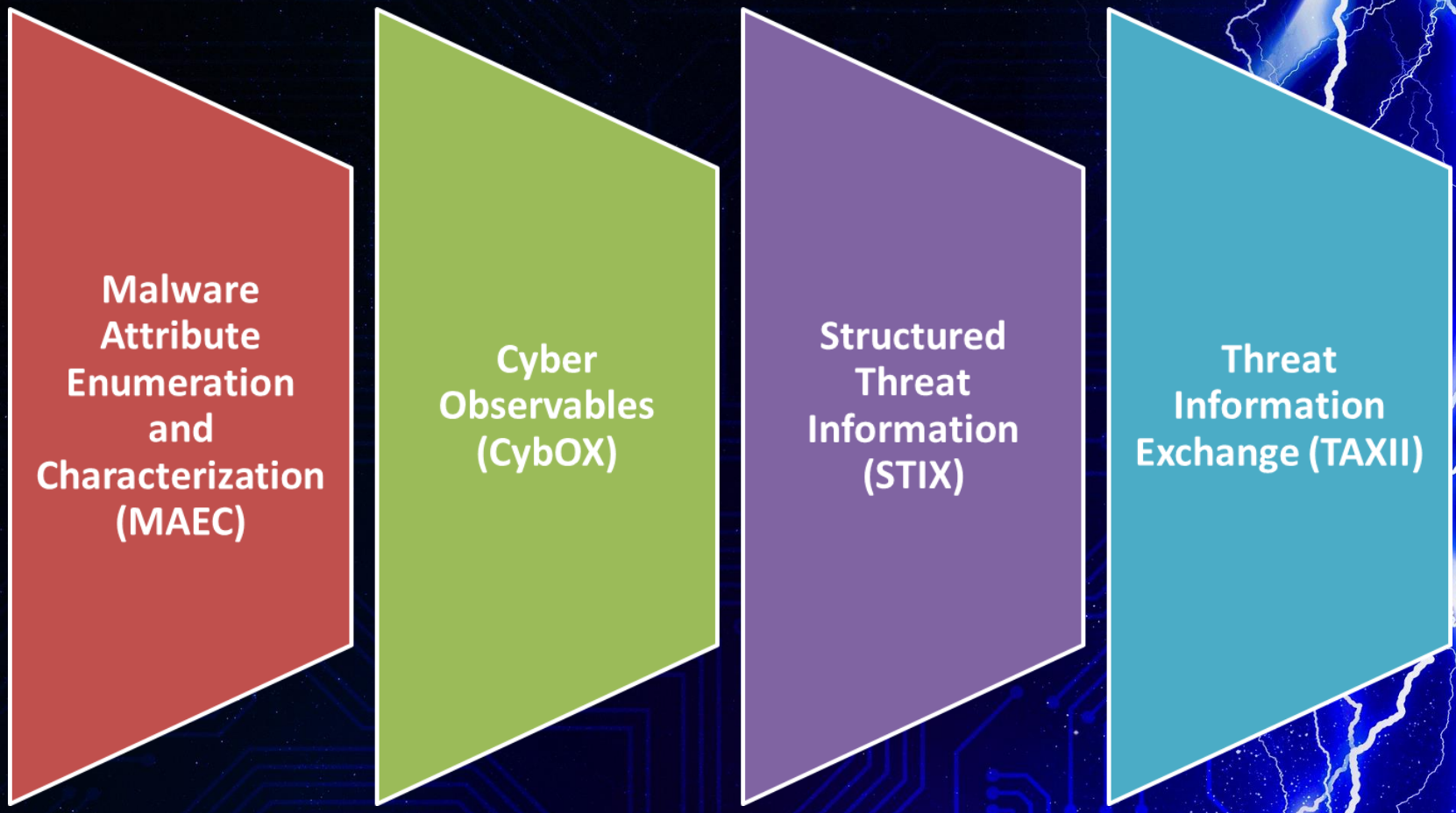


Why don’t these products talk to each other and devise a response mechanism which works like a single system?

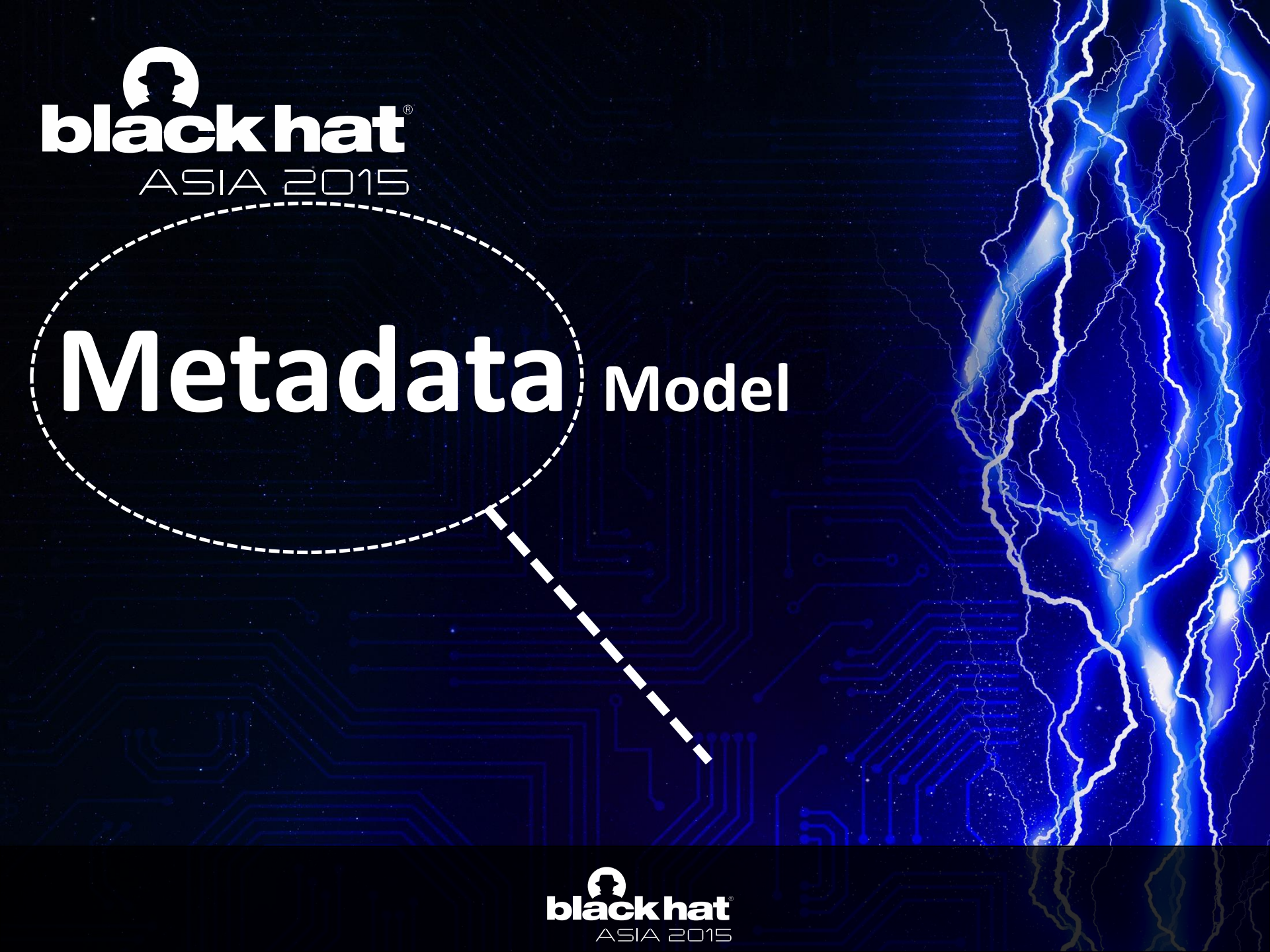
SCAP


Languages
OVAL
XCCDF
OCIL
Enumeration
CPE
CVE
CCE
CWE
Metrics
CVSS
CCSS
Reporting
ARF
Asset Identification
Integrity
TMSAD

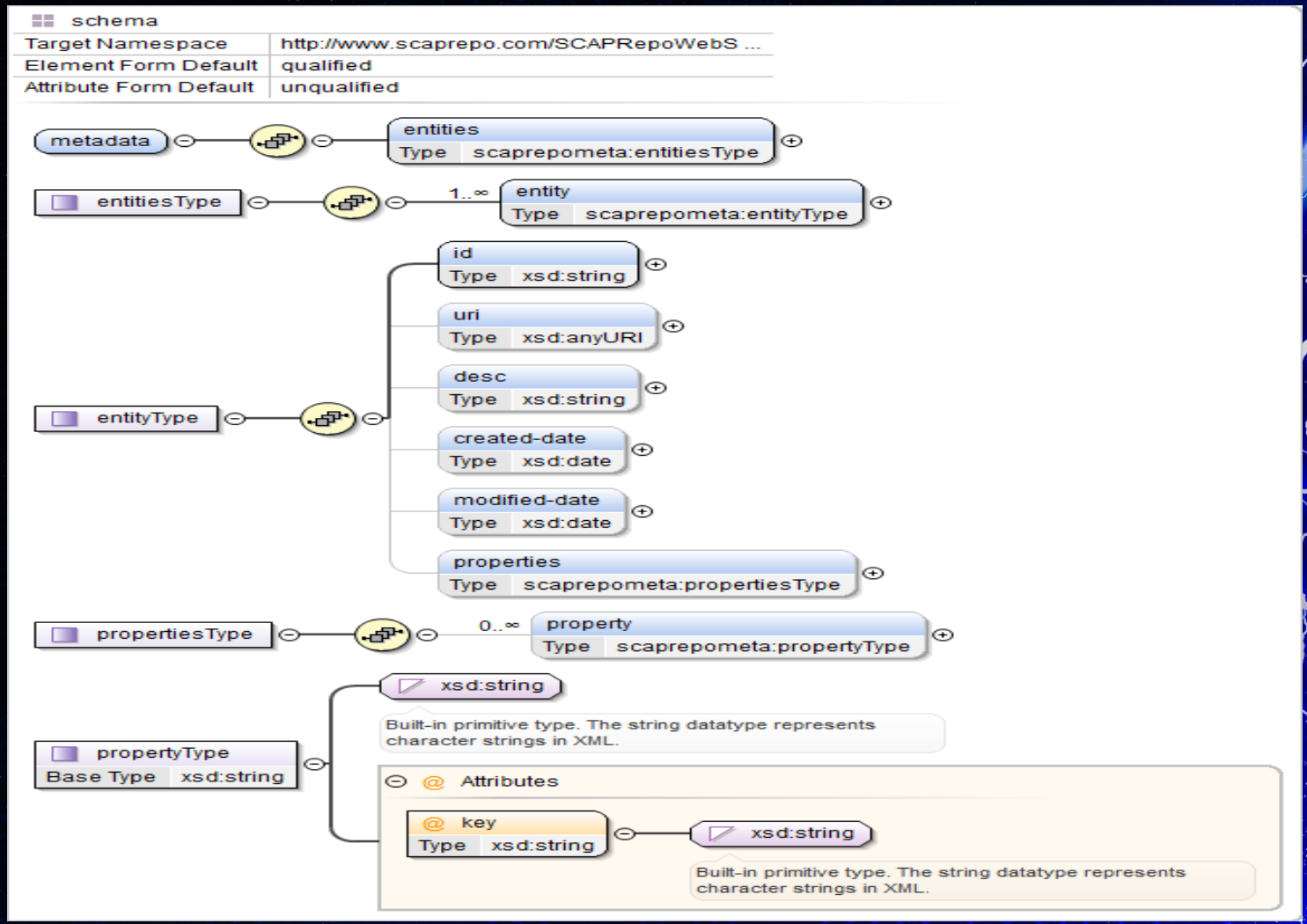
Threat Intelligence




Source: gcaptain.com


black hat
ASIA 2015
Metadata Model
black hat
ASIA 2015

Metadata Model Schema



Metadata of CVE-2015-0310

Id	CVE-2015-0310
Desc	Adobe Flash Player before 13.0.0.262 and 14.x through 16.x before 16.0.0.287 on Windows and OS X and before 11.2.202.438 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism on Windows, and have an unspecified impact on other platforms, via unknown vectors, as exploited in the wild in January 2015.
URI	http://www.scaprepo.com/control.jsp?command=viewXML&id=CVE-2015-0310
Created-Date	2015-01-27
Modified-Date	2015-02-05
Score	10.0
Exploitability_score	10.0
Impact_score	10.0
Access_vector	NETWORK
Access_complexity	LOW
Availability_impact	COMPLETE
Authentication_status	NONE
Confidentiality_impact	COMPLETE
Integrity_impact	COMPLETE
Ext_ref	CONFIRM http://helpx.adobe.com/security/products/flash-player/apsb15-02.html
Published-Date	2015-01-23
Generated-Date	2015-01-26

Searching Metadata

SCAP repo recent threats

Sample Queries

Filter Matches : 72 Download | Alert*

CVE-2015-1483 Preview

Symantec NetBackup OpsCenter 7.6.0.2 through 7.6.1 on Linux and UNIX allows remote attackers to execute arbitrary JavaScript code via unspecified vectors.

xml

CVE-2014-2130

Cisco Secure Access Control Server (ACS) provides an unintentional administration web interface based on Apache Tomcat, which allows remote authenticated users to modify application files and configuration files, and consequently execute arbitrary code, by leveraging administrative privileges, aka Bug ID CSCuj83189.

xml

CVE-2015-2218

Multiple cross-site scripting (XSS) vulnerabilities in the wp_ajax_save_item function in wonderpluginaudio.php in the WonderPlugin Audio Player plugin before 2.1 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) item[name] or (2) item[customcss] parameter in a wonderplugin_audio_save_item action to wp-admin/admin-ajax.php or the itemid parameter in the (3) won ...

xml

CVE-2015-2220

Multiple cross-site scripting (XSS) vulnerabilities in the Ninja Forms plugin before 2.8.9 for WordPress allow (1) remote attackers to inject arbitrary web script or HTML via the ninja_forms_field_1 parameter in a ninja_forms_ajax_submit action to wp-admin/admin-ajax.php or (2) remote administrators to inject arbitrary web script or HTML via the fields[1] parameter to wp-admin/post.php.

xml

Details of a CVE

SCAP repo CVE-2015-0310

Sample Queries

Download | Alert*

CVE xml

CVE-2015-0310

Date: (C)2015-01-27 (M)2015-02-24

CVSS Score: 10.0
Exploitability Subscore: 10.0
Impact Subscore: 10.0

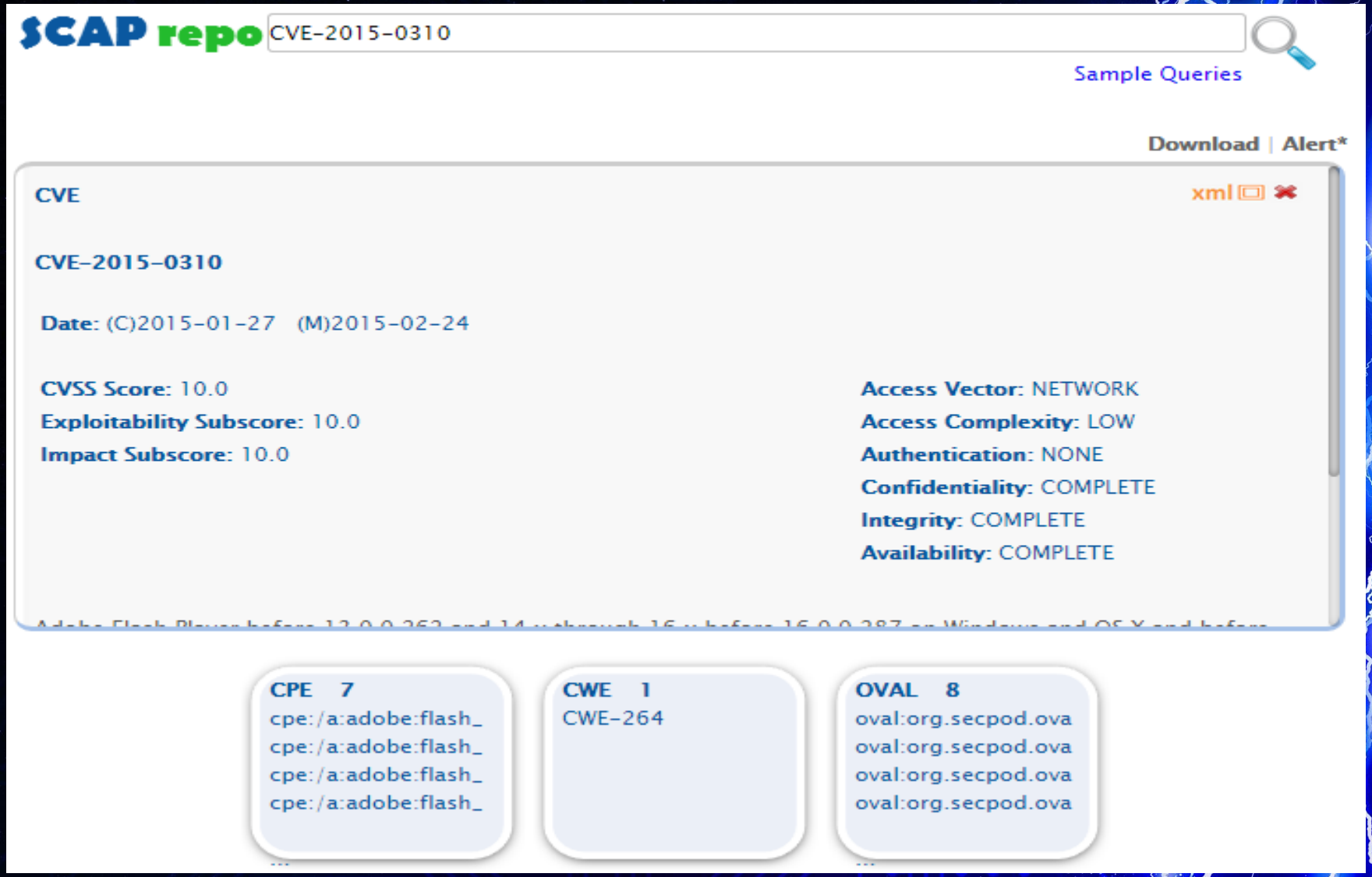
Access Vector: NETWORK
Access Complexity: LOW
Authentication: NONE
Confidentiality: COMPLETE
Integrity: COMPLETE
Availability: COMPLETE

Adobe Flash Player before 13.0.0.262 and 14.x through 16.x before 16.0.0.287 on Windows and OS X and before 11.2.202.438 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism on Windows, and have an unspecified impact on other platforms, via unknown vectors, as exploited in the wild in January 2015.

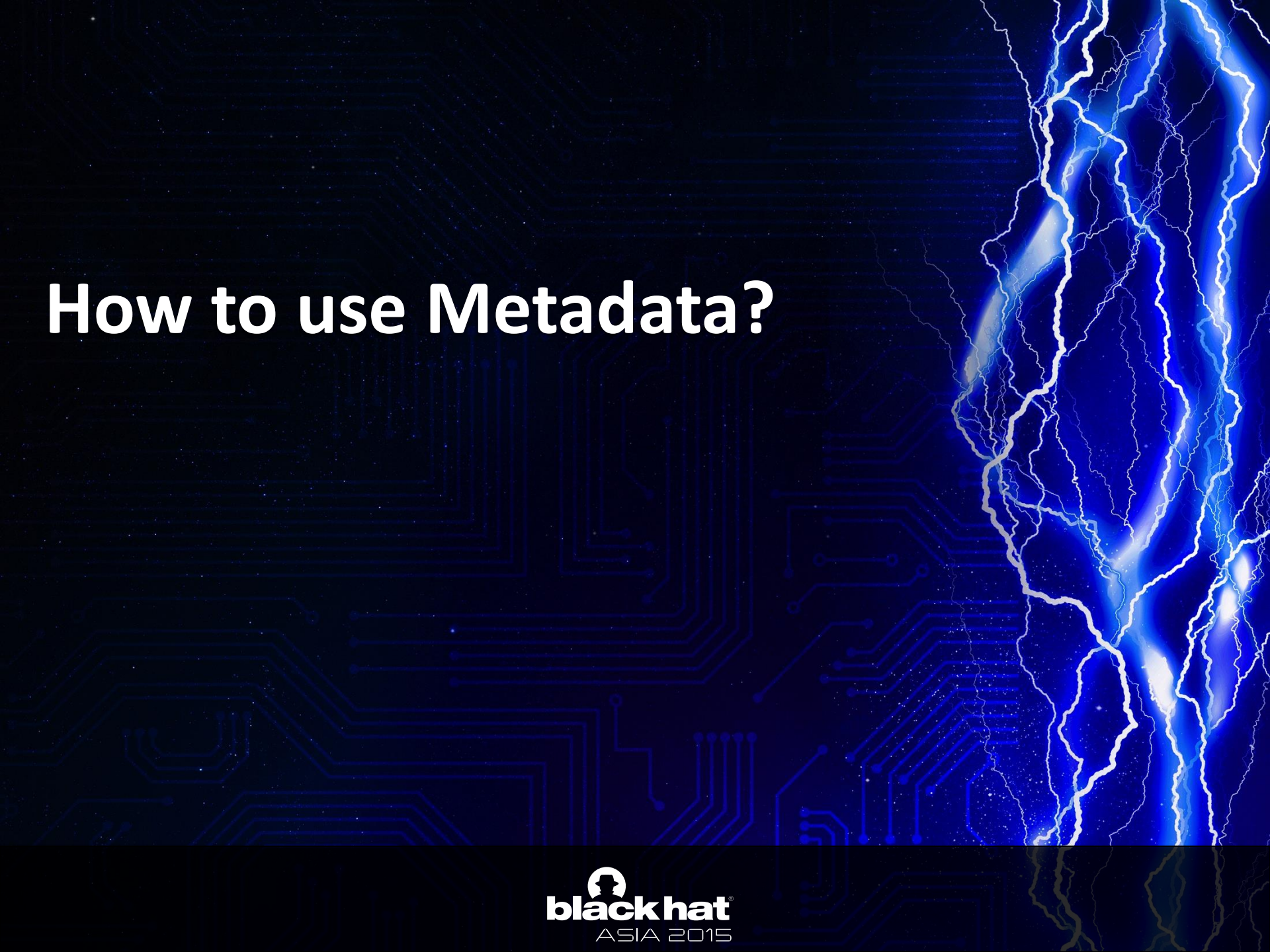
Reference:

http://helpx.adobe.com/security/products/flash-player/apsb15-02.html

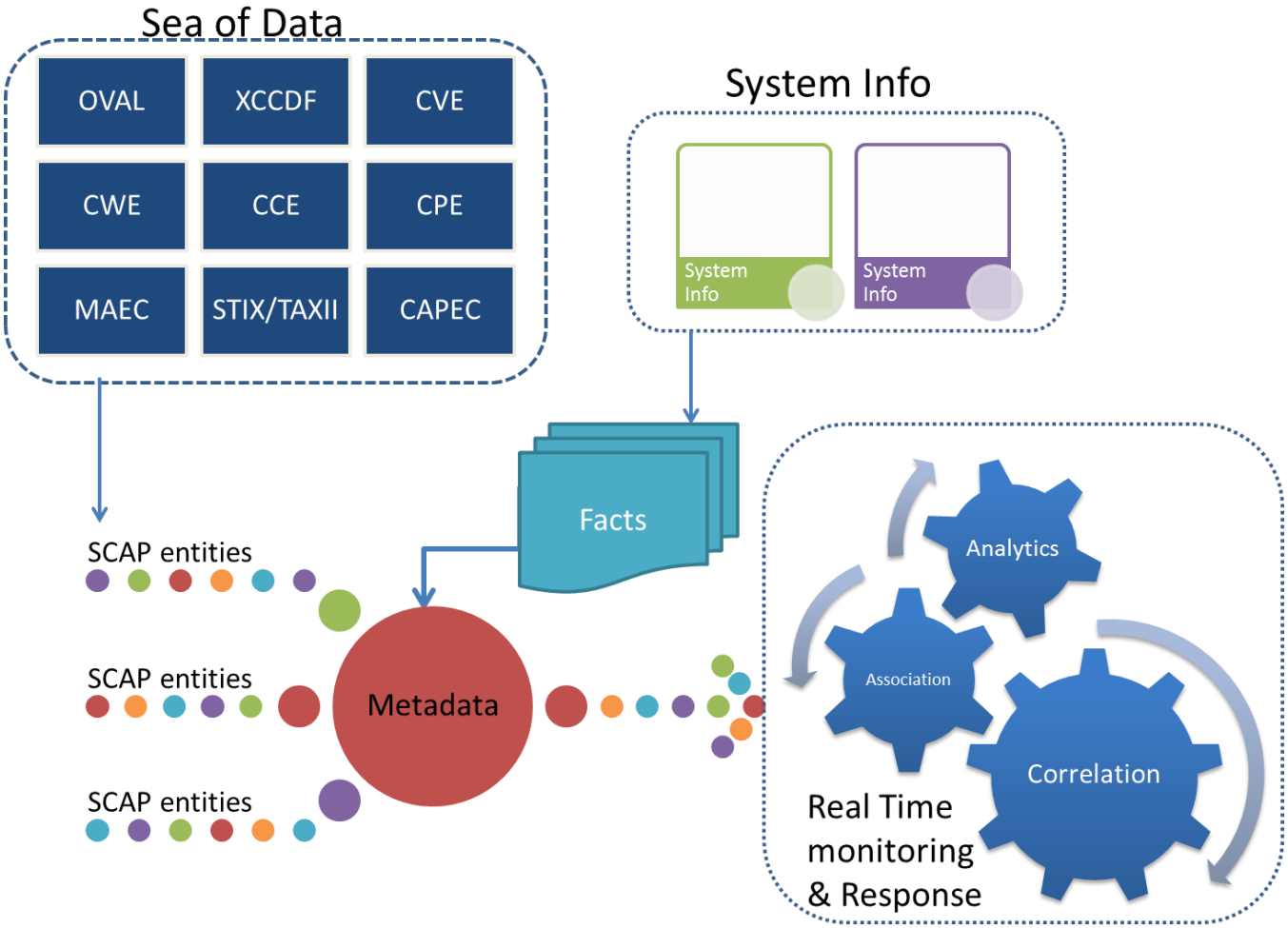
Relationship between SCAP entities



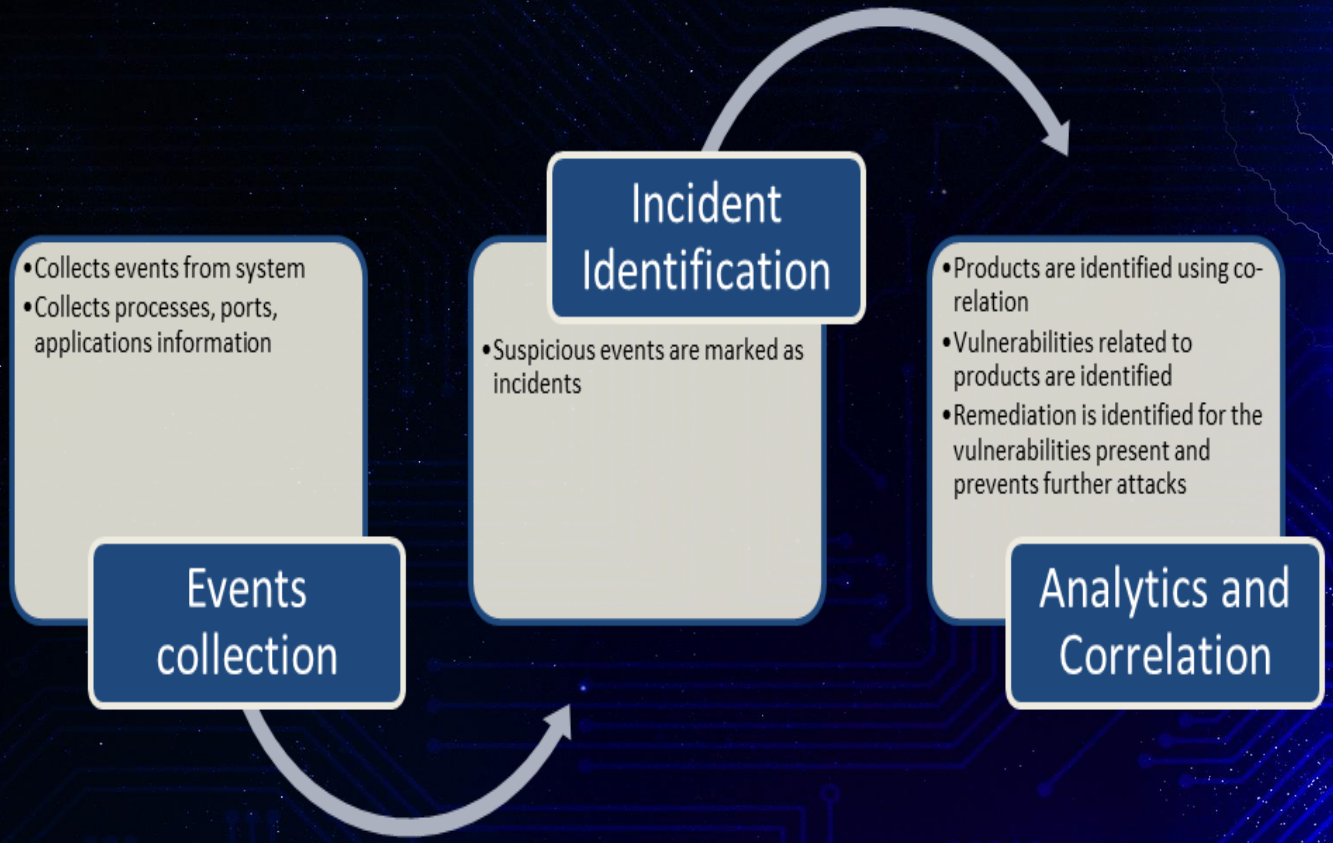
How to use Metadata?



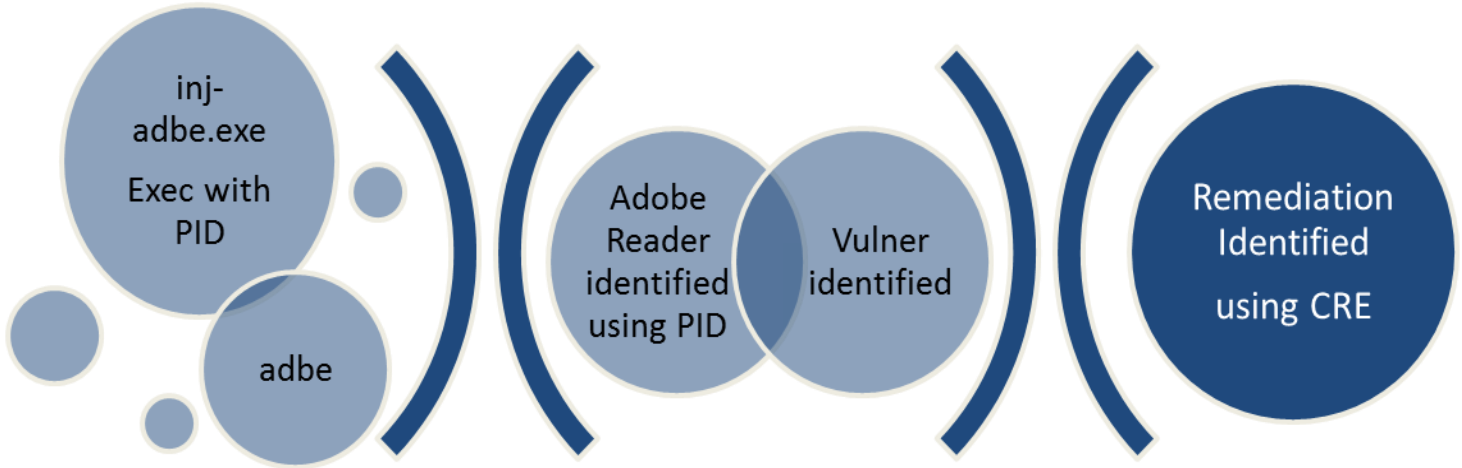
How to use metadata?



Flow of Incidence Response



Real Time Threat Monitoring using Security Content Metadata Model



Incident Identification
Using Systems Metadata
And MAEC etc.

Correlation using SCAP Metadata

Remediation Identification

Demo

?

Reminder!

Please do not forget to fill the feedback form