XORCISM

# eXpandable Open Research for Cyber Information Security Management

**XORCISM Data Model**

Overview and Concepts

Version 1.0.0 Beta

DRAFT

**Document History**

Classified: Public

Status: RC Draft



|  |  |  |
| --- | --- | --- |
| **Date** | **Author** | **Description** |
| December 30, 2013 | Jerome Athias | First draft (1.0.0 Beta) |
| January 4, 2014 | Jerome Athias | Public pre-release for peer review |

*Reference:* [*http://www.frhack.org/research/xorcism.php*](http://www.frhack.org/research/xorcism.php)

Please consider the environment before printing.

The MITRE Corporation. MITRE, the MITRE logo, CVE, the CVE logo, OVAL, and the OVAL logo are registered trademarks and the Making Security Measurable logo, CWE, the CWE logo, CAPEC, the CAPEC logo, CEE, the CEE logo, MAEC, the MAEC logo, CWSS, the CWSS logo, CWRAF, the CWRAF logo, CybOX, the CybOX logo, STIX, the STIX logo, TAXII, the TAXII logo, and Recommendation Tracker are trademarks of The MITRE Corporation.

All other marks, trademarks or brands are the property of their respective owners.

## Table of contents

eXpandable Open Research for Cyber Information Security Management 1

Table of contents 2

Abstract, Introduction and Requirements 15

XORCISM Database Model 16

Abstraction 16

Mappings 17

Internationalization 19

Use Cases 25

Benefits 26

XORCISM Core Entities 30

XORCISM Normalized/Standardized Entities/Objects 37

XORCISM Vulnerability Data Model 38

XORCISM Key Entities/Objects/Concepts/Properties 39

XORCISM Internal Entities/Objects/Concepts/Properties 40

XORCISM Other Entities/Objects/Concepts/Properties 43

Specifications/Standards/Frameworks/Methodologies/Guidelines/Models/Languages/Formats 65

Architectural Model 65

Asset Identification (AI) 65

Asset Reporting Format (ARF) 65

Asset Summary Reporting (ASR) 66

AWS Security Best Practices 66

BSIMM (Building Security In Maturity Model) 66

Build Security In (BSI) 66

CAESARS (Continuous Asset Evaluation, Situational Awareness, and Risk Scoring) architectural reference 67

CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model 67

CAP: Common Alerting Protocol 68

CAPEC: Common Attack Pattern Enumeration and Classification 68

CCE (Common Configuration Enumeration) 68

CCS (Council on CyberSecurity) 68

CDXI 69

CEE (Common Event Expression) 69

CERT Resilience Management Model (CERT-RMM) 70

Collective Intelligence Framework (CIF) 70

CIS Benchmarks 70

CloudAudit 70

Cloud Controls Matrix (CCM) 70

Cloud Trust Protocol (CTP) 70

COBIT 70

Common Configuration Scoring System (CCSS) 70

Common Remediation Enumeration (CRE) 70

Consensus Assessments Initiative (CAI) Questionnaire 71

COSO 71

CPE (Common Platform Enumeration) 71

CVE (Common Vulnerabilities and Exposures) 71

CVRF (Common Vulnerability Reporting Framework) 72

CVSS (Common Vulnerability Scoring System) 73

CWE (Common Weaknesses and Exposures) 74

CWRAF: Common Weakness Risk Analysis Framework 75

CWSS: Common Weakness Scoring System 75

Cybersecurity Framework 75

CybOX (Cyber Observable eXpression) 75

Dependency Modeling (O-DM) 75

Distributed Audit Service (XDAS) 75

DoD Information Assurance Risk Management Framework (DIARMF) 75

DPE (Default Password Enumeration) 75

Factor Analysis of Information Risk (FAIR) 76

FrameworkX (TM Forum) 76

GRC Stack (Governance, Risk Management and Compliance) 76

ICS Security Standard (Qatar) 76

Intrusion Detection Message Exchange Format (IDMEF) 76

IFX Forum Framework 76

Information Risk Analysis Methodology (IRAM) 76

Intermediary Vulnerability Information Language (IVIL) 76

Internet Users' Glossary (RFC1392) 76

IODEF (Incident Object Description Exchange Format) 76

iPost Scoring Methodology 76

ISA 99.02.01 76

ISO 3166 (Country Codes) 77

ISO 27000/ISO 27001 Information Security Risk Management System  ISO/IEC 19770  ISO 31000 Enterprise Management 77

ISO/IEC 27001 77

Key Management Interoperability Protocol (KMIP) TC 78

MAEC (Malware Attribute Enumeration and Characterization) 78

Malware Metadata Exchange Format (MMDEF) 78

NERC CIP (North American Electric Reliability Corporation, Critical Infrastructure Protection) 78

Network Defense Data Models (NDDM) 78

NIST Risk Management Framework (RMF) 78

NIST SP 500-291 79

NIST SP 800-34 79

NIST SP 800-37 79

NIST SP 800-53 Rev. 4 79

NRF: U.S. National Response Framework 79

OAuth (Open standard for Authorization), OAuth Framework 79

OASIS Customer Information Quality Committee (CIQ) 79

OASIS xCIL : extensible Customer Information Language 80

OASIS xCRL : extensible Customer Relationships Language 80

OASIS xNAL : extensible Name and Address Language 80

OASIS xNL 80

OCIL (Open Checklist Interactive Language) 80

OCTAVE 80

Open Automated Compliance Expert Markup Language (O-ACEML) 80

Open Checklist Interactive Language (OCIL) 80

OpenID 80

Open Information Security Management Maturity Model (O-ISM3) 80

OpenIOC 80

OpenSAMM (Software Assurance Maturity Model) 80

Open Source Security Testing Methodology Manual (OSSTMM) 80

Open Threat Exchange (OTX) 81

OVAL (Open Vulnerability and Assessment Language) 81

OWASP 81

OWASP ASVS (Application Security Verification Standard Project) 81

OWASP Testing Guide 82

Penetration Testing Execution Standard (PTES) 83

Predictive Model Markup Language (PMML) 83

RID: Real-time Inter-network Defense protocol 83

Risk Taxonomy (O-RT) 83

SCAP (Security Content Automation Protocol) 83

Security Description and Exchange Format (SecDEF) 83

SES - Security Event System 84

Situational Awareness Reference Architecture (SARA) 84

Software Assurance (SwA) Competency Model 84

Software Defined Perimeter (SDP) 85

STAR (Security, Trust & Assurance Registry) 85

STIGs: Defense Information Systems Agency Security Technical Implementation Guides 85

STIX (Structured Threat Information eXpression) 86

STRIDE Threat Model 87

SQUARE (Security Quality Requirements Engineering) 87

SWID Tags 88

TAXII (Trusted Automated eXchange of Indicator Information) 88

TOGAF 88

Traffic Light Protocol (TLP) Matrix 88

Trust Model for Security Automation Data (TMSAD) 88

VERIS: Vocabulary for Event Recording and Incident Sharing 89

Web Application Security Evaluation Criteria 89

Web Application Firewall (WAF) Evaluation Criteria 89

XCCDF: Extensible Configuration Checklist Description Format 89

XEP-0268: Incident Handling 89

XML Encryption 89

XORCISM Tools 90

XORCISM Database conversion script 90

XORCISM DLL 90

XORCISM Import\_capec 90

XORCISM Import\_cpe 90

XORCISM Import\_cve 90

XORCISM Import\_cwe 90

Other Security Tools 91

Tools Repositories 91

AbuseHelper 91

Apache Lucene 91

Appcmd.exe 91

AppLocker 91

Aqueduct 91

BitLocker 92

BitMail 92

Bitmessage 92

Bro-IDS 92

capirca 92

CIS-CAT 92

Cuckoo Sandbox 92

EMET (Enhanced Mitigation Experience Toolkit) 92

ESAPI (OWASP Enterprise Security API) 93

File Vault 93

Forensic Toolkit (FTK) 93

GnuPG (GPG) / PGP 93

hadoop-pcap 93

IOCExtractor 93

Malware Hash Registry 93

MANTIS 93

Microsoft System Center Configuration Manager (SCCM) 93

MISP 93

Minion 93

Moloch 93

Moon Secure Antivirus 94

Nfsight 94

Nmap 94

OCIL Interpreter 94

OpenDNS (DNSCrypt) 94

OpenSCAP 94

OpenVAS (Open Vulnerability Assessment System) 94

OpenVPN 94

OSSIM 94

OTR (Off-the-Record Messaging) 94

OVAL Interpreter (ovaldi) 95

OWASP Projects and Guides 95

pfSense 95

Request Tracker (RT) 95

RIPS 95

RTIR (RT for Incident Response) 95

scap-security-guide 95

Secpod Saner 95

Secunia PSI 95

Shodan 95

Silent Phone / Silent Text 96

Snort 96

Splunk 96

Spybot 2 Search & Destroy 96

sshuttle 96

Suricata 96

ThreadFix 96

ThreatModeler 96

Tor 96

TrueCrypt 96

VirusTotal 96

XCCDF Interpreter 96

YARA 96

YETI 97

Wireshark 97

WP-CLI 97

Acronyms/Terms/Definitions/Abbreviations/Symbols 98

A&I database: Abstracting and Indexing database 98

ABAC: Attribute Based Access Control 98

ACL: Access Control List 98

AI: Asset Identification [5] 98

AI: Artificial Intelligence 98

AM: Asset Management 98

ANSI: American National Standards Institute 98

ANSSI: Agence Nationale de la Sécurité des Systèmes d’Information (France) 98

AppSec: Application Security 98

APT: Advanced Persistent Threat 98

ARF: Asset Reporting Format [6] 98

ASN: Autonomous System Numbers 98

ASVS: Application Security Verification Standard Project 98

Bloom filter 98

BSIMM: Building Security In Maturity Model 98

BYOD: Bring Your Own Device 98

C2: Command and Control 99

CADF: Cloud Auditing Data Federation Working Group 99

CAESARS: Continuous Asset Evaluation, Situational Awareness, and Risk Scoring architectural reference 99

CAI: Consensus Assessments Initiative 99

CAP: Common Alerting Protocol 99

CC: Common Criteria 99

CERT: Cyber Emergency Response Team 99

CIA: Confidentiality, Integrity, Availability or Authenticity 99

CIS: Center for Internet Security 99

CNIL: Commission Nationale de l’Informatique et des Libertés (France) 99

COTS: Commercial-off-the-shelf 99

CS&C: U.S. Office of Cybersecurity and Communications 99

CSA: Cloud Security Alliance 99

CCM: Cloud Controls Matrix 99

CCS: Council on CyberSecurity 99

CCSA: Collaborative Cyber Situational Awareness 100

CCV: Cybersecurity Compliance Validations 100

CEE: Common Event Expression 100

CERT: Computer Emergency Response Team 100

CIA: Confidentiality, Integrity, Availability 100

CIF: Collective Intelligence Framework 100

CIQ: Customer Information Quality Committee 100

CIS: Center for Internet Security 100

CLASP: Comprehensive, Lightweight Application Security Process 100

CMRS: Continuous Monitoring and Risk Scoring 100

CMU: Carnegie Mellon University 100

CNCI: U.S. Comprehensive National Cybersecurity Initiative 100

CNE: Computer Network Espionage 100

COA: Course of Action 100

COBIT: Control Objectives for Information and Related Technology 100

COL: Course of Law 100

CPE: Common Platform Enumeration 100

CPNI: United Kingdom's Centre for the Protection of National Infrastructure 100

CSIC: Computer Security Incident Coordination 100

CSIRT: Computer Security Incident Response Team 100

CSRC: Computer Security Resource Center 100

C-TIP: Cyber Threat Intelligence Program 101

CTP: Cloud Trust Protocol 101

CVE: Common Vulnerabilities and Exposures 101

CVSS: Common Vulnerability Scoring System (CVSS-SIG) 101

CWE: Common Weaknesses Enumeration 101

CWRAF: Common Weakness Risk Analysis Framework 101

CWSS: Common Weakness Scoring System 101

CybOX: Cyber Observable eXpression 101

DISA: U.S. Defense Information Systems Agency 101

DLP: Data Loss Prevention 101

DMG: Data Mining Group 101

DMZ: Demilitarized zone 102

dnsSinkhole 102

DNS Amplification 102

DoD: U.S. Department of Defense 102

DRM: Digital Rights Management 102

DSS: Defense Security Service (U.S. Department of Defense) 102

ECPA: Electronic Communications Privacy Act 102

ENISA: European Union Agency for Network and Information Security 102

ESAPI: OWASP Enterprise Security API 102

FIDO: Fast Identity Online 102

FINE: Format for Incident Information Exchange 102

FIPS: U.S. Federal Information Processing Standards 102

FISM: Federal Information Security Memorandum 102

FISMA: Federal Information Security Management Act 102

GHDB: Google Hacking Database 102

Google Dork 102

GPO: Microsoft Group Policy 102

GRC Stack: Governance, Risk Management and Compliance 102

HMI: Human-Machine Interface 102

HOST: Homeland Open Security Technology 102

hpfeeds: Honeynet Project generic authenticated datafeed protocol 102

IATF: Information Assurance Technical Framework 103

ICS: Industrial Control System 103

ICS-ISAC: Industrial Control System Information Sharing and Analysis Center 103

IDS: Intrusion Detection System 103

IEEE: Institute of Electrical and Electronics Engineers 103

IETF: Internet Engineering Task Force 103

IOC: Indicator of Compromise 103

IP: Internet Protocol 103

IPS: Intrusion Prevention System 103

ISA: International Society of Automation 103

ISACA: Information Systems Audit and Control Association 103

ITSM: IT Service Management 104

ITU: International Telecommunication Union 104

Jammer 104

JSON: JavaScript Object Notation 104

KISS: Keep it Simple, Stupid 104

KNOX: Samsung KNOX 104

MAEC: Malware Attribute Enumeration and Characterization 104

MACCSA: Multinational Alliance for Collaborative for Cyber Situational Awareness 104

MAPP: Microsoft Active Protections Program 104

MARS: Microsoft Active Response for Security 104

MCC: Motor Control Center 104

Megatron 104

MISP: Malware Information Sharing Platform 104

MSRC: Microsoft Security Response Center 104

MTPIS: Managed Trusted Internet Protocol Services 104

NAICS: North American Industry Classification System 104

NATO: North Atlantic Treaty Organization 104

NCCIC: U.S. National Cybersecurity and Communications Integration Center 104

NCCoE: U.S. National Cybersecurity Center of Excellence 104

NCP: U.S. National Checklist Program repository 104

NDA: Non-Disclosure Agreement 105

NISPOM: National Industrial Security Program Operating Manual 105

NIST: U.S. National Institute of Standards and Technology 105

NRF: U.S. National Response Framework 105

NTP: Network Time Protocol 105

NVD: U.S. National Vulnerability Database 105

OASIS: Organization for the Advancement of Structured Information Standards 105

OAuth: Open standard for Authorization 105

OCTAVE 105

OCIL: Open Checklist Interactive Language 105

OISF: Open Information Security Foundation 105

OpenID 105

OpenVAS: Open Vulnerability Assessment System 105

OpenSAMM: Software Assurance Maturity Model 105

OSSTMM: Open Source Security Testing Methodology Manual 106

OSVDB: Open Sourced Vulnerability Database 106

OVAL: Open Vulnerability and Assessment Language 106

OWASP: Open Web Application Security Project 106

PCS: Process Control System 106

PGP: Pretty Good Privacy 106

PKE: Public Key Enablement 106

PKI: Public Key Infrastructure 106

PLC: Programmable Logic Controller 106

Plover 106

PMML: Predictive Model Markup Language 106

PPSM: Ports, Protocols, and Services Management 106

Protocol Buffers 106

PTES: Penetration Testing Execution Standard 106

RACE: Rapid Access Computing Environment 106

RFC1392: Internet Users' Glossary 106

RID: Real-time Inter-network Defense protocol 107

ROLIE: Resource-Oriented Lightweight Indicator Exchange 107

RVA: Risk and Vulnerability Assessment 107

SAIR: Situational Awareness and Incident Response 107

SCADA: Supervisory Control And Data Acquisition 107

SCAP: Security Content Automation Protocol 107

SCIMP: Silent Circle Instant Messaging Protocol 107

SCM: Software Configuration Management 107

SDLC: Secure Development Life Cycle 107

SDN: Software Defined Networking 107

Shredder 107

SIEM: Security Information & Event Management solution 107

SOC: Security Operation Center 107

SQUARE: Security Quality Requirements Engineering 107

STAR: Security, Trust & Assurance Registry 107

STIG: Defense Information Systems Agency Security Technical Implementation Guide 107

STIX: Structured Threat Information eXpression 107

SwA: Software Assurance 107

TAXII: Trusted Automated eXchange of Indicator Information 108

Threatsaurus: “The A-Z of computer and data security threats” 108

TPM: Trusted Platform Module 108

TTP: Tactics, Techniques and Procedures 108

UAC: User Access Control 108

URI: Uniform Resource Identifiers 108

US-CERT: U.S. Computer Emergency Readiness Team 108

USGCB: United States Government Configuration Baseline 108

VCDB: VERIS Community Database 108

VDM: Vulnerability Data Model 108

VERIS: Vocabulary for Event Recording and Incident Sharing 108

VFD: Variable Frequency Drive 108

VLAN: Virtual Local Area Network 108

VoIP: Voice over IP 108

VoSIP: Voice over Secure Internet Protocol 108

VPN: Virtual Private Network 108

W3C: World Wide Web Consortium 108

Waiver 109

WAF: Web Application Firewall 109

WAPT: Web Application Penetration Test 109

WASC: Web Application Security Consortium 109

WHID: Web Hacking Incidents Database 109

xCIL: extensible Customer Information Language 109

xCRL: extensible Customer Relationships Language 109

xNAL: extensible Name and Address Language 109

XML: Extensible Markup Language 109

XVDM: XORCISM Vulnerability Data Model 109

Waiver 109

Warrant 109

Ontologies/Taxonomies/Controlled Vocabularies/Thesauri/Classifications 110

BIZEC APP/11 110

BIZEC TEC/11 110

CSIRT Case Classification 110

CybOX (Cyber Observable eXpression) 110

HP Fortify Taxonomy: Software Security Errors 110

Internet Users' Glossary (RFC1392) 110

IODEF (Incident Object Description Exchange Format) 110

ISO 3166 (Country Codes) 110

North American Industry Classification System 110

OWASP Attack Category 110

Risk Taxonomy (O-RT) 111

SANS- Twenty Critical Security Controls for Effective Cyber Defense 111

STIX 111

Threatsaurus (“The A-Z of computer and data security threats”) 111

VERIS: Vocabulary for Event Recording and Incident Sharing 111

Web Security Glossary 112

Web Security Threat Classification (WSTC) 112

Repositories/Data Feeds 113

CIS Benchmarks 113

Cybercrime tracker 113

DShield 113

FIPS: U.S. Federal Information Processing Standards 113

GRC Repository 113

Inventory of Standards Relevant to Cloud Computing (NIST) 113

National Checklist Program (NCP) repository 113

National Vulnerability Database (NVD) (NIST) 113

Open Sourced Vulnerability Database (OSVDB) 113

OVAL Repositories 113

SCAP Repositories 114

SSL Labs 114

STIGs: Defense Information Systems Agency Security Technical Implementation Guides 114

Tools Repositories 114

VirusTotal 114

XCCDF Repositories 114

Communities/Working Groups/Mailing lists 115

BSIMM 115

Buqtraq 115

Center for Internet Security 115

Cloud Security Alliance (CSA) 115

Communities of Trust 115

Continuous Monitoring Working Group 115

DShield 115

FIDO (Fast Identity Online) 115

IETF Working Groups 115

MITRE/NIST Communities 115

Inventory of Standards Relevant to Cloud Computing 115

ISACA 116

Making Security Measurable 116

OAuth: Open standard for Authorization 116

OWASP 116

RIPE 116

Team Cymru 116

The Open Group 116

VERIS Community 116

Web Application Security Consortium (WASC) 116

Web Security Mailing List 116

Informative References 117

Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (France) 117

An Algebra for Specifying Valid Compound Terms in Faceted Taxonomies 117

ANSI/API Standard 780 methodology 117

Application Security Architecture 117

Application Security Verification Standard Project (ASVS) 117

Asset Identification (AI) 117

Asset Reporting Format (ARF) 117

Avoiding Social Engineering and Phishing Attacks 117

Bitmessage: A Peer‐to‐Peer Message Authentication and Delivery System 117

BIZEC APP11 117

BIZEC TEC11 117

Bloom filters 117

BSI: Build Security In 118

BSIMM (Building Security In Maturity Model) 118

Bug Tracking System 118

C-Based Toolchain Hardening Cheat Sheet 118

CAESARS (Continuous Asset Evaluation, Situational Awareness, and Risk Scoring) architectural reference 118

CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model (NISTIR-7756) 118

CAP: Common Alerting Protocol 118

CAPEC (Attack Patterns) 118

Center for Internet Security (CIS) 118

CIP-CSP Mind Map 118

CIS Benchmarks 118

CLASP 118

CloudAudit 118

Cloud Auditing Data Federation Working Group (CADF) 118

Cloud Controls Matrix (CCM) 118

Cloud Trust Protocol (CTP) 119

COBIT 119

Codes for the representation of currencies and funds (ISO 4217:2001) 119

Computer Security: Reducing Risks of Malware Infections 119

Computer Security Incident Coordination (CSIC) 119

Computer Security Resource Center (CSRC) 119

Consensus Assessments Initiative (CAI) Questionnaire (CAIQ) 119

CSIRT Case Classification 119

Cuckoo Hashing 119

Cuckoo Sandbox 119

CVE: Common Vulnerabilities and Exposures 119

CVSS: Common Vulnerability Scoring System (CVSS-SIG) 119

CWE: Common Weaknesses Enumeration 119

CWE/SANS Top 25 Most Dangerous Software Errors 119

CWRAF: Weakness Risk Analysis Framework 120

CWSS: Weakness Scoring System 120

Cybersecurity Assurance (CA) 120

Cybersecurity Framework 120

Cyber Security Standards 120

Cyber Technology and Information Security Laboratory (CTISL) 120

Cyber Threat Landscape Report 120

CybOX (Cyber Observables) 120

Database Model 120

Data Classification 120

Data Models 120

Data Structures 120

Data Structures/Stacks and Queues 120

Date and Time on the Internet: Timestamps (RFC3339) 121

Deep learning with word2vec and gensim 121

Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs 121

Disk Encryption 121

Distributed Web Honeypots 121

Dublin Core Metadata 121

eCSIRT 121

Encryption Laws 121

Encryption Using Chaos 121

ESAPI: OWASP Enterprise Security API 121

FIDO (Fast Identity Online) 121

FileVault 121

FIPS: U.S. Federal Information Processing Standards 121

FIRST 122

GRC Stack (Governance, Risk Management and Compliance) 122

hpfeeds (Honeynet Project generic authenticated datafeed protocol) 122

Hushmail 122

IANA Protocol Registries 122

IETF Vulnerability Data Model (VDM) 122

Internet Message Format (RFC2822) 122

Internet Users' Glossary (RFC1392) 122

ISO 3166 (Country Codes) 122

ISO/IEC 27001 122

ITIL 122

ITL Security Bulletins 122

ITU Recommendation X.1524 : Common weakness enumeration 122

IVIL: Intermediary Vulnerability Information Language 122

Large-scale PCAP Data Analysis Using Apache Hadoop 122

Lumberjack Project 123

MAEC (Malware) 123

Making Security Measurable (MSM) 123

MANTIS (Cyber Threat Intelligence Management Framework) 123

McAfee Labs 2014 Predictions Report 123

Methodology for Managing Privacy Risks 123

Minion (Security Automation platform) 123

Misuses and Code Errors (What you should NOT do) 123

MSM: Making Security Measurable 123

NIST Computer Security Publications 123

NISP Library 123

NIST SP 500-291 123

NIST SP 800-34 123

NIST SP 800-53 Rev. 4 124

NRF: U.S. National Response Framework 124

OAuth (Open standard for Authorization), OAuth Framework 124

OpenID 124

OpenSAMM (Software Assurance Maturity Model) 124

Open Source Licenses 124

Open Source Security Testing Methodology Manual (OSSTMM) 124

OSVDB: Open Sourced Vulnerability Database 124

OWASP TOP10 124

OWASP TOP10 For .NET 124

OWASP TOP10 For JavaScript 124

Penetration Testing Execution Standard (PTES) 124

Personal Data Definition 124

pfSense 124

Plover 125

Prince 2 125

Protocol Buffers 125

Resilience and Cyber Security of Technology in the Built Environment 125

Resilient Control Systems 125

Revision Control 125

RFC 6189 ZRTP: Media Path Key Agreement for Unicast Secure RTP 125

Risk Taxonomy (O-RT) 125

SCADA Patching recommendations 125

SCAP (Security Content Automation Protocol) 125

Secure Coding Cheat Sheet 126

Secure Development Life Cycle (SDLC) 126

Security Automation and Continuous Monitoring (sacm) 126

Security Battleground 126

Security Guidelines 126

Security of personal data 126

Selecting Mathematical Models With Greatest Predictive Power: Finding Occam's Razor in an Era of Information Overload 126

Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors 126

SimpleRisk 126

Software Assurance 126

Software Configuration Management (SCM) 126

Software Defined Networking (SDN) 126

Software Defined Perimeter (SDP) 126

Software Vulnerability Exploitation Trends 126

Spamhaus 127

Spear Phishing - Understanding the Threat 127

SQL Injection Prevention Cheat Sheet 127

SQUARE (Security Quality Requirements Engineering) 127

SSL Labs 127

STAR (Security, Trust & Assurance Registry) 127

STIG: Defense Information Systems Agency Security Technical Implementation Guide 127

STIX (Structured Threat Information) 127

Supply Chain Assurance 127

Supply Chain Risk Management 127

Tags for Identifying of Languages (RFC4646) 127

TAXII (Trusted Automated eXchange of Indicator Information) 127

Taxonomies, Controlled Vocabularies, Thesauri and Ontologies 127

THEMIS 127

ThreadFix 128

Threatsaurus 128

TOGAF 128

Ultimate SANS Pen Test Poster 128

Uncover Security Design Flaws Using The STRIDE Approach 128

United States Government Configuration Baseline (USGCB) 128

VERIS: Vocabulary for Event Recording and Incident Sharing 128

Version Control 128

W3C: World Wide Web Consortium 128

Water and wastewater SCADA Cybersecurity 128

Web Application Firewall (WAF) Evaluation Criteria 128

Web Application Security Consortium (WASC) 128

Web Application Security Evaluation Criteria 129

Web Application Cheat Sheets 129

Web Security Threat Classification (WSTC) 129

What is the exact difference between parallel and concurrent programming? 129

Winning the Cybersecurity Battle 129

X-Frame-Options, or solving the wrong problem 129

XML Database 129

XML Encryption 129

XORCISM Database model 129

XORCISM Tools 129

.NET Security Cheat Sheet 129

Acknowledgements 130

Appendix A: Threats Taxonomies Examples 131

Cyber Attacks extracted from “Winning the Cybersecurity Battle” 131

Threat Actors (attackers) extracted from “Winning the Cybersecurity Battle” 131

ThreatModeler Glossary (Threat Library by MyAppSecurity) 132

## Abstract, Introduction and Requirements

***“The cyber threat is one of the most serious economic and national security challenges we face”****,* President Obama

<http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>

In Cyber Security, Organizations have to deal, for example, with Big Data and Privacy.

Frameworks, structured data representation (models [1]), and structured common shared ontologies [2], are necessary for normalizing data, and so, for sharing information to reach interoperability [4] and being able to increase automation.

Specifications and Standards are needed to reach this goal.  
This also helps to obtain Metrics, making the Cyber Security more measurable and manageable.

XORCISM uses a relational *(and holistic)* approach comparable to an XML-enabled, as opposed to a Native XML (NXD), approach [3]. XORCISM intends to improve the Interoperability Maturity of the adopters and contribute to Cyber Peacefare.

The XORCISM database model is a relational model describing Cyber Objects and Observables.

It tends to leverage currently publicly available descriptions used of cyber objects [5] and properties through an in-depth description of their relationships.

It offers data structures easily usable by programming languages, and is easily expandable.

XORCISM only intends to be a framework to convey commonly exchanged Cyber Security Information.

[1] Data models

<http://en.wikipedia.org/wiki/Data_model>

[2] Taxonomies, Controlled Vocabularies, Thesauri and Ontologies

<http://www.taxonomies-sig.org/about.htm>

See also: Faceted taxonomies

<http://www.ics.forth.gr/_publications/algebraDKE07_final_pv.pdf>

[3] XML database

<http://en.wikipedia.org/wiki/XML_database>

[4] Interoperability

<http://www.himss.org/library/interoperability-standards/what-is>

Foundational Interoperability

Structural Interoperability

Syntactic and Semantic Interoperability

<https://en.wikipedia.org/wiki/Semantic_interoperability>

[5] CybOX

<http://cybox.mitre.org>

## XORCISM Database Model

The XORCISM Database Model’s schema is available as an .SQL file to create the tables available at:

<https://github.com/athiasjerome/XORCISM>

A detailed and exhaustive technical documentation describing the XORCISM Database Model, including schema, tables, attributes/properties and data types could be found at the same location and was not in scope of this document.

*XORCISM does not pretend or intend to provide an exhaustive Cybersecurity Ontology.*

*However, readers could find useful the following compilation of Cybersecurity Vocabularies:*

[*http://www.frhack.org/research/Information\_Security\_Vocabularies.xlsx*](http://www.frhack.org/research/Information_Security_Vocabularies.xlsx) *[TODO] Update*

Furthermore, operational implementation technical details are out of scope of this document.

### Abstraction

**A high level of abstraction was not wanted in XORCISM version 1.0.0.**

Some XORCISM tables’ names make direct use of the exact same names, or similar names\* of well-known [Cyber Security objects/specifications](#_Specifications/Standards/Frameworks/Met).

Examples: [WASC](#_Web_Security_Threat_1), [CWE](#_CWE), [CVE](#_CVE_(Common_Vulnerabilities), [CPE](#_CPE_(Common_Platform).

*\* Names of the properties in the XORCISM’s tables tend to be -entity specific- to facilitate manipulation and research, for example, in a programming context.*

*(i.e.: CWEAbstraction versus Abstraction in the* [*CWE specification*](#_CWE_1)*)*

A continuous balance is researched for an adequate level of abstraction against a practical description of cyber objects and concepts, which is quick and easy to use in the programming area.

In this area, abstraction adds **complexity**, or **ambiguity**.

Examples:

* Using only one [Category](#_Category) table to categorize multiple objects/entities lead to an unpractical approach.
* Naming an object Contact, in place of [Person](#_Person_2) could lead to some level of ambiguity in some cases, i.e.: "Contact is the probable frequency, within a given timeframe, that a threat agent will come into contact with an asset.” [Risk Taxonomy](#_Risk_Taxonomy_(O-RT))

On the contrary, creating multiple tables to specify one object/entity could also lead to complexity.

Example:

Creating different tables to specify the different [categories](#_Category_5) of Persons Groups, i.e. those in [RFC1392](#_Internet_Users'_Glossary) (the Internet Users' Glossary)

The author made some choices based on his own appreciation while naming the tables in XORCISM.

Examples:

[Vulnerability](#_Vulnerability) table, including the properties found in the [CVE specification](#_CVE_(Common_Vulnerabilities_1)

Weakness table in addition of the CWE table, to use other classifications such as

Further **improvement and simplification changes** are expected after operational implementation validation [phases](#_Phase). (i.e. Benchmarks or OVAL tables)

Please kindly note that the current version of the XORCISM model comes with a *relatively high* number of tables, partially due to the lack of consensus, in some cases, for a naming convention for some entities/concepts, by Cyber Security parties/specifications/standards.

Examples:

[Protocol](#_Protocol) versus [Procedure](#_Procedure_1)

[Language](#_Language) versus [Locale](#_Locale_2) (C++, Java versus English, US-English, French…)

Note that some Tables are provided in the current XORCISM version for those who would like to “simplify” the model.

Examples:

Model, Entity, Type

### Mappings

To ensure *compatibility* with Cyber Security Specifications such as, for example, **inter-exchange formats** *(interchange formats)*; in-depth analysis and mappings were performed between these Specifications and the XORCISM Data Model.

Existing available mappings were used.

Examples:

IAVM to CVE

<http://iase.disa.mil/stigs/iavm-cve.html>

Furthermore, as various specifications exist, or emerge and evolve, to describe the same concepts in a particular area, such as, for example, [Threats](#_Threat_1) and [Incidents](#_Incident), cross mappings between these specifications were also performed.

Examples:

[STIX](#_STIX), [IODEF](#_IODEF_(Incident_Object), [OpenIOC](#_OpenIOC)

[OpenSAMM](#_OpenSAMM_(Software_Assurance), [BSIMM](#_BSIMM_(Building_Security)

In addition, using emerging (beta) specifications, some work was performed for a **strategic** perspective.

Examples:

Link between [OWASP ASVS](#_OWASP_ASVS_(Application_2) (*web application security requirements checklist*) and [OWASP Testing Guide](#_OWASP_Testing_Project_1) (*WAPT methodology*)

Converting [OWASP ASVS](#_OWASP_ASVS_(Application_1) to [OCIL](#_OCIL_(Open_Checklist)

Drill-down of [WSTC](#_Web_Security_Threat_2)/OWASP TOP 10/CWE/CVE

Some additional efforts are actually performed.

Examples:

Mapping or integration of [BIZEC APP/11](#_BIZEC_APP/11) and [BIZEC TEC/11](#_BIZEC_TEC/11) with [CWE](#_CWE_(Common_Weaknesses).

Mapping between the FIRST CSIRT Case Categories and [VERIS](#_VERIS:_Vocabulary_for_2).

The adopters can also find interest in mapping different [*Repositories*](#_Repositories/Data_Feeds).

Examples:

[CPE](#_CPE_(Common_Platform_2) with Nmap banners

[CPE](#_CPE_(Common_Platform_2) with Default Passwords (DPE)

### Internationalization

The Cyberspace is international.

The Cybersecurity challenge involves collaboration, often across language barriers.

It is of specific concern to the XORCISM project.

The [Country](#_Country) table can be used to create relationships, for example to define [Laws](#_Law_2) applicable in a Country or Region.

For Physical Location purposes, the Country Codes of [ISO 3166](#_ISO_3166_(Country) are used.

See also: Codes for the representation of currencies and funds (ISO 4217:2001)

Example of Cybersecurity internationalization efforts:

SATEC (Static Analysis Technologies Evaluation Criteria)

Spanish Translation: <http://projects.webappsec.org/w/page/69506488/Static%20Analysis%20Technologies%20Evaluation%20%20Criteria%20-%20Spanish>

Russian Translation: <http://projects.webappsec.org/w/page/71979863/Static%20Analysis%20Technologies%20Evaluation%20Criteria%20-%20Russian>

#### Locale

XORCISM introduces [locales](#_Locale_5) to support the internationalization goal (i.e. in the [Description](#_Description_2) of its records).

Examples:

|  |  |  |
| --- | --- | --- |
| Afrikaans - South Africa | 0436 | 1078 |
| Albanian - Albania | 041c | 1052 |
| Alsatian | 0484 | 1156 |
| Amharic - Ethiopia | 045e | 1118 |
| Arabic - Saudi Arabia | 0401 | 1025 |
| Arabic - Algeria | 1401 | 5121 |
| Arabic - Bahrain | 3c01 | 15361 |
| Arabic - Egypt | 0c01 | 3073 |
| Arabic - Iraq | 0801 | 2049 |
| Arabic - Jordan | 2c01 | 11265 |
| Arabic - Kuwait | 3401 | 13313 |
| Arabic - Lebanon | 3001 | 12289 |
| Arabic - Libya | 1001 | 4097 |
| Arabic - Morocco | 1801 | 6145 |
| Arabic - Oman | 2001 | 8193 |
| Arabic - Qatar | 4001 | 16385 |
| Arabic - Syria | 2801 | 10241 |
| Arabic - Tunisia | 1c01 | 7169 |
| Arabic - U.A.E. | 3801 | 14337 |
| Arabic - Yemen | 2401 | 9217 |
| Armenian - Armenia | 042b | 1067 |
| Assamese | 044d | 1101 |
| Azeri (Cyrillic) | 082c | 2092 |
| Azeri (Latin) | 042c | 1068 |
| Bashkir | 046d | 1133 |
| Basque | 042d | 1069 |
| Belarusian | 0423 | 1059 |
| Bengali (India) | 0445 | 1093 |
| Bengali (Bangladesh) | 0845 | 2117 |
| Bosnian (Bosnia/Herzegovina) | 141A | 5146 |
| Breton | 047e | 1150 |
| Bulgarian | 0402 | 1026 |
| Burmese | 0455 | 1109 |
| Catalan | 0403 | 1027 |
| Cherokee - United States | 045c | 1116 |
| Chinese - People's Republic of China | 0804 | 2052 |
| Chinese - Singapore | 1004 | 4100 |
| Chinese - Taiwan | 0404 | 1028 |
| Chinese - Hong Kong SAR | 0c04 | 3076 |
| Chinese - Macao SAR | 1404 | 5124 |
| Corsican | 0483 | 1155 |
| Croatian | 041a | 1050 |
| Croatian (Bosnia/Herzegovina) | 101a | 4122 |
| Czech | 0405 | 1029 |
| Danish | 0406 | 1030 |
| Dari | 048c | 1164 |
| Divehi | 0465 | 1125 |
| Dutch - Netherlands | 0413 | 1043 |
| Dutch - Belgium | 0813 | 2067 |
| Edo | 0466 | 1126 |
| English - United States | 0409 | 1033 |
| English - United Kingdom | 0809 | 2057 |
| English - Australia | 0c09 | 3081 |
| English - Belize | 2809 | 10249 |
| English - Canada | 1009 | 4105 |
| English - Caribbean | 2409 | 9225 |
| English - Hong Kong SAR | 3c09 | 15369 |
| English - India | 4009 | 16393 |
| English - Indonesia | 3809 | 14345 |
| English - Ireland | 1809 | 6153 |
| English - Jamaica | 2009 | 8201 |
| English - Malaysia | 4409 | 17417 |
| English - New Zealand | 1409 | 5129 |
| English - Philippines | 3409 | 13321 |
| English - Singapore | 4809 | 18441 |
| English - South Africa | 1c09 | 7177 |
| English - Trinidad | 2c09 | 11273 |
| English - Zimbabwe | 3009 | 12297 |
| Estonian | 0425 | 1061 |
| Faroese | 0438 | 1080 |
| Farsi | 0429 | 1065 |
| Filipino | 0464 | 1124 |
| Finnish | 040b | 1035 |
| French - France | 040c | 1036 |
| French - Belgium | 080c | 2060 |
| French - Cameroon | 2c0c | 11276 |
| French - Canada | 0c0c | 3084 |
| French - Democratic Rep. of Congo | 240c | 9228 |
| French - Cote d'Ivoire | 300c | 12300 |
| French - Haiti | 3c0c | 15372 |
| French - Luxembourg | 140c | 5132 |
| French - Mali | 340c | 13324 |
| French - Monaco | 180c | 6156 |
| French - Morocco | 380c | 14348 |
| French - North Africa | e40c | 58380 |
| French - Reunion | 200c | 8204 |
| French - Senegal | 280c | 10252 |
| French - Switzerland | 100c | 4108 |
| French - West Indies | 1c0c | 7180 |
| Frisian - Netherlands | 0462 | 1122 |
| Fulfulde - Nigeria | 0467 | 1127 |
| FYRO Macedonian | 042f | 1071 |
| Galician | 0456 | 1110 |
| Georgian | 0437 | 1079 |
| German - Germany | 0407 | 1031 |
| German - Austria | 0c07 | 3079 |
| German - Liechtenstein | 1407 | 5127 |
| German - Luxembourg | 1007 | 4103 |
| German - Switzerland | 0807 | 2055 |
| Greek | 0408 | 1032 |
| Greenlandic | 046f | 1135 |
| Guarani - Paraguay | 0474 | 1140 |
| Gujarati | 0447 | 1095 |
| Hausa - Nigeria | 0468 | 1128 |
| Hawaiian - United States | 0475 | 1141 |
| Hebrew | 040d | 1037 |
| Hindi | 0439 | 1081 |
| Hungarian | 040e | 1038 |
| Ibibio - Nigeria | 0469 | 1129 |
| Icelandic | 040f | 1039 |
| Igbo - Nigeria | 0470 | 1136 |
| Indonesian | 0421 | 1057 |
| Inuktitut | 045d | 1117 |
| Irish | 083c | 2108 |
| Italian - Italy | 0410 | 1040 |
| Italian - Switzerland | 0810 | 2064 |
| Japanese | 0411 | 1041 |
| K'iche | 0486 | 1158 |
| Kannada | 044b | 1099 |
| Kanuri - Nigeria | 0471 | 1137 |
| Kashmiri | 0860 | 2144 |
| Kashmiri (Arabic) | 0460 | 1120 |
| Kazakh | 043f | 1087 |
| Khmer | 0453 | 1107 |
| Kinyarwanda | 0487 | 1159 |
| Konkani | 0457 | 1111 |
| Korean | 0412 | 1042 |
| Kyrgyz (Cyrillic) | 0440 | 1088 |
| Lao | 0454 | 1108 |
| Latin | 0476 | 1142 |
| Latvian | 0426 | 1062 |
| Lithuanian | 0427 | 1063 |
| Luxembourgish | 046e | 1134 |
| Malay - Malaysia | 043e | 1086 |
| Malay - Brunei Darussalam | 083e | 2110 |
| Malayalam | 044c | 1100 |
| Maltese | 043a | 1082 |
| Manipuri | 0458 | 1112 |
| Maori - New Zealand | 0481 | 1153 |
| Mapudungun | 0471 | 1146 |
| Marathi | 044e | 1102 |
| Mohawk | 047c | 1148 |
| Mongolian (Cyrillic) | 0450 | 1104 |
| Mongolian (Mongolian) | 0850 | 2128 |
| Nepali | 0461 | 1121 |
| Nepali - India | 0861 | 2145 |
| Norwegian (Bokmål) | 0414 | 1044 |
| Norwegian (Nynorsk) | 0814 | 2068 |
| Occitan | 0482 | 1154 |
| Oriya | 0448 | 1096 |
| Oromo | 0472 | 1138 |
| Papiamentu | 0479 | 1145 |
| Pashto | 0463 | 1123 |
| Polish | 0415 | 1045 |
| Portuguese - Brazil | 0416 | 1046 |
| Portuguese - Portugal | 0816 | 2070 |
| Punjabi | 0446 | 1094 |
| Punjabi (Pakistan) | 0846 | 2118 |
| Quecha - Bolivia | 046B | 1131 |
| Quecha - Ecuador | 086B | 2155 |
| Quecha - Peru | 0C6B | 3179 |
| Rhaeto-Romanic | 0417 | 1047 |
| Romanian | 0418 | 1048 |
| Romanian - Moldava | 0818 | 2072 |
| Russian | 0419 | 1049 |
| Russian - Moldava | 0819 | 2073 |
| Sami (Lappish) | 043b | 1083 |
| Sanskrit | 044f | 1103 |
| Scottish Gaelic | 043c | 1084 |
| Sepedi | 046c | 1132 |
| Serbian (Cyrillic) | 0c1a | 3098 |
| Serbian (Latin) | 081a | 2074 |
| Sindhi - India | 0459 | 1113 |
| Sindhi - Pakistan | 0859 | 2137 |
| Sinhalese - Sri Lanka | 045b | 1115 |
| Slovak | 041b | 1051 |
| Slovenian | 0424 | 1060 |
| Somali | 0477 | 1143 |
| Sorbian | 042e | 1070 |
| Spanish - Spain (Modern Sort) | 0c0a | 3082 |
| Spanish - Spain (Traditional Sort) | 040a | 1034 |
| Spanish - Argentina | 2c0a | 11274 |
| Spanish - Bolivia | 400a | 16394 |
| Spanish - Chile | 340a | 13322 |
| Spanish - Colombia | 240a | 9226 |
| Spanish - Costa Rica | 140a | 5130 |
| Spanish - Dominican Republic | 1c0a | 7178 |
| Spanish - Ecuador | 300a | 12298 |
| Spanish - El Salvador | 440a | 17418 |
| Spanish - Guatemala | 100a | 4106 |
| Spanish - Honduras | 480a | 18442 |
| Spanish - Latin America | 580a | 22538 |
| Spanish - Mexico | 080a | 2058 |
| Spanish - Nicaragua | 4c0a | 19466 |
| Spanish - Panama | 180a | 6154 |
| Spanish - Paraguay | 3c0a | 15370 |
| Spanish - Peru | 280a | 10250 |
| Spanish - Puerto Rico | 500a | 20490 |
| Spanish - United States | 540a | 21514 |
| Spanish - Uruguay | 380a | 14346 |
| Spanish - Venezuela | 200a | 8202 |
| Sutu | 0430 | 1072 |
| Swahili | 0441 | 1089 |
| Swedish | 041d | 1053 |
| Swedish - Finland | 081d | 2077 |
| Syriac | 045a | 1114 |
| Tajik | 0428 | 1064 |
| Tamazight (Arabic) | 045f | 1119 |
| Tamazight (Latin) | 085f | 2143 |
| Tamil | 0449 | 1097 |
| Tatar | 0444 | 1092 |
| Telugu | 044a | 1098 |
| Thai | 041e | 1054 |
| Tibetan - Bhutan | 0851 | 2129 |
| Tibetan - People's Republic of China | 0451 | 1105 |
| Tigrigna - Eritrea | 0873 | 2163 |
| Tigrigna - Ethiopia | 0473 | 1139 |
| Tsonga | 0431 | 1073 |
| Tswana | 0432 | 1074 |
| Turkish | 041f | 1055 |
| Turkmen | 0442 | 1090 |
| Uighur - China | 0480 | 1152 |
| Ukrainian | 0422 | 1058 |
| Urdu | 0420 | 1056 |
| Urdu - India | 0820 | 2080 |
| Uzbek (Cyrillic) | 0843 | 2115 |
| Uzbek (Latin) | 0443 | 1091 |
| Venda | 0433 | 1075 |
| Vietnamese | 042a | 1066 |
| Welsh | 0452 | 1106 |
| Wolof | 0488 | 1160 |
| Xhosa | 0434 | 1076 |
| Yakut | 0485 | 1157 |
| Yi | 0478 | 1144 |
| Yiddish | 043d | 1085 |
| Yoruba | 046a | 1130 |
| Zulu | 0435 | 1077 |
| HID (Human Interface Device) | 04ff | 1279 |

References:

<http://msdn.microsoft.com/en-gb/goglobal/bb964664.aspx>

<https://en.wikipedia.org/wiki/IETF_language_tag>

<https://www.iana.org/assignments/language-subtag-registry/language-subtag-registry>

<http://www.w3.org/International/articles/language-tags/>

*Note:* [*NVD*](#_NVD:_National_Vulnerability) *provides an XML feed for translations of* [*CVE*](#_CVE:_Common_Vulnerabilities) *vulnerabilities into other languages.*

#### Description

XORCISM uses a [Description](#_Description) table, linked to other tables, to be able to describe data in various *languages* ([Locales](#_Locale)).

See also the tables Name and Title.

### Use Cases

XORCISM can be used for a wide range of use cases.

Use Cases MAY be found in the documentation of the used Specifications/Standards.

Examples:

* Asset Management (including authorized and unauthorized IT Assets, lifecycle, accountability)
* Enable interoperability among security products (conformance)
* Data correlation, repository
* Educate vendors on best practices
* Security Advisory Distribution
* Continuous Vulnerability Assessment and Remediation
* Patch Management
* Configuration Management
* Auditing and Centralized Audit Validation
* Security Information Management Systems (SIMS)
* System Inventory
* Malware Defense and Threat Indicator Sharing
* Incident Response
* Application Software Security
* Advanced analytics

References:

<https://oval.mitre.org/adoption/usecasesguide.html>

For validation purposes, use cases defined by the IETF SACM Working Group were also used.

<https://ietf.org/wg/sacm/>

Other examples:

* Becoming “CWE-Compatible”
* Building an OVAL Repository

<https://github.com/athiasjerome/XORCISM/tree/master/XORCISMOVAL>

* Cyber Peacefare
* Digital Forensics
* Mitigation and Remediation
* Predictive Security

See also:

**Twenty Critical Security Controls for Effective Cyber Defense**

<https://www.sans.org/critical-security-controls/>

### Benefits

#### Information Correlation

While XORCISM was designed using **standardized structured data** specifications, **data normalization** and easy bindings [6] was found to be very practical.

Also the **aggregation** of data from various sources and formats (i.e. CSV, XML, JSON) in a normalized structured representation offers multiple advantages.

It was possible to obtain relationships between information coming from different sources/repositories.

Examples:

Relationship between:

* An exploit code, posted into a mailing list, containing a [Reference](#_Reference) to a particular URL (but no CVE ID or official vendor URL)
* A CVE, containing a [Reference](#_Reference) to [OSVDB](#_Open_Sourced_Vulnerability), itself containing a [Reference](#_Reference) to the same URL

Relationship between:

* A Threat Actor, identified in the past by an Organisation A to have used a Malware containing a particular Mutex
* A new Malware found by Organisation B containing a similar Mutex

To ensure **Interoperability**, and facilitate **Data Sharing**, various data models were used and in some cases redesigned or extended.

Examples:

The [XORCISM Vulnerability Data Model](#_XORCISM_Vulnerability_Data).

**Data marking** (with the use of [Tags](#_Tag)) facilitates the search functionalities.

References:

Exploiting a Thesaurus-Based Semantic Net for Knowledge-Based Search

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.7197&rep=rep1&type=pdf>

Bloom filters

<https://en.wikipedia.org/wiki/Bloom_filter>

See also [Categories](#_Category_4), Importance

[6] Bindings Examples:

TAXII Bindings Specifications

<http://taxii.mitre.org/specifications/index.html>

#### Data interexchange

XORCISM facilitates interchange of structured data, by offering an easy and extensible way for serializing and de-serializing structured data. (i.e.: [XML](#_XML:_Extensible_Markup) and [JSON](#_JSON:_JavaScript_Object) format)

The use of specifications and standards during the conception of XORCISM makes it directly and easily usable (compatible) with, for example: [IODEF](#_IODEF_(Incident_Object_1), [RID](#_RID:_Real-time_Inter-network) or [STIX](#_STIX_(Structured_Threat_1), [TAXII](#_TAXII_(Trusted_Automated) for **data sharing**.

Note: The use of [Protocol Buffers](#_Protocol_Buffers) was found to be relevant and interesting during XORCISM implementation experiments in terms of speed (small and fast).

Due to the high volume of data in some cases, and scale needs, implementers are invited to take into consideration the use of optimized protocols/frameworks/functions.

While providing operational implementation details is out of scope of this document, some links are provided “as is”:

Version Control

<http://git-scm.com/book/en/Getting-Started-About-Version-Control>

For CPU bound applications, Python is magnitudes slower than compiled languages. The primary advantage of interpreted languages is development speed.

Data Structures/Stacks and Queues

<http://en.wikibooks.org/wiki/Data_Structures/Stacks_and_Queues>

Data Parallelism

<http://www.quora.com/What-is-the-exact-difference-between-parallel-and-concurrent-programming>

ØMQ

<http://zguide.zeromq.org/page:all>

<http://www.rabbitmq.com/getstarted.html>

<https://github.com/stucco/docs>

TCMalloc : Thread-Caching Malloc

<http://google-perftools.googlecode.com/svn/trunk/doc/tcmalloc.html>

Selecting Mathematical Models With Greatest Predictive Power: Finding Occam's Razor in an Era of Information Overload

<http://www.sciencedaily.com/releases/2013/11/131120103619.htm>

Cybersecurity Algorithms, Techniques Being Developed Through Anthropology Methods

<http://www.sciencedaily.com/releases/2013/11/131107103406.htm>

Regular Expression (Regex) and Patterns

#### Expandability

XORCISM is easily extensible.

Extensibility is important to ensure the support of organization-specific data.

##### Example: Extension of the [Device](#_Device_1) table.

For being more granular in the description of a Device, the following tables can be used:

DEVICECOMPONENT: this table allows the description of Devices’ Components

This should be, for example, a [Requirement](#_Requirement) for **Supply Chain Assurance**.

Examples of such are: SIM Card, Transistor, and Processor

Then, another table could be additionally used (using inheritance) to also describe the potential Components of a Device’s Component:

DEVICECOMPONENTFORDEVICECOMPONENT

By using unique identifiers (IDs and GUIDs), one could obtain the following tables:

DEVICE

DEVICECOMPONENT  
DEVICECOMPONENTFORDEVICE  
DEVICECOMPONENTFORDEVICECOMPONENT

Which could be extended by adding another concept:

DEVICE   
DEVICE**BLACKLIST**   
DEVICECOMPONENT

DEVICECOMPONENT**BLACKLIST**  
DEVICECOMPONENTFORDEVICE  
DEVICECOMPONENTFORDEVICECOMPONENT

DEVICECOMPONENT**WHITELIST**

DEVICE**WHITELIST**

Note: This mechanism can be used to extend currently available [Specifications](#_Specifications_and_Standards,)

(i.e.: <https://tools.ietf.org/html/rfc5209>)

New attributes/properties could be added, such as Size (Length/Width/Height), Weight or Color.

Then relationships to entities such as Software, Driver, Firmware, Code, etc. can be created.

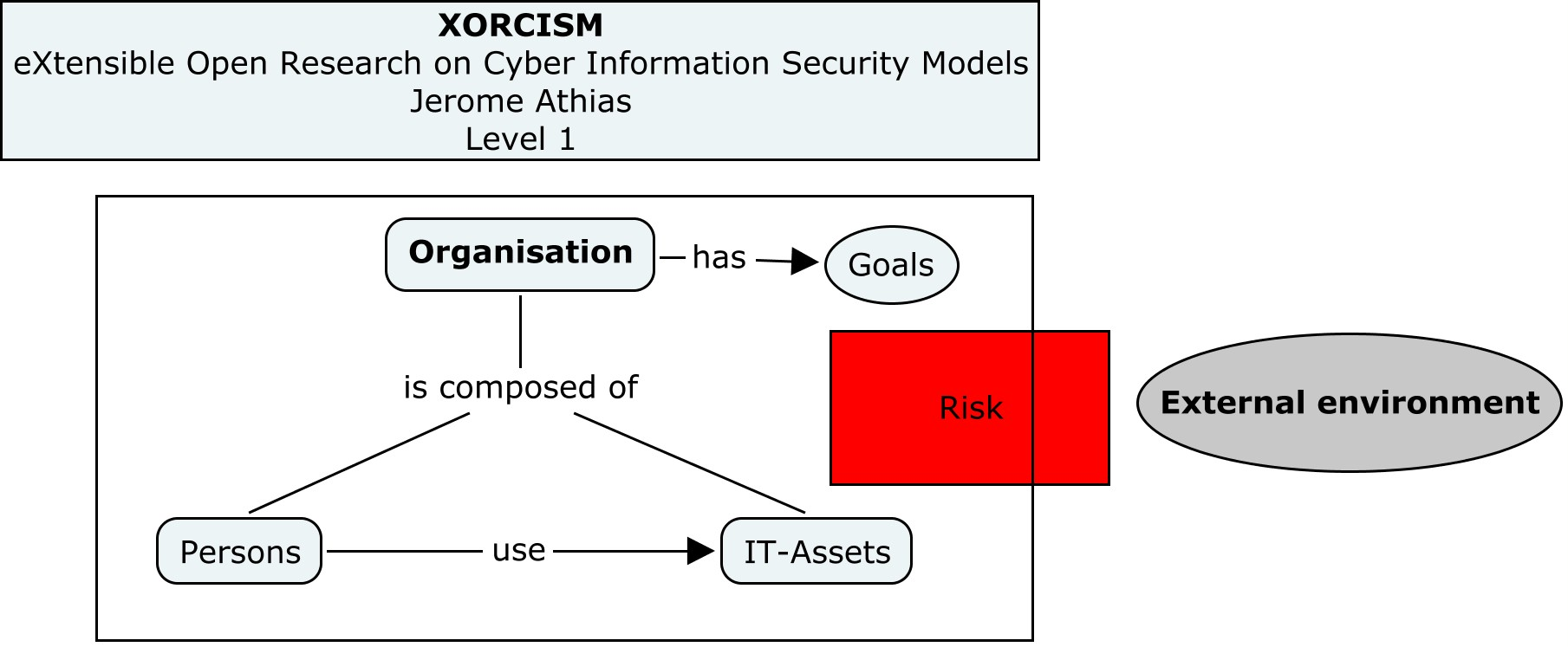
#### Knowledge Database

[Tips](#_Tip_1) and Tricks for **Security Awareness** can be stored in an XORCISM database.

See also the [Recommendation](#_Recommendation) table.

### XORCISM Core Entities

#### XORCISM Level 01



Cyber Security involves various parties.

It is important for an organisation to identify its dependencies, and its mission drivers (i.e. [laws](#_Law_4) and regulation, [policies](#_Policy_2)).

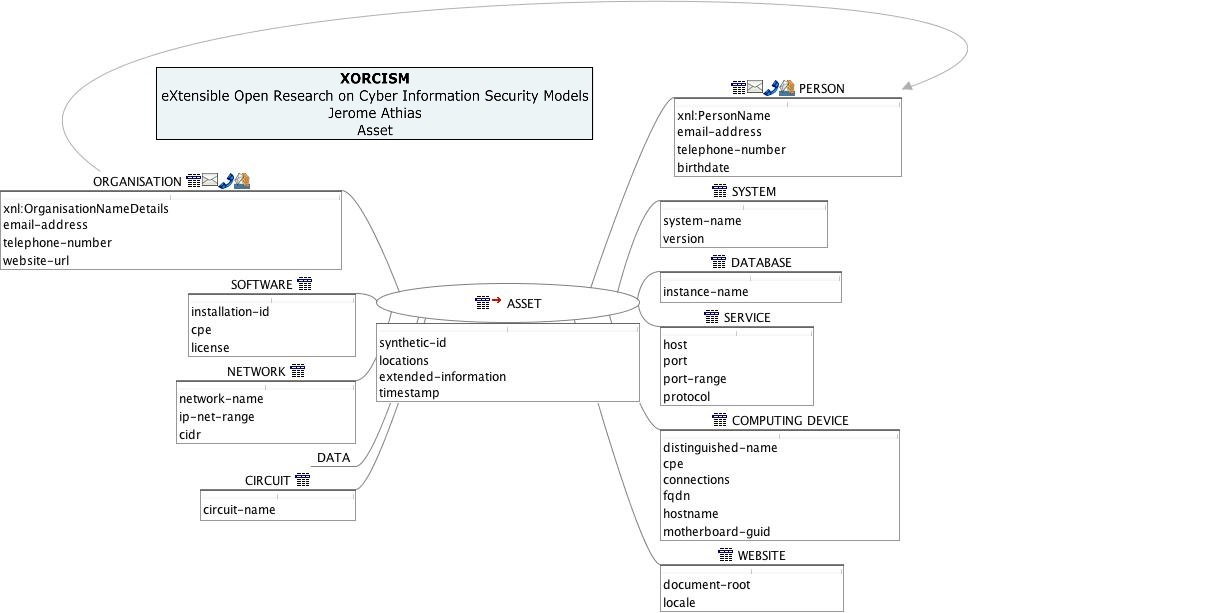
It is recommended to have operational situation awareness of the desired and current state of physical and logical assets.

The three top-level core entities of XORCISM are:

1. [**Organisations**](#_Organisation_(Organization)) **(Organizations)**
2. [**Persons**](#_Person)
3. [**IT Assets**](#_IT_Asset)

These entities are described in XORCISM mainly using the [Asset Identification specification](#_Asset_Identification) [5].

##### XORCISM Assets



Information about assets can be described and exchanged using the [Asset Reporting Format (ARF)](#_Asset_Reporting_Format) [6].

**Asset Management** (AM) is the first Category of the first Function (IDENTIFY) of the (*Preliminary*) [Cybersecurity Framework](#_Cybersecurity_Framework) [7] Core.

Informative References from the Cybersecurity Framework are:

[ISA 99.02.01 (ANSI/ISA-99.02.01-2009)](#_ISA_99.02.01)

[COBIT](#_COBIT)

[ISO/IEC 27001](#_ISO/IEC_27001)

[NIST SP 800-53 Rev. 4](#_NIST_SP_800-53)

[CCS (Council on CyberSecurity)](#_CCS)

[NIST SP 500-291](#_NIST_SP_500-291)

[NIST SP 800-34](#_NIST_SP_800-34)

See also:

<https://en.wikipedia.org/wiki/Asset_management>

<http://measurablesecurity.mitre.org/directory/areas/assetmanagement.html>

For Physical Location purposes, the **Country Codes** of [ISO 3166](#_ISO_3166_(Country) are used.

##### Organisation (Organization)

Note: Use of [ORGANISATION instead of ORGANIZATION](http://grammarist.com/spelling/organise-organize/), as per [OASIS xNL](https://www.oasis-open.org/committees/ciq/ciq.html) used in [Asset Identification](#_Asset_Identification_(AI)_1).

See: <http://grammarist.com/spelling/organise-organize/>

“An Organisation could be: Company (i.e. Enterprise, Commercial, Non Commercial), Institution (i.e. University, School), Not for Profit, Association (i.e. Club), Public Service (i.e. Railway Station, Post Office), a Group (i.e. Standard body), etc. “, OASIS CIQ V2.0

An Organisation could have various [Organizational Units](#_Organizational_Units) (i.e.: Business Units), like Divisions and Departments.

For Physical Location purposes, the Country Codes of [ISO 3166](#_ISO_3166_(Country) are used.

For Classification, the North American Industry Classification System (NAICS) is actually used.

<http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012>

See also: <http://schema.org/Organization>

##### Person

Various Persons (Individuals/People) are linked to Organisations and IT Assets.

**Resources Management** is fundamental for any Organisation.

These Persons could be part of various **Persons Groups**.

For example, in the Forensic domain, a Person could be an Attorney, an Investigator, a Witness, etc.

Persons can be targeted by **Social Engineering** attacks.

For Physical Location purposes, the Country Codes of [ISO 3166](#_ISO_3166_(Country) are used.

##### IT Asset

Cyber Security involves many various different IT Assets.

These can be classified (as per [Asset Identification](#_Asset_Identification_(AI)_2)) into the following:

1. System
2. Computing Device
3. Software
4. Service
5. Website
6. Database
7. Network
8. Circuit
9. Data

Note: For Physical Location purposes, the Country Codes of [ISO 3166](#_ISO_3166_(Country) are used.

#### XORCISM Level 02

##### Organizational Units

An Organisation could have various Organizational Units (i.e.: Business Units), like Divisions and Departments.

##### Persons Groups

Persons could be part of different Persons Groups.

##### System

In the “internet of things”, various types of systems can be found.

Examples:

Servers, Laptops, Workstations

Operating Systems, Database Systems, Machines (including SCADA, ATMs and Embedded systems)

##### Computing Device

**Hardware**, as opposed to [Software](#_Software_2)

See also [Device](#_Device)

**Physical Inventory Maintenance**

##### Software

**Backup**, **Recovery**…

**Software Configuration Management, Software Assurance, Software License Inventory, Software Flaw Scanning**

References:

<https://en.wikipedia.org/wiki/Software_configuration_management>

<http://measurablesecurity.mitre.org/directory/areas/softwareassurance.html>

##### Service

##### Website

##### Database

**Database Flaw Scanning**

##### Network

Network Mapping and Discovery provides, for example: **Asset Management**, **Rogue Asset Detection**, **Physical Inventory Maintenance**

##### Circuit

##### Data

### XORCISM Normalized/Standardized Entities/Objects

#### CAPEC

Attack Patterns

<http://capec.mitre.org/>

#### CCE

Unique Identifiers for Common System Configuration Issues

<https://nvd.nist.gov/cce/index.cfm>

#### CPE (Common Platform Enumeration)

A structured naming scheme for IT systems, platforms, and packages

<https://nvd.nist.gov/cpe.cfm>

See also SWID Tags

#### CVE (Common Vulnerabilities and Exposures)

Security related software flaws.

<https://cve.mitre.org/>

#### CWE (Common Weakness Enumeration)

#### CybOX Objects

#### WASC

### XORCISM Vulnerability Data Model

The author has developed a customized Vulnerability Data Model.

A number of considerations were made in the design of the Data Model.

This model can serve as a transport format.

The XORCISM Vulnerability Data Model (XVDM) has been intensively tested in automation scenarios.

The following tools and resources (*list not exhaustive*) were used during the data model validation phases\*:

Acunetix

Arachni

Burp

Cenzic Hailstorm

Code Profiler

GoLismero

IBM AppScan

McAfee Database Security Scanner (DSS)

McAfee Vulnerability Manager (MVM)

Metasploit Framework (MSF)

NVD (CVE)

OpenVAS

OWASP ZAP

Qualys

Rapid7 NeXpose

Tenable Nessus

***All trademarks and registered trademarks are the property of their respective owners.***

\* [Specific Tools](#_XORCISM_Tools)/Classes/[APIs](#_API) such as parsers, dissectors and aggregators were developed to support bindings, parsing and import/export of the data exchanged (in various, not standardized, often proprietary, formats) with the tools listed above.

Various Vulnerability models and exchange formats were analyzed.

Examples:

CVRF (Common Vulnerability Reporting Framework)

<http://www.icasi.org/cvrf>

IETF Vulnerability Data Model (VDM)

<http://tools.ietf.org/html/draft-booth-sacm-vuln-model-02>

[Intermediary Vulnerability Information Language (IVIL)](http://www.cupfighter.net/index.php/2010/10/ivil-an-xml-schema-to-exchange-vulnerability-information/)

<http://www.cupfighter.net/index.php/2010/10/ivil-an-xml-schema-to-exchange-vulnerability-information/>

They were found not optimal for on-disk storage, long-term archiving, or in-memory processing.

Note: CVSS actually included in the Vulnerability table, users could decide to use the SCORINGSYSTEM table instead.

[TODO] Include full specification.

### XORCISM Key Entities/Objects/Concepts/Properties

The following list is based on the number of direct relationships that these elements have with others in XORCISM (and not by importance, i.e. [Threats](#_Threat)).

The **Integrity** of these data is consequently very important.

(List provided in alphabetical order)

#### Reference

XORCISM largely relies on references (*links*) for data correlation.

A Reference could be an [URL](#_URL) or a path to a [File](#_File).

References such as to **Security Principles** and **Best Practices** are crucial for Cyber Security.

Examples:

<https://www.owasp.org/index.php/Category:Principle>

<https://www.owasp.org/index.php/Application_Security_Architecture_Cheat_Sheet>

<https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet>

<https://www.owasp.org/index.php/Secure_Coding_Cheat_Sheet>

<https://www.owasp.org/index.php/Cheat_Sheets>

<https://www.owasp.org/index.php/Category:OWASP_Video>

Relationships with other XORCISM tables are made using the **ReferenceID** key.

Note: The author also recommends using the **ReferenceGUID** property.

The References could be classified by Categories, i.e. Software Assurance (Swa).

Note: Reference is also used to identify the Source (resource) of information.

#### Vocabulary

Proper **Classification** is very important to obtain **Statistics** and **Metrics**.

Examples:

Web Application Security Statistics

WASC using the [Web Security Threat Classification](#_Web_Security_Threat)

<http://www.webappsec.org/projects/statistics/>

<http://www.microsoft.com/en-sg/download/details.aspx?id=39680>

<http://www.govloop.com/profiles/blogs/the-govloop-guide-winning-the-cybersecurity-battle>

The Vocabularies used (if not internal ones) come from various [**Repositories**](#_Repository_1).

**The Vocabulary table is actually used in XORCISM to store information about Ontologies, Taxonomies, Classifications and Vocabularies without a real distinction.**

Relationships with other XORCISM tables are made using the **VocabularyID** key.

Note: The author also recommends using the **VocabularyGUID** property.

See also [Category](#_Category_3)

### XORCISM Internal Entities/Objects/Concepts/Properties

Note: some of the following entities/properties are also used by some specifications/standards.

#### CREATIONOBJECT

This table is used to capture XORCISM’s records creation.

For database’s **Integrity**.

*Note: This table could be renamed as CREATIONRECORD*

Note: The author recommends using this table in addition (and NOT in replacement) of the DBMS, System and other logs.

The following related table is also proposed: CREATIONRECORDHASH, it could be used for Integrity verification, for example, if the database is replicated.

#### CHANGERECORD

This table is used to capture XORCISM’s records modification.

It is useful for database’s **Integrity**.

Note: The author recommends using this table in addition (and NOT in replacement) of the DBMS, System and other logs.

#### ACCESSRECORD

This table can be used to capture when, by whom, and how a XORCISM record was accessed.

This can be used for **Logging** and **non-repudiation**.

Note: This is NOT intended to replace or offer a better mechanism than DBMS, System or other logs.

The following related tables are also proposed: ACCESSRECORDEVIDENCE and ACCESSRECORDHASH.

NB: This table could be used solely, by capturing the records’ GUIDs, or could be attached (by creating a relationship) with some specific, or all, other tables. *(i.e.: CREDENTIALACCESSRECORD)*

#### GUIDs

Actually open to the choices of adopters.

Synthetic IDs.

Examples: attributes *@indicator-uid* and *@indicator-set-id* in [IODEF](#_IODEF_(Incident_Object_3) (RFC5070).

See also DIDA, SACM, Alternative IDs.

#### CreatedDate

This property is used to capture and store the date and time when a record was created into the database.

This can be used for sorting data (or for future cleanup).

This can also be used to maintain **Integrity** by comparing this value to database/system events and logs.

#### timestamp

A timestamp to specify the date and time when an information/record was last modified into the database.

This can be used for sorting data (or for maintenance).

This can also be used to maintain **Integrity** by comparing this value to database/system events and logs.

#### ValidFromDate

Date and time specifying the starting date and time of validity of an information/record.

Note: the CreatedDate or timestamp value could be used by default.

This can be used to store information that will be used in the future (i.e.: definition of an upcoming Version of a Software, or future Location of a Sensor to perform Attack Surface analysis in advance).

#### ValidUntilDate

Optional date and time to specify that an information/record is/will be valid until this date and time.

Note: This can be used to keep a history of the information/records, as a filter for softwares consuming the database, or for future cleanup of the database.

#### LastCheckedDate

Optional timestamp to capture the last date and time an information/record was checked/verified to be accurate.

*Note: This can help to maintain* ***Integrity*** *of the data.*

#### CollectionMethod

Specifying, for example, if an information/record was collected automatically (i.e. by a Sensor) or manually is interesting to capture.

#### ConfidenceLevel

XORCISM tends to enforce the specification of the level of confidence, or confidence assertion into the information/record.

A use case example is that information collected via a software (i.e.: an Automated Vulnerability Scanner) could obtain a lower confidence level (due to potential false positives) than information collected and verified by a human.

*Note: This can help to maintain* ***Integrity*** *of the data.*

Care must be taken in automation scenarios to ensure an appropriate level of confidence to the data prior to perform [Actions](#_Action_1).

#### ConfidenceReason

Explicitly specifying the reason why a confidence level was attributed to an information/record (i.e.: verified manually, or captured by 3 different sensors, or same result with 5 different tools) is interesting for analysts, **reliability** and **consistency**.

Furthermore, this can help in decision-making and automated [Actions](#_Action).

#### ConfidentialityLevel

This can be used to maintain **Confidentiality**, for example, to avoid unintended access or sharing of information with unauthorized users or third parties (***Data Leakage***).

Note: see also [isEncrypted](#_isEncrypted)

#### Restriction

Data access restrictions can be defined in XORCISM by using this entity.

Example: Selective Sharing

Note that **Access Control Lists** (ACL) can also be used as an additional security mechanism.

Objective: protecting data-at-rest, data-in-use, data-in-transit

#### Source

Source of information. (Repository, Reference, Organisation, Person, Sensor, etc.)

#### Tag

Data marking is important for correlation and search functionalities.

It can also be used for various mechanisms, i.e. intended use.

A tagging approach is included in XORCISM.

References:

<https://en.wikipedia.org/wiki/Bloom_filter>

Exploiting a Thesaurus-Based Semantic Net for Knowledge-Based Search

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.7197&rep=rep1&type=pdf>

See also [Keyword](#_Keyword)

#### Importance

XORCISM offers the possibility to define the importance of information.

This could be used during **Data Processing**, i.e. for **Prioritization**.

#### TrustLevel

XORCISM tends to enforce the specification of the level of trust into the information/record.

Useful for **Trust Management**.

A use case example is for automation purposes: information (i.e.: fix script for a configuration issue) with a low level of trust should not be processed automatically (without user interaction) by software.

#### TrustReason

XORCISM tends to enforce the specification of a reason why the information/record is trusted.

#### isEncrypted

boolean/bit to indicates if the content of a XORCISM’s record is encrypted for **Confidentiality** purposes.

Data that can be encrypted could be: Name, Description, GUID, Password, etc.

Note: the type of Encryption is not specified/stored at the database level for security reason; the users of an XORCISM database should manage this level of encryption, for example, at the application level.

PS: The use of strong Encryption mechanisms, at various levels/layers is strongly recommended, such as, but not limited to, Hard Disk encryption, Database Encryption, Transport Encryption. Other **Data Protection** mechanisms are also strongly recommended.

See [Encryption](#_Encryption)

See also: [ACL](#_ACL), [Restriction](#_Restriction), [Classification Level](#_Classification_Level), [Clearance](#_Clearance), Hash, [X509 Certificate](#_X509_Certificate)

### XORCISM Other Entities/Objects/Concepts/Properties

The list provided here is NOT exhaustive. Please kindly see the Technical Documentation if needed.

#### Account

Example: Windows User Account

#### ACL

Access Control Lists

<https://en.wikipedia.org/wiki/Access_control_list>

Note: An ACL could be a list of Access Control Entries (ACE)

<http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx>

See also Firewall Rules

#### Acronym

#### Action

Decidability

Measures, i.e.: <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf>

#### Address

Examples:

IPv4 address

IPv6 address

See: CybOX Adress Object

#### Advisory

Multiple vendors publish security advisories, bulletins, alerts or notes related to bugs, vulnerabilities, patches or security configuration.

As these advisories are currently not standardized, it is difficult to define a structured data representation of the information contained in the bulletins.

It is recommended, for now, to use the relationship with the [Reference](#_Reference_1) table.

Examples:

<https://www.us-cert.gov/ncas/bulletins>

#### Alert

Generation of Alerts, for example, by a SIEM [Sensor](#_Sensor), configuration change from a baseline, etc.

This table could be used by an application (i.e. a web-based front-end) to manage various alerts.

#### API

Application Programming Interface, type of Software

Examples: DLL, ESAPI

#### Application

[Code](#_Code_1), [API](#_API_1), [Technologies](#_Technology) and [Platforms](#_Platform_1) ([CPE](#_CPE_(Common_Platform_3)), Revision and Versioning

**Application Security** (APPSEC), Security Requirements, [SDLC](#_Secure_Development_Life), Audit, Code Analysis, Code Review, Penetration Testing, WAPT

#### Artefact

Reference: Malware, see [MAEC](#_MAEC_(Malware_Attribute)

#### Assurance

Example: [Software Assurance](#_Software_Assurance_1) (SwA)

#### Attack Category

Examples:

* Brute Force: Is an exhaustive attack that works by testing every possible value of a parameter (password, file name, etc.)
* Cache Poisoning: Is an attack that seeks to introduce false or malicious data into a web cache, normally via HTTP Response Splitting.
* DNS Poisoning: Is an attack that seeks to introduce false DNS address information into the cache of a DNS server, where it will be served to other users enabling a variety of attacks. (e.g., Phishing)

References:

<https://www.owasp.org/index.php/Category:Attack>

See [Attack Pattern](#_Attack_Pattern) and [CAPEC](#_CAPEC).

#### Attack Pattern

“An "attack pattern" is an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed. Each pattern defines a challenge that an attacker may face, provides a description of the common technique(s) used to meet the challenge, and presents recommended methods for mitigating an actual attack. Attack patterns help categorize attacks in a meaningful way in an effort to provide a coherent way of teaching designers and developers how their systems may be attacked and how they can effectively defend them.” MITRE

See [CAPEC](#_CAPEC).

#### Attack Surface

XORCISM offers mechanisms to define and help to reduce efficiently the Attack Surface.

Example: Reverse Threat Modeling

[TODO] Add details

#### Biometric

Identity Management

#### Breach

See Intrusion, Compromise

#### Bulletin

Security Bulletin

See [Advisory](#_Advisory)

#### Category

**Data Classification** is important; it helps for example to obtain Statistics and [Metrics](#_Metric).

XORCISM makes use of a Category table, which can be used and linked (*using inheritance*) to other Categories tables (as opposite of an [abstraction](#_Abstraction) approach) to categorize the different objects/entities, when relevant.

#### Campaign

**Attack Scenarios** like **Threat Campaigns** conducted by **Adversaries** such as [Threat Actors](#_Threat_Actor_1) (i.e.: Cyber criminals or Terrorists).

Reference: [STIX](#_STIX_(Structured_Threat)

Examples: Aurora

#### Certification

**Product Certification**, **Professional Certification, Compliance Certification**

#### Classification Level

Example: Data Classification

[TODO] Add enumerations examples

#### Clearance

#### Code

Source Code is produced using various programming [Languages](#_Language_1) and used in various [Scripts](#_Script), [Applications](#_Application) and [Softwares](#_Software_1), and so different [Products](#_Product_1) for multiple [Platforms](#_Platform) and [Devices](#_Device_2).

**Source Control** and [Versioning](#_Version) ([Version Control](#_Version_Control)) of code in [Repositories](#_Repository_2) are important.

**Code Review** and Analysis must be performed as part of a **Secure Development Life Cycle** (SDLC).

Various [Tools](#_Tool_1) are available to perform **Static and Dynamic Source Code Scanning and Analysis**.

**Security Principles**, **Best Practices** and **Standards** must be known (***Developers Security Awareness and Training Programs***), properly used and verified to reach adequate Security Requirements.

This can, for example, help to: reduce the **Attack Surface**, reach **Compliance** or obtain **Quality** ([Software Assurance](#_Software_Assurance)) and **Security Certifications**.

XORCISM can be used to define [Strategies](#_Strategy_1), assess and measure the quality and security of various codes by managing different [Projects](#_Project_1).

Furthermore, XORCISM can be used as a [**Knowledge Database**](#_Knowledge_Database). (Misuse Cases, Methodologies, Techniques, Code Snippets, Demonstrative Examples, CWE, Tips, Recommendations, etc.)

*Potentially* [*Exploit*](#_Exploit) *Code.*

See also [Script](#_Script_1)

Notes:

The number of Lines of Codes (CODELINE) can be used in [Metrics](#_Metric_1).

Code is using various Functions.

#### Command

In XORCISM, mainly used for Operating Systems Commands.

*In opposed to Chain of Command*

Examples:

apt-get update

yum update

wp plugin update --all

*Reference:* [*http://wp-cli.org/commands/plugin/update/*](http://wp-cli.org/commands/plugin/update/)

for i in G M K; do du -ah | grep [0-9]$i | sort -nr -k 1; done | head -n 11

See also [Script](#_Command)

#### Compliance

Conformity to Compliances and Directives, like **Regulatory Compliances**, are very important, as there can be a significant [Impact](#_Impact) in case of [Violation](#_Finding).

Examples:

* **Safety Compliance** (CAN/CSA-C22.2 No. 60950-1, UL 60950-1, CE Compliance for Europe, EMC Directive 2004/108/EC)
* **HIPAA** requires certain healthcare providers to implement technical safeguards to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network, including encryption of data where appropriate.
* The IT Control Objectives of **Sarbanes-Oxley** (**SOX**) similarly that when appropriate, public companies should 'determine if encryption techniques are [to be] used to support the confidentiality of financial information sent from one system to another.
* PCI DSS

See also [Laws](#_Law), Regulation and [Certification](#_Certification)

#### Country

For [Physical Location](#_Physical_Location), or [Geo Location](#_Geo_Location) purposes, the Country Codes of [ISO 3166](#_ISO_3166_(Country) are used.

Note: users could decide to create [Groups](#_Group) of Countries or to add tables like Region (i.e.: Europe)

#### Course of Action (COA)

References: [STIX](#_STIX_(Structured_Threat)

#### Course of Law (COL)

Examples: Forensics

#### Description

Description of a record, that can be made in multiple *languages*.

XORCISM makes use of [Locales](#_Locale_1) for **Internationalization**.

Note: the XORCISM Database (SQL Creation Script) include descriptions of the properties, such as the descriptions found in the documentation of the specifications and standards used.

#### Device

Electronic Devices, i.e. Smartphone, USB Devices, Keyboard, Mouse, Arduino, Teensy, Jammer, Bluetooth Devices, Antenna, etc.

Important, for example, for: **Mobile Security**

See also: Firmware, Driver

#### Devices’ Components

Processor, Cell, Capacitor, SIM card, Memory modules

The identification and tracking of Devices’ Components is important for example in a [Supply Chain](#_Supply_Chain_1).

#### Document

**Documentation**, and **Data Classification** is very important for the Documents manipulated by Organizations.

Examples:

**Baselines, Policies, Mutual Non-Disclosure Agreement, Warranty, Directive or Circular**

See also: [File](#_File_2)

#### Domain

Example: Domain Name

See also: Whois

#### Driver

Software often distributed with Hardware.

See also: Firmware, Cybox/MAEC

#### Effect

#### Encryption

Used in Cryptography, i.e. Symmetric key encryption, Public key encryption

Examples:

PGP

[Encryption using Chaos](#_Encryption_Using_Chaos_1)

Homomorphic Encryption

[XML Encryption](#_XML_Encryption)

References:

<https://en.wikipedia.org/wiki/Encryption>

Please make sure to see also [Laws](#_Law_3).

[TODO] Add examples and references

#### Endpoint

In XORCISM, an Endpoint is actually defined as a termination point (*by analogy: a human nerve termination, Synapse Receptor*).

Example:

Service X Version 1.3 *(Web Server CPE:aaa:bbb:ccc serving the SOAP API Version 2.5 of a Web Service of the Application ABC Version 1.2.3 written in PHP Version 5.3, using the Functions Fa, Fb, Fc… defined in the File websvc.wsdl… using Code making calls to the PHP language Functions PHPA(), PHPB()…)* listening on Port TCP/80 served by the Device: Network Card Y having the MAC Address 1:2:3:4:5 of the Asset GUID: XOR:WEBSERVER123 accessed in Zone: DMZ via the ip-address-ipv4 10.11.12.13.

Note: Could be more granular than RFC5209 <https://tools.ietf.org/html/rfc5209>

See also Connection\_End\_Point in NDDM.

#### Event

Examples: DHCP event, Registry modified

See [STIX](#_STIX_3)

#### Evidence

Digital Evidence, for example, used in Chain of Custody, Chain of Evidence (Forensics)

#### Exploit

Reference:

<http://www.exploit-db.com>

#### Exploit Target

The Victim of an Attack through the use of an Exploit Code, Target of Exploitation *(via a Vulnerability with Exposure)*.

Examples:

Organization

Asset

ip-address-IPv4

Service

Endpoint

#### Factory

“A factory (previously manufactory) or manufacturing plant is an industrial site, usually consisting of buildings and machinery, or more commonly a complex having several buildings, where workers ([Persons](#_Person_1)) manufacture [goods](https://en.wikipedia.org/wiki/Good_(economics)) (i.e. [Products](#_Product) like [Computing Devices](#_Computing_Device) or [Softwares](#_Software)) or operate machines ([Systems](#_System)) processing one product into another.” Wikipedia

<https://en.wikipedia.org/wiki/Factory>

Information about Factories, and how they are managed by Organisations are important, for example, in the [Supply Chain](#_Supply_Chain) domain. (i.e. Contraband)

In XORCISM, relationships exist, for example, between Factory, [Devices](#_Device_3) (and Components), [Assurance](#_Assurance), [Compliance](#_Compliance), [Policy](#_Policy).

#### File

Organisations manipulate a large spectrum of Files and [Documents](#_Document), of various **types** and **formats**.

Examples:

Executable

Archives

EPub

Image Files (Pictures with EXIF data, QRcodes, etc.)

Media Files (Videos from Surveillance Systems, Audio Files, etc.)

Microsoft Office Files (Word, Excel, etc.)

PCAP

PDF Files

Prefetch

Files are concerned by multiple concepts, such as **Data Classification**, **Confidentiality**, **Privacy**, **Integrity**, **and Availability**.

**Digital Rights Management** (DRM) and **Intellectual Property Protection** are also applicable.

XORCISM relies mainly on the files’ descriptions of [CybOX](#_CybOX) and [MAEC](#_MAEC).

See also:

<https://en.wikipedia.org/wiki/Revision_control>

#### Finding

During the conduct of a Project, various findings can come up.

Examples:

Violation of **Privacy**, [Policy](#_Policy_1), [Compliance](#_Compliance_2) or [Law](#_Law_1) during an **Investigation** or **Audit**.

Vulnerabilities found during an **Audit**, **Code Review** or **Penetration Test**.

#### Firmware

*Note: Could contain a Backdoor*

#### Frequency

#### Geo Location

GPS coordinates, i.e. lagitude/longitude

See also the LocationPoint table, with elevation and radius

#### Group

Examples: Person Group, Asset Group, Software Group

#### Guideline

“Guidelines are general recommendations or instructions that provide a framework for achieving compliance with one or more Policies.  They use terms such as "should" and "should not" and are not by themselves enforceable.  Guidelines are usually tailored to a specific technology or environment.  As a result, Guidelines are reviewed and updated more frequently than Policy.” CMU

Examples:

<https://www.cmu.edu/iso/governance/guidelines/index.html>

#### Identification System

Identity Management

#### Impact

See [VERIS](#_VERIS:_Vocabulary_for)

#### Incident

See [IODEF](#_IODEF_(Incident_Object_2), [STIX](#_STIX_1), [VERIS](#_VERIS:_Vocabulary_for_1)

#### Indicator

Atomic, Computed, or Behavioral. Example: IOC (Indicator of Compromise)

#### Infrastructure

Critical Infrastructures, Power grids, Dams

Examples: [CAESARS](#_CAESARS_(Continuous_Asset_1), [CDXI](#_CDXI), [SARA](#_Situational_Awareness_Reference)

#### Keyword

See also [Tag](#_Tag_2)

#### Kill Chain

Example: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, C2, Actions on Objectives

See also F2T2EA

Reference: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin Corporation

#### Language

Programming languages.

[C, C++, Objective C](#_C-Based_Toolchain_Hardening), [.NET](#_.NET_Security_Cheat), [SQL](#_SQL_Injection_Prevention), High Performance Fortran, Data Parallel Haskell, Cython, etc.

As opposed as [Locale](#_Locale_3)

#### Law

Laws, Regulations and [Compliances](#_Compliance_1) are very important. Avoiding **Legal Issues** is critical.

“Many countries around the world have similar laws.

* European Union Directive 95/46/EC, Chapter I, Article 17 requires that Member States provide that the controller implement appropriate technical and organizational measures to protect personal data against accidental or unlawful or unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network.
* A 1999 Royal Decree from Spain requires that any sensitive data may only be transmitted through telecommunications networks if it has been previously encrypted or made illegible to any unauthorized third party.

Many companies have worked to ensure the security of their data stored within the enterprise. However, in an environment in which company personnel more frequently bring their own devices, the question remains: 'what happens after I hit send?” Silent Circle

But different Countries also have different Laws.

Examples:

Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (France)

<http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf>

Cable Act, 47 U.S.C. $551

References:

<https://silentcircle.com/web/encryption-laws/>

#### License

This table can be used to store information about Serial Numbers or Softwares’ Licenses.

References:

<http://opensource.org/licenses>

Examples:

* [Apache License 2.0](http://opensource.org/licenses/Apache-2.0)
* [BSD 3-Clause "New" or "Revised" license](http://opensource.org/licenses/BSD-3-Clause)
* [BSD 2-Clause "Simplified" or "FreeBSD" license](http://opensource.org/licenses/BSD-2-Clause)
* [GNU General Public License (GPL)](http://opensource.org/licenses/gpl-license)
* [GNU Library or "Lesser" General Public License (LGPL)](http://opensource.org/licenses/lgpl-license)
* [MIT license](http://opensource.org/licenses/MIT)
* [Mozilla Public License 2.0](http://opensource.org/licenses/MPL-2.0)
* [Common Development and Distribution License](http://opensource.org/licenses/CDDL-1.0)
* [Eclipse Public License](http://opensource.org/licenses/EPL-1.0)

#### Locale

<http://msdn.microsoft.com/en-gb/goglobal/bb964664.aspx>

#### Message

SMS, MMS, TAXII message, etc.

#### Meta Data

#### Method

Examples:

##### HTTPMethod

Examples:

GET, POST

HEAD, PUT, OPTIONS, DELETE, TRACE, TRACK, COPY, MOVE, LOCK, UNLOCK, PROPFIND, PROPPATCH, SEARCH, MKCOL, CONNECT

See also [OCTAVE](#_OCTAVE)

#### Methodology

Defining or/and using Methodologies and [Guidelines](#_Guideline) is important in Cyber Security, i.e. for Risk Assessment.

The [OWASP Testing Project](#_OWASP_Testing_Project) ([OWASP Testing Guide](https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents)), [Open Source Security Testing Methodology Manual (OSSTMM),](#_Open_Source_Security) or [Penetration Testing Execution Standard (PTES)](#_Penetration_Testing_Execution) are examples.

References:

Information Risk Analysis Methodology (IRAM)

<https://www.securityforum.org/tools/isf-risk-manager/>

#### Metric

Important for **Security Governance**.

Examples:

* Percentage of source traffic covered by foundational cyber defense assets in DMZs
* Currency of enterprise virus signatures
* Percentage of client systems that have current enterprise virus signatures
* Percentage of desktops with automated patching
* Percentage of desktops with automated integrity checking
* Volume of traffic blocked at border router (segmented by type)
* Blocked port scan volume at border router
* Currency of firmware patches for foundational cyber defense assets
* Known zero day export exposure (publicly known)
* Uptime and availability for assets
* Number of cyber attacks that are detected: Viruses, spam, phishing attacks, etc.
* Assets not patched to current standard
* Firmware not updated to enterprise standards
* Assets failing integrity check
* Non-standard software installations detected
* Known zero-day exploit exposure (publicly known)
* Currency of required administrator training
* Vulnerability scan statistics
* Source code scan results (where available and applicable)

References:

GovLoop, Jim Richmann

<https://benchmarks.cisecurity.org/downloads/metrics/>

<http://www.webappsec.org/projects/statistics/>

#### Motivation

Example: [Threat Actor](#_Threat_Actor_2)’s Motivations

See [STIX](#_STIX_4)

#### Notification

#### Objective

Examples: Business Objectives

#### Ontology

See [Taxonomy](#_Taxonomy) and [Vocabulary](#_Vocabulary_1)

#### Patch

Important for remediation of bugs, weaknesses and vulnerabilities.

Virtual Patch (WAF)

#### Phase

[TODO] Ref NIST

#### Physical Location

Examples:

Work area, Building, Room, Partner facility, Personal residence, Public facility, Data Center

#### Plan

Examples:

**Business Continuity Plan**

**Disaster Recovery Plan**

**Incident Response Plan**

**Contingency Planning** (i.e. Redundancy)

Note: A Plan can be materialized by a [Document](#_Document_1), and consequently by a [File](#_File_1).

A Plan can define [Procedures](#_Procedure_2), and involve various [Projects](#_Project) and [Strategies](#_Strategy).

#### Platform

[TODO]

See [CPE](#_CPE_(Common_Platform_1)

#### Policy

Used to improve business performance.

Examples:

**Password Security Policy**

**Privacy Policy**

**Workstation Security Policy**

**Physical Security Policy**

**Internet Access (at Work) Policy**

<https://www.cmu.edu/iso/governance/index.html>

**Harassment Avoidance Policy**

**Anti-Corruption Policy**

**BYOD**

XORCISM makes policies storage, management, control and enforcement easier in a centralized manner.

#### Port

Example: TCP/21, UDP/53

See also Port List

#### Procedure

Example: Procedures for Evidence Collection

*Used in place of* [*Protocol*](#_Protocol_1)*.*

*See also* [*Process*](#_Process)

#### Process

Operational aspects

People, Process, Technology, Environment

Examples:

[CLASP](#_CLASP:_Comprehensive,_Lightweight)

See also: CybOX Process Object (i.e. Unix Process)

#### Product

Organizations interact with various Products, like [Computing Devices](#_Computing_Device) or [Softwares](#_Software).

Products **Security Evaluation** is important.

References:

Web Application Security Evaluation Criteria, WASC

“The Web Application Security Evaluation Criteria is a set of guidelines to evaluate web application security scanners on their identification of web application vulnerabilities and its completeness.” WASC

<http://www.webappsec.org/projects/wassec/>

Web Application Firewall (WAF) Evaluation Criteria, WASC

“The goal of this project is to develop a detailed web application firewall (WAF) evaluation criteria; a testing methodology that can be used by any reasonably skilled technician to independently assess the quality of a WAF solution.” WASC

<http://www.webappsec.org/projects/wafec/>

Note: Products’ support period is good to know.

#### Profile

[TODO]

#### Project

Organizations and Persons will manage and be involved in various Cyber Security Projects.

Examples are **Security Awareness**, **Incident Response**, **Forensic Investigation**, **Malware Analysis**, **Penetration Tests**, etc.

XORCISM includes the concept of Project and related entities such as Tasks or Schedules.

However Project Management is currently not fully in scope, and consequently there is a lack in, for example, Cost and Performance management.

#### Protocol

IANA

Examples: Security Protocols (TLS), DHCP *(DHCP server logging)*, DNS, IRC

See Port

*See also* [*Procedure*](#_Procedure)

#### RACIMatrix

<https://en.wikipedia.org/wiki/Responsibility_assignment_matrix>

#### Recommendation

See also [Tip](#_Tip)

[Internationalization](#_Internationalization): Recommendations can be stored in different *languages* (see [Description](#_Description_1) and [Locales](#_Locale_4))

#### Registry Key

Root Folders, Registry Path, File Path, Hive, Key Cell (offsets, LastWrite), Value Cell, Subkey List Cell, Value List Cell, Security Descriptor Cell

See CybOX/MAEC

#### Report

#### Repository

XORCISM allows storing information related to [Repositories](#_Repositories,_Data_Feeds).

Examples:

[OVAL Repository](#_OVAL_Repositories)

[SCAP Repository](#_SCAP_Repositories)

[Tools Repository](#_Tools_Repositories)

Note: It is interesting, for example, to easily obtain information such as [References](#_Reference_2) or [Confidence](#_ConfidenceLevel)/[Trust](#_TrustLevel) levels about repositories.

#### Request

Examples:

Change Request (for configuration, review, approval, documentation) (see Waiver)

HTTP Request/Session

#### Requirement

The definition of Security Requirements is important for Organisations for quality, security, privacy, etc.

In the Software (and Application) domain, for example, Organisations can use [OWASP ASVS](#_OWASP_ASVS_(Application) or CERT.org’s [SQUARE](#_SQUARE_(Security_Quality) for security improvement of their own softwares, but also off-the-shelf ones, to reach security goals (confidentiality, availability, integrity, accountability, and assurance).

#### Restriction

Example: Need to Know

Utilization Examples: IODEF

Could be used in the Chain of Trust <http://en.wikipedia.org/wiki/Chain_of_trust>

#### Risk Rating

The Risk Rating depends of the Factors used in the [Methodology](#_Methodology).

**Risk Management**, **Risk Tolerance**, **Risk Assessment**

#### Script

Lines of Code (*CODELINE*) written in a [Programming Language](#_Language_2), using various Commands and or Functions and potentially having various Parameters.

[Code](#_Code) used for, by example; **System Configuration**, **Audit of Compliance**, **Database Management**

**Hardening Scripts, Fix Scripts**.

Examples:

Bash Script

PERL Script

SQL Script

Utilization Examples: OVAL

#### Security Principle

Security Principles and Good Practices are fundamental.

By collecting and documenting them in a XORCISM database, Organization can easily manage them and use them to spread good knowledge, for example, during Security Awareness and Prevention Programs.

Examples:

**Avoid Security by Obscurity**

**Backup**

**Input Sanitization (Don’t Trust User Input)**

**Keeping Softwares Up-to-date**

**Least Privilege**

**Logging**

**Network Segmentation**

**Prevent, Detect, Contain, and Recover**

**Privileges Separation**

**Separation of Duties**

**Whitelisting**

References:

<https://www.owasp.org/index.php/Category:Principle>

<http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>

#### Sensor

Sensors, such like IDS, IPS or Honeypot, are important [IT Assets](#_IT_Asset_1) in term of security.

Example:

Sensor Taxonomy extracted from the [DHS](#_DHS:_Department_of) [CAESARS](#_CAESARS_(Continuous_Asset) architecture specification.

* FDCC Scanner
* Authenticated Configuration Scanner
* Authenticated Vulnerability Scanner
* Authenticated Patch Scanner
* Network Management Tool
* Unauthenticated Vulnerability Scanner
* Web Vulnerability Scanner
* Database Vulnerability Scanner
* System Management Tool
* Anti-Virus Tool

#### Service

Examples:

FTP Server

SSH Server

VPN Server

Web Server

Note: can cover Social Networks (**Privacy**)

#### Severity

See Scoring System (i.e. [CVSS](#_CVSS_(Common_Vulnerability), [CWSS](#_CWSS:_Common_Weakness))

#### Standard

Various Cyber Security Standards coexist, evolve and are created continuously.

See the list of [Cyber Security Standards](#_Specifications/Standards/Frameworks/Met_) provided in this document.

It is very important to use them, and for this, organizations have to be aware of their existence.

XORCISM allows the possibility to build a **Repository of Standards** that can be easily managed, updated and exchanged.

#### Statute

Examples: Wirestap Statute, Pen Registers and Trap and Trace Devices

#### Strategy

Examples:

**Defense-in-Depth**

Defining Web Application Security Requirements using OWASP ASVS, Using the OWASP ESAPI to help reach these Requirements, Assessing the Security of these Web Applications with the OWASP Testing Guide for WAPT, Acquiring a Source Code Analysis Tool to improve Code Review as part of the SDLC improvement, Evaluate the Organization Maturity with OpenSAMM before moving to BSSIM, while performing PCI DSS assessment of the e-commerce Web Applications, and then try to reach an ISO Compliance.

#### Supply Chain

##### Supply Chain Assurance

“Organizations are increasingly acquiring commercial-off-the-shelf and open source software products or outsourcing development. Current approaches to acquisition don’t account for the risk management issues of complex software supply chains. On-time delivery and costs often get attention, but some of the most serious risks are related to system assurance, the confidence that the system behaves as expected. Software defects, such as design and implementation errors, can lead to unexpected behaviors, system failure, or vulnerabilities that can lead to attacks.” CERT.org

<http://www.cert.org/sse/supplychain.html>

In XORCISM, a relationship exists between **Supply Chain** and [Assurance](#_Assurance_1).

Use cases: Software Development Outsourcing

##### Supply Chain Risk

References:

**Supply Chain Risk Management**: Enabling Transparency for Informing Decision-Making in Reducing Residual Risk Exposures, DHS

<http://csrc.nist.gov/scrm/documents/workshop_oct2012/jarzombek_ict_supply_chain_workshop_oct-15-2012.pdf>

<https://buildsecurityin.us-cert.gov/swa>

#### Tactic

**Adversaries** such as [Threat Actors](#_Threat_Actor) can elaborate and use Tactics to perform Attacks (such as Social Engineering, Phishing, DDoS, etc.) during [Campaigns](#_Campaign).

Tactics, Techniques and Procedures (TTP)

Examples:

Define Target (i.e. Energy sector)

Find accomplices (i.e. Recruitment in Africa, using Virtual Currencies)

Organize accomplices (i.e Manager o Trojan Command and Control, Campaign Manager, Stolen Data Reseller)

Build or acquire tools (i.e. Blackmarket Exploit Kits)

Research target infrastructure/employees (i.e. ShodanHQ, LinkedIn)

Test for detection (i.e.: Upload feature with EICAR, WAF checks)

Deployment (i.e.: spear phishing, Java Drive-by-download)

Initial intrusion (i.e. Blind SQL Injection)

Implant

Outbound connection initiated (i.e. Use of Bulletproof hosting)

Expand access and obtain credentials (i.e. using pass-the-hash, Mimikatz/Veil)

Internal reconnaissance (i.e.: Meterpreter)

Move laterally (i.e. Pivot)

Strengthen foothold (persistent backdoor)

Exfiltrate data (i.e. using a DNS or NTP exfiltration Technique)

Cover tracks and remain undetected (i.e. change access dates using timecomp, NTFS ADS)

Reference:

<http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threats/understand-threat/>

#### Taxonomy

See [Vocabulary](#_Vocabulary)

#### Technique

Example: Obfuscation

See also [Tactic](#_Tactic) (TTP)

#### Technology

Organizations use and develop multiple and various technologies, offering different levels of security.

Examples:

Certificate Trust

Full Disk Encryption

Virtualization

Cloud Computing

Microsoft Group Policy (GPO)

[Samsung KNOX](#_KNOX:_Samsung_KNOX)

[FIDO](#_FIDO:_Fast_Identity)

[OAuth](#_OAuth_(Open_standard)

[OpenID](#_OpenID)

[Encryption Using Chaos](#_Encryption_Using_Chaos)

XML Encryption

Specific technologies can be used, for example, in the context of **Privacy**.

References:

<https://silentcircle.com/web/technology/>

#### Threat

“Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events.” NIST SP800-27

A growing sophistication of **Cyber Threats** has been recently observed. The Threat Landscape is quickly changing.

XORCISM is intended to help in the **Threat Intelligence** area.

References:

<http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape>

<http://www.govloop.com/profiles/blogs/the-govloop-guide-winning-the-cybersecurity-battle>

See also [Appendix A: Threats Taxonomies Examples](#_Appendix_A:_Threats)

#### Threat Actor

**Adversaries**

Examples: Cyber criminals, Hacktivists, Terrorists

Reference: [STIX](#_STIX_(Structured_Threat), VERIS

#### Ticket

Ticket as used, for Ticket Tracking, examples: in **Defect Tracking Systems**, **Incident Handling** and **Ticketing Systems**.

References:

<https://en.wikipedia.org/wiki/Bug_tracking_system>

<https://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/at_download/fullReport>

#### Tip

Tips can be particularly useful for **Security Awareness** programs and **Cyber Hygiene**.

Examples:

* Set strong passwords, change them regularly, and don’t share them with anyone.
* Keep your operating system, browser, and other critical software optimized by installing updates.
* Maintain an open dialogue with your friends, family, colleagues and community about Internet safety.
* Use privacy settings and limit the amount of personal information you post online.
* Be cautious about offers online – if it sounds too good to be true, it probably is.

<http://www.dhs.gov/stopthinkconnect-cyber-tips>

Spear Phishing - Understanding the Threat, [CPNI](#_CPNI:_United_Kingdom's)

<http://www.cpni.gov.uk/advice/cyber/spear-phishing/>

Avoiding Social Engineering and Phishing Attacks, US-CERT

<http://www.us-cert.gov/ncas/tips/ST04-014>

HTTPOnly can be set at the Application level AND at the Web Server level.

<http://believeinmiraclesx.wordpress.com/2013/11/19/isapi-filter-set-httponly-for-mulitple-cookies/>

Block egress traffic to known malicious IP addresses and domains.

Block dynamic DNS providers.

#### Tool

Many various [**Security Tools**](#_Other_Security_Tools_1) are available.

This includes **Attack Tools** and **Defense Tools**. (Where some could be in both [Categories](#_Category_1))

XORCISM offers the possibility, for example, to store Tools’ [Licenses](#_License).

#### Training

Trainings are important for **Security Awareness** (i.e. Courses, Workshops, Webinars, Seminars and Conferences) and **Certification Programs**.

*Note: the Training table could be a “duplicate” of the Project table, and so could be removed in a future version*

#### Transaction

Fraud Management

#### URL

The URL object/entity is often used directly (as a property inside another object/entity data structure), and in place of an URI object, i.e. in [Reference](#_Reference_3).

#### Version

Versioning is important in various areas.

Examples:

Versions of Documents, Files

Versions of Policies, Compliances, Standards, Vocabularies

Versions of Softwares, Applications

XORCISM offers the possibilities to capture and manage the different versions of its entities.

#### Vulnerability

“A weakness in system security requirements, design, implementation, or operation, that could be accidentally triggered or intentionally exploited and result in a violation of the system’s security policy.” NIST SP800-27

It is critical to act for the **Mitigation**, and **Remediation** of Vulnerabilities.

**Vulnerability Management** and **Patch Management** are essential for Cyber Security.

Different [Strategies](#_Strategy_2) could be adopted.

See [XORCISM Vulnerability Data Model](#_XORCISM_Vulnerability_Data_1)

#### Weakness

See also [CWE](#_CWE_2)

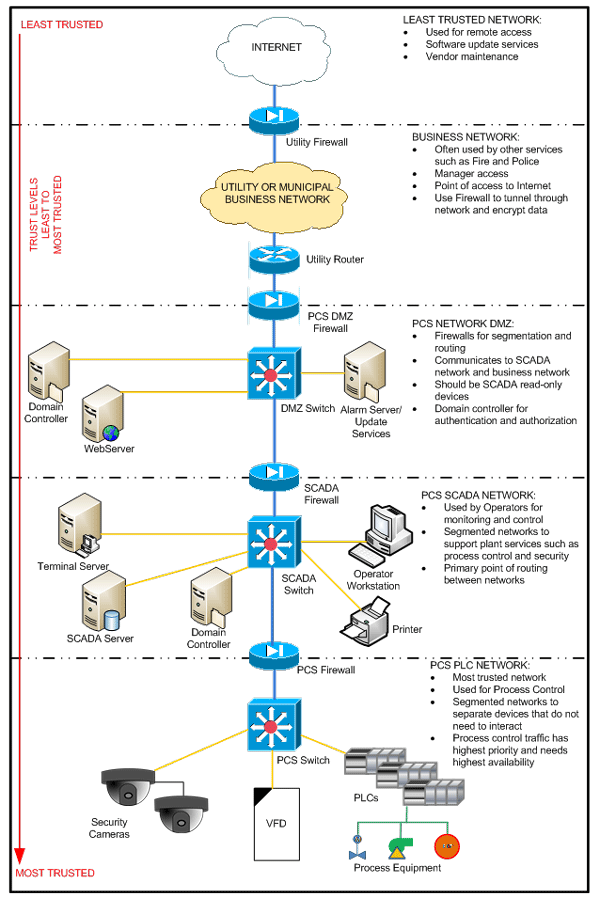
#### X509 Certificate

#### Zone

IT Assets could be in various Zones for Layered Protections (From Least to Most Trusted)

Examples:

DMZ, DMZ Zone *X*, Intranet, DNS split-horizon, WAN/LAN



*Source:* [*http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=94401*](http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=94401)

## Specifications/Standards/Frameworks/Methodologies/Guidelines/Models/Languages/Formats

[Tip](#_Tip_2): Use XORCISM to store the following information and classify them by [Categories](#_Category_6). You can also use [Tags](#_Tag_1).

### Architectural Model

Dr Cohen

<http://all.net/Arch/index.html>



*Source: Dr. Cohen* [*http://all.net/Arch/index.html*](http://all.net/Arch/index.html)

### Asset Identification (AI)

NIST

<http://scap.nist.gov/specifications/ai/>

“Asset identification plays an important role in an organization's ability to quickly correlate different sets of information about assets. This specification provides the necessary constructs to uniquely identify assets based on known identifiers and/or known information about the assets. This specification describes the purpose of asset identification, a data model for identifying assets, methods for identifying assets, and guidance on how to use asset identification. It also identifies a number of known use cases for asset identification.” NIST

[Asset Identification 1.1 Schema](http://scap.nist.gov/schema/asset-identification/1.1/asset-identification_1.1.0.xsd) (XSD 1.0)

[Asset Identification Specification](http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7693)

### Asset Reporting Format (ARF)

NIST

<http://scap.nist.gov/specifications/arf/>

“The Asset Reporting Format (ARF) is a data model to express the transport format of information about assets, and the relationships between assets and reports. The standardized data model facilitates the reporting, correlating, and fusing of asset information throughout and between organizations. ARF is vendor and technology neutral, flexible, and suited for a wide variety of reporting applications.” NIST

### Asset Summary Reporting (ASR)

NIST

<http://scap.nist.gov/specifications/asr/>

### AWS Security Best Practices

Amazon Web Services & AWS Security Best Practices

<https://s3.amazonaws.com/awsmedia/AWS_Security_Best_Practices.pdf>

### BSIMM (Building Security In Maturity Model)

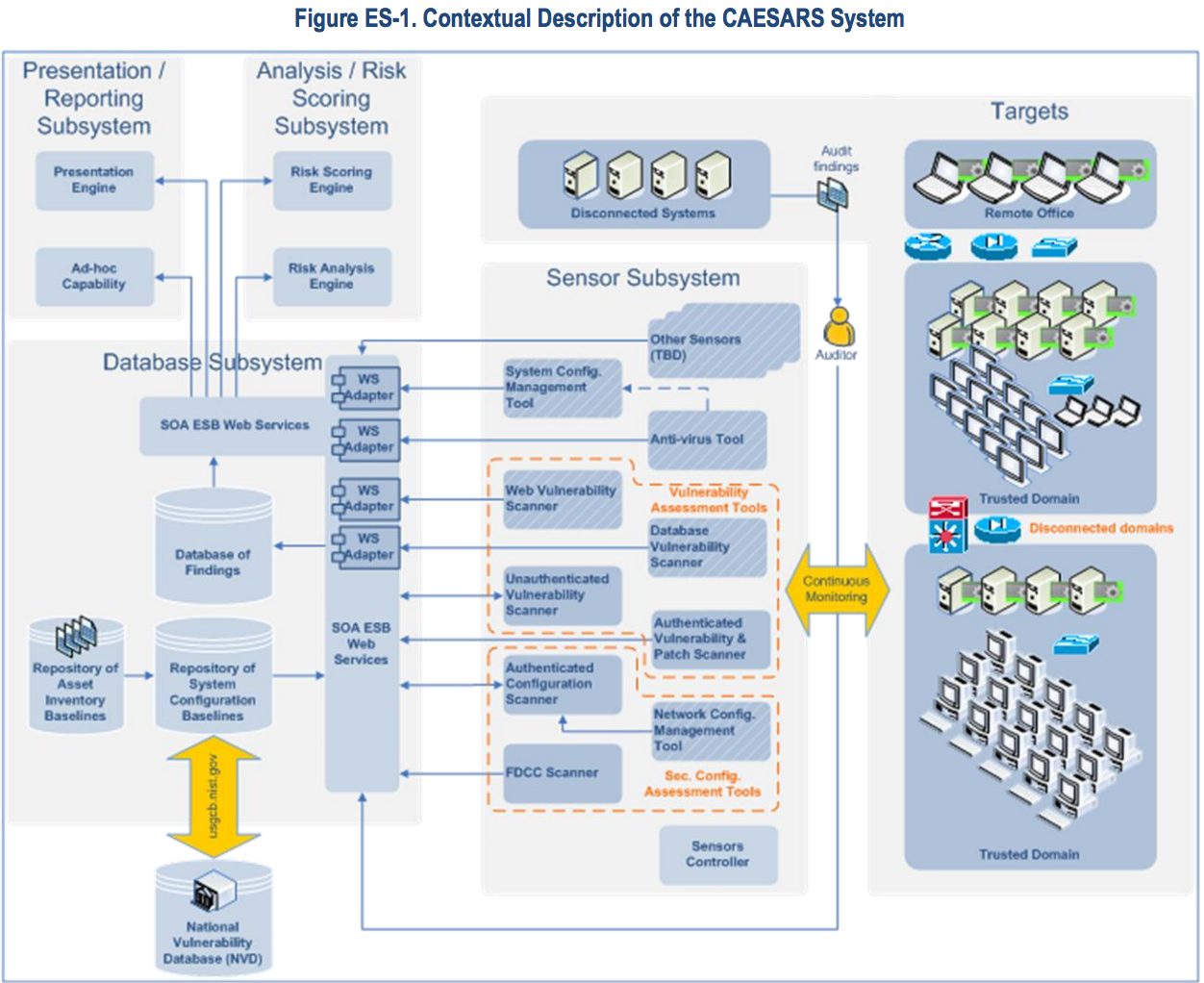
<http://bsimm.com/>

### Build Security In (BSI)

<https://buildsecurityin.us-cert.gov/>

### CAESARS (Continuous Asset Evaluation, Situational Awareness, and Risk Scoring) architectural reference

<http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf>



*Source: DHS* [*https://www.dhs.gov/xlibrary/assets/fns-caesars.pdf*](https://www.dhs.gov/xlibrary/assets/fns-caesars.pdf)

### CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model

NISTIR-7756

<http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf>

### CAP: Common Alerting Protocol

"The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks." [3] CAP was developed by the Organization for the Advancement of Structured Information Standards (OASIS).

<https://www.oasis-open.org/committees/download.php/14759/emergency-CAPv1.1.pdf>

### CAPEC: Common Attack Pattern Enumeration and Classification

“International in scope and free for public use, CAPEC is a publicly available, community-developed list of common attack patterns along with a comprehensive schema and classification taxonomy. Each attack pattern captures knowledge about how specific parts of an attack are designed and executed, providing the attacker’s perspective on the problem and the solution, and gives guidance on ways to mitigate the attack’s effectiveness. Attack patterns help those trying to defend against attacks better understand the specific elements of an attack and how to stop them from succeeding.” MITRE

<http://capec.mitre.org/>

### CCE (Common Configuration Enumeration)

Unique Identifiers for Common System Configuration Issues

<http://nvd.nist.gov/cce/index.cfm>

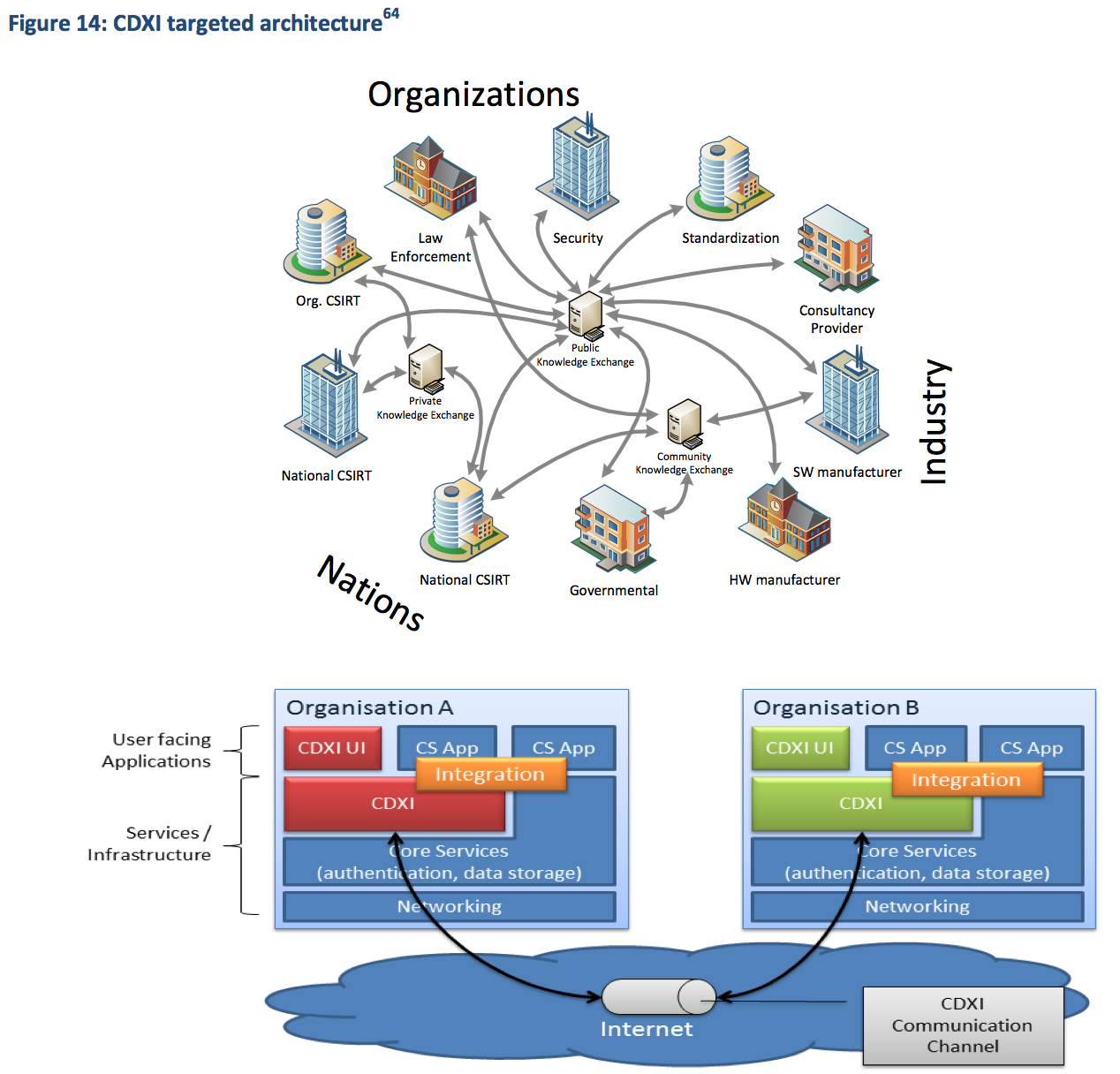
### CCS (Council on CyberSecurity)

Council on CyberSecurity

<http://www.counciloncybersecurity.org/>

### CDXI

ENISA



Source: ENISA <http://www.slideserve.com/nalani/cyber-defence-data-exchange-and-collaboration-infrastructure-cdxi>

### CEE (Common Event Expression)

A Unified Event Language for Interoperability

<http://cee.mitre.org/>

### CERT Resilience Management Model (CERT-RMM)

“The CERT Resilience Management Model is a capability model for operational resilience management. It has two primary objectives:

Establish the convergence of operational risk and resilience management activities such as security, business continuity, and aspects of IT operations management into a single model.

Apply a process improvement approach to operational resilience management through the definition and application of a capability level scale that expresses increasing levels of process improvement.”

<https://www.cert.org/resilience/rmm.html>

### Collective Intelligence Framework (CIF)

### CIS Benchmarks

Center for Internet Security

<https://benchmarks.cisecurity.org/downloads/benchmarks/>

### CloudAudit

Cloud Security Alliance (CSA)

<https://cloudsecurityalliance.org/research/cloudaudit/>

“The goal of CloudAudit is to provide a common interface and namespace that allows enterprises who are interested in streamlining their audit processes (cloud or otherwise) as well as cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology.” CSA

### Cloud Controls Matrix (CCM)

Cloud Security Alliance (CSA)

Security Controls Framework for Cloud Providers and Consumers

<https://cloudsecurityalliance.org/research/ccm/>

### Cloud Trust Protocol (CTP)

Cloud Security Alliance (CSA)

Promoting Elements of Transparency in the Cloud

<https://cloudsecurityalliance.org/research/ctp/>

### COBIT

ISACA

<http://www.isaca.org/COBIT/Pages/default.aspx>

“A Business Framework for the Governance and Management of Enterprise IT.” ISACA

### Common Configuration Scoring System (CCSS)

### [Common Remediation Enumeration (CRE)](http://scap.nist.gov/specifications/cre/)

“The Common Remediation Enumeration (CRE) is part of an emerging suite of enterprise remediation specifications that enable automation and enhanced correlation of enterprise remediation activities. Each CRE entry represents a unique remediation activity and is assigned a globally unique CRE identifier (CRE-ID).” NIST

<http://scap.nist.gov/specifications/cre/>

### Consensus Assessments Initiative (CAI) Questionnaire

<https://cloudsecurityalliance.org/research/cai/>

### COSO

### CPE (Common Platform Enumeration)

A structured naming scheme for IT systems, platforms, and packages

<https://nvd.nist.gov/cpe.cfm>

### CVE (Common Vulnerabilities and Exposures)

Security related software flaws.

<https://cve.mitre.org/>

### CVRF (Common Vulnerability Reporting Framework)

“The ICASI Common Vulnerability Reporting Framework (CVRF) is an XML-based language that enables different stakeholders across different organizations to share critical security-related information in a single format, speeding up information exchange and digestion. CVRF is a common and consistent framework for exchanging not just vulnerability information, but any security-related documentation.”

<http://www.icasi.org/cvrf>

### 

*Source:* [*http://www.icasi.org/cvrf-1.1-mindmap*](http://www.icasi.org/cvrf-1.1-mindmap)

### CVSS (Common Vulnerability Scoring System)

CVSS-SIG

“CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability.” FIRST

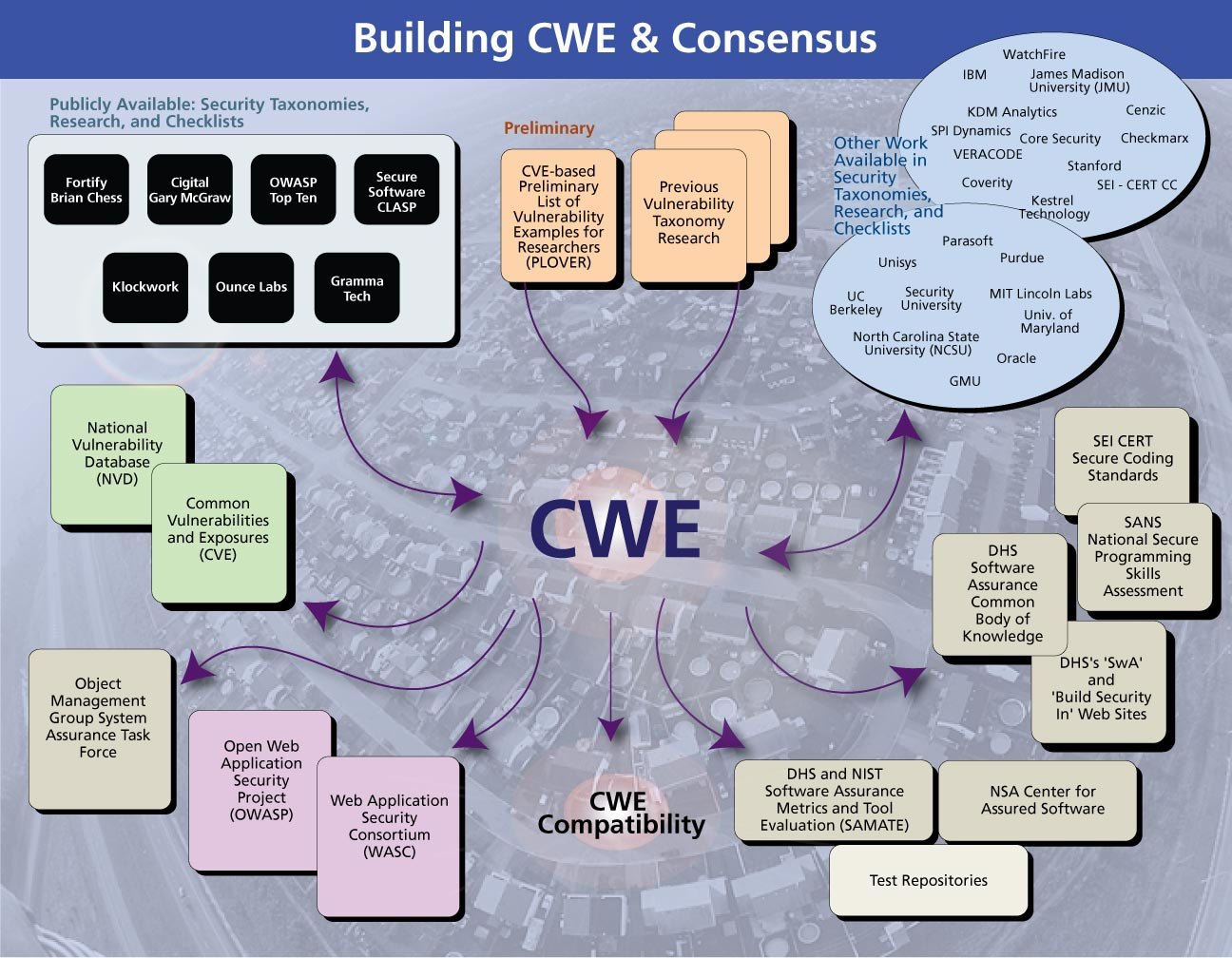
<http://www.first.org/cvss>

### CWE (Common Weaknesses and Exposures)

Software Weaknesses Types

<http://cwe.mitre.org/>

“International in scope and free for public use, CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.” MITRE



*Source:* [*http://cwe.mitre.org/about/images/lg\_consensus.jpg*](http://cwe.mitre.org/about/images/lg_consensus.jpg)

#### CWE/SANS Top 25 Most Dangerous Software Errors

<http://cwe.mitre.org/top25/index.html>

### CWRAF: Common Weakness Risk Analysis Framework

<http://cwe.mitre.org/cwraf/>

“CWRAF provides a framework for scoring software weaknesses in a consistent, flexible, open manner, while accommodating context for the various business domains.” MITRE

### CWSS: Common Weakness Scoring System

“The Common Weakness Scoring System (CWSS) provides a mechanism for scoring weaknesses in a consistent, flexible, open manner while accommodating context for the various business domains. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry.” MITRE

<http://cwe.mitre.org/cwss/>

### Cybersecurity Framework

NIST, Compendium

<http://www.nist.gov/cyberframework/index.cfm>

<http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf>

See also:

CIP-CSP Mind Map

<http://www.tripwire.com/state-of-security/wp-content/uploads/2013/11/CIP-CSF-Framework.pdf>

### CybOX (Cyber Observable eXpression)

“International in scope and free for public use, CybOX is a standardized schema for the specification, capture, characterization, and communication of events or stateful properties that are observable in the operational domain. A wide variety of high-level cyber security use cases rely on such information including: event management/logging, malware characterization, intrusion detection, incident response/management, attack pattern characterization, etc. CybOX provides a common mechanism (structure and content) for addressing cyber observables across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.” MITRE

<http://cybox.mitre.org/>

### Dependency Modeling (O-DM)

The Open Group

“This O-DM standard defines how to construct a data model to manage risk and build trust on organizational dependencies between enterprises, or between operational divisions in a large organization. It involves constructing a data model for key dependencies, then assigning quantitative risk sensitivities for each dependency component in the model.”

<https://www2.opengroup.org/ogsys/catalog/C133>

### Distributed Audit Service (XDAS)

### DoD Information Assurance Risk Management Framework (DIARMF)

“DIARMF represents DoD adoption of the NIST Risk Management Framework process.”

### DPE (Default Password Enumeration)

<http://resources.infosecinstitute.com/dpe-the-structured-enumeration-of-default-credentials-and-passwords/>

<https://github.com/toolswatch/DPE>

### Factor Analysis of Information Risk (FAIR)

### FrameworkX (TM Forum)

### GRC Stack (Governance, Risk Management and Compliance)

Cloud Security Alliance

<https://cloudsecurityalliance.org/research/grc-stack/>

“Achieving Governance, Risk Management and Compliance (GRC) goals requires appropriate assessment criteria, relevant control objectives and timely access to necessary supporting data. Whether implementing private, public or hybrid clouds, the shift to compute as a service presents new challenges across the spectrum of GRC requirements. The Cloud Security Alliance GRC Stack provides a toolkit for enterprises, cloud providers, security solution providers, IT auditors and other key stakeholders to instrument and assess both private and public clouds against industry established best practices, standards and critical compliance requirements.” CSA

### ICS Security Standard (Qatar)

National Industrial Control Systems Security Standard

<http://www.ictqatar.qa/sites/default/files/documents/National%20Industrial%20Control%20Systems%20Security%20Standard-English.pdf>

### Intrusion Detection Message Exchange Format (IDMEF)

### IFX Forum Framework

### Information Risk Analysis Methodology (IRAM)

“The Information Risk Analysis Methodology (IRAM) is a business tool essential that helps organisations identify, analyse and manage information risk throughout the enterprise. It is based on over ten years of research and derived from good practice in leading organisations.”

ISF (Information Security Forum)

<https://www.securityforum.org/tools/isf-risk-manager/>

### Intermediary Vulnerability Information Language (IVIL)

<http://www.cupfighter.net/index.php/2010/10/ivil-an-xml-schema-to-exchange-vulnerability-information/>

### Internet Users' Glossary (RFC1392)

IETF

<http://tools.ietf.org/search/rfc1392>

### IODEF (Incident Object Description Exchange Format)

“The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents.”

IETF (MILE Working Group), RFC5070

<http://tools.ietf.org/html/draft-ietf-mile-rfc5070-bis-02>

### iPost Scoring Methodology

### ISA 99.02.01

ANSI/ISA

Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

“Formerly designated ANSI/ISA-99.02.01-2009, this standard is part of a multipart series that addresses the issue of security for industrial automation and control systems. It has been developed by Working Group 2 of the ISA99 committee.  
  
This standard describes the elements contained in a cyber security management system for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element.  
  
This standard has been developed in large part from a previous Technical Report produced by the ISA99 committee, ANSI/ISA–TR99.00.02–2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment. The majority of the contents of this Technical Report have been included in this standard and as such this standard supersedes the Technical Report.  
  
The ISA99 series addresses electronic security within the industrial automation and control systems environment. The series will serve as the foundation for the IEC 62443 series of the same titles, as being developed by IEC TC65 WG10, “Security for industrial process measurement and control - Network and system security.”” ISA

<http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FISA+99.02.01-2009>

<http://www.isa.org/Template.cfm?Section=Standards8&template=/Ecommerce/ProductDisplay.cfm&ProductID=10242>

### ISO 3166 (Country Codes)

<http://www.iso.org/iso/home/standards/country_codes.htm>

“ISO 3166 is the International Standard for country codes and codes for their subdivisions. The purpose of ISO 3166 is to establish internationally recognised codes for the representation of names of countries, territories or areas of geographical interest, and their subdivisions. However, ISO 3166 does not establish the names of countries, only the codes that represent them.” ISO

### ISO 27000/ISO 27001 Information Security Risk Management System  ISO/IEC 19770  ISO 31000 Enterprise Management

### ISO/IEC 27001

<http://www.27000.org/iso-27001.htm>

“The ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. It is the specification for an ISMS, an Information Security Management System. BS7799 itself was a long standing standard, first published in the nineties as a code of practice. As this matured, a second part emerged to cover management systems. It is this against which certification is granted. Today in excess of a thousand certificates are in place, across the world.

On publication, ISO 27001 enhanced the content of BS7799-2 and harmonized it with other standards. A scheme was been introduced by various certification bodies for conversion from BS7799 certification to ISO27001 certification.

The objective of the standard itself is to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)". Regarding its adoption, this should be a strategic decision. Further, "The design and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization".”, ISO

<https://en.wikipedia.org/wiki/ISO/IEC_27001:2005>

### Key Management Interoperability Protocol (KMIP) TC

OASIS

### MAEC (Malware Attribute Enumeration and Characterization)

“International in scope and free for public use, MAEC is a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns.

By eliminating the ambiguity and inaccuracy that currently exists in malware descriptions and by reducing reliance on signatures, MAEC aims to improve human-to-human, human-to-tool, tool-to-tool, and tool-to-human communication about malware; reduce potential duplication of malware analysis efforts by researchers; and allow for the faster development of countermeasures by enabling the ability to leverage responses to previously observed malware instances.” MITRE

<http://maec.mitre.org/>

### 

### Malware Metadata Exchange Format (MMDEF)

“The *IEEE* Malware Metadata Exchange Format (MMDEF) Working Group is working on expanding the breadth of information able to be captured and shared about malware in a standardized fashion.” IEEE

<http://standards.ieee.org/develop/indconn/icsg/mmdef.html>

### NERC CIP (North American Electric Reliability Corporation, Critical Infrastructure Protection)

### Network Defense Data Models (NDDM)

### NIST Risk Management Framework (RMF)

“The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the **management of organizational risk**---that is, the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system---the security controls necessary to protect individuals and the operations and assets of the organization.“ NIST

<http://csrc.nist.gov/groups/SMA/fisma/framework.html>

<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

### NIST SP 500-291

NIST

<http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf>

NIST Cloud Computing Standards Roadmap

### NIST SP 800-34

NIST

<http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>

Contingency Planning Guide for Federal Information Systems

### NIST SP 800-37

### NIST SP 800-53 Rev. 4

NIST

<http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>

Security and Privacy Controls for Federal Information Systems and Organizations

(Security Control Families)

See also:

<https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53>

### NRF: U.S. National Response Framework

FEMA (Federal Emergency Management Agency)

<http://www.fema.gov/national-response-framework>

“The Response Framework covers the capabilities necessary to save lives, protect property and the environment and meet basic human needs after an incident has occurred. Response activities take place immediately before, during and in the first few days after a major or catastrophic disaster. Then, recovery efforts begin to help the community get back on its feet.” FEMA

### OAuth (Open standard for Authorization), OAuth Framework

<https://en.wikipedia.org/wiki/OAuth>

<http://oauth.net/>

“An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications.” oauth.net

### OASIS Customer Information Quality Committee (CIQ)

<https://www.oasis-open.org/committees/ciq/ciq.html>

### OASIS xCIL : extensible Customer Information Language

### OASIS xCRL : extensible Customer Relationships Language

### OASIS xNAL : extensible Name and Address Language

### OASIS xNL

### OCIL (Open Checklist Interactive Language)

<http://scap.nist.gov/specifications/ocil/>

“The Open Checklist Interactive Language (OCIL) defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. Although the OCIL specification was developed for use with IT security checklists, the uses of OCIL are by no means confined to IT security. Other possible use cases include research surveys, academic course exams, and instructional walkthroughs.” NIST

### OCTAVE

“OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning.”

<https://www.cert.org/octave/>

### Open Automated Compliance Expert Markup Language (O-ACEML)

<https://www2.opengroup.org/ogsys/catalog/C111>

### Open Checklist Interactive Language (OCIL)

<http://scap.nist.gov/specifications/ocil/>

### OpenID

<https://en.wikipedia.org/wiki/OpenID>

### Open Information Security Management Maturity Model (O-ISM3)

<https://www2.opengroup.org/ogsys/catalog/C102>

### OpenIOC

MANDIANT

<http://www.openioc.org/>

“OpenIOC is an extensible XML schema that enables you to describe the technical characteristics that identify a known threat, an attacker’s methodology, or other evidence of compromise.” MANDIANT

### OpenSAMM (Software Assurance Maturity Model)

OWASP

<http://www.opensamm.org/>

### Open Source Security Testing Methodology Manual (OSSTMM)

ISECOM

<http://www.isecom.org/research/osstmm.html>

“The OSSTMM is about operational security. It is about knowing and measuring how well security works. This methodology will tell you if what you have does what you want it to do and not just what you were told it does.” ISECOM

### Open Threat Exchange (OTX)

### OVAL (Open Vulnerability and Assessment Language)

MITRE

“International in scope and free for public use, OVAL is an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.” MITRE

<https://oval.mitre.org/>

### OWASP

OWASP

<https://www.owasp.org/index.php/OWASP_Testing_Project>

<https://www.owasp.org/index.php/Category:Principle>

<https://www.owasp.org/index.php/Application_Security_Architecture_Cheat_Sheet>

<https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet>

<https://www.owasp.org/index.php/Secure_Coding_Cheat_Sheet>

<https://www.owasp.org/index.php/Cheat_Sheets>

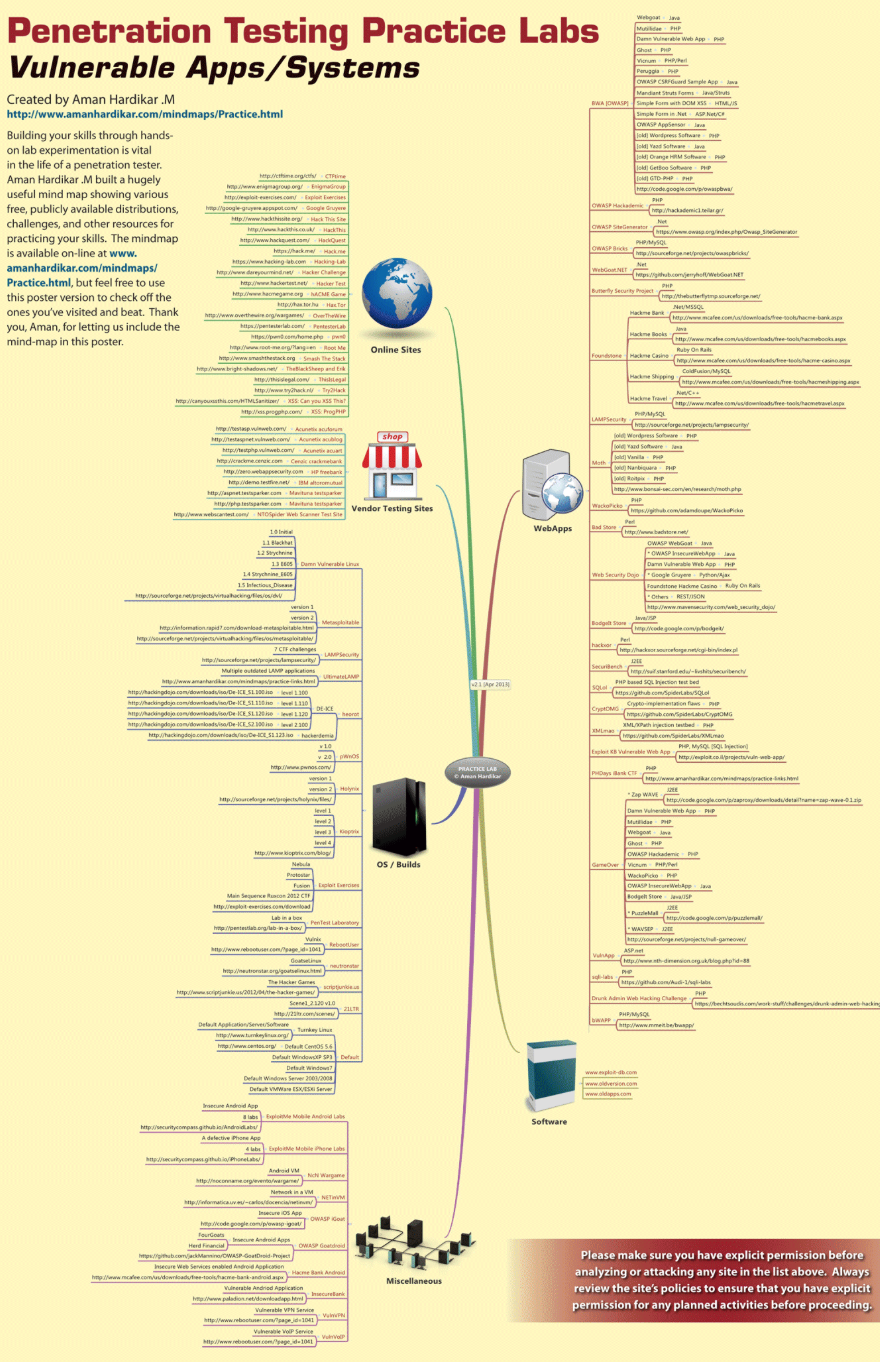
### OWASP ASVS (Application Security Verification Standard Project)

OWASP

<https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project>

### OWASP Testing Guide

<https://www.owasp.org/index.php/OWASP_Testing_Project>



*Source:* [*http://pen-testing.sans.org/blog/pen-testing/2013/06/20/announcing-the-ultimate-sans-pen-test-poster*](http://pen-testing.sans.org/blog/pen-testing/2013/06/20/announcing-the-ultimate-sans-pen-test-poster)

### Penetration Testing Execution Standard (PTES)

<http://www.pentest-standard.org/index.php/Main_Page>

Following are the main sections defined by the standard as the basis for penetration testing execution:

* [Pre-engagement Interactions](http://www.pentest-standard.org/index.php/Pre-engagement)
* [Intelligence Gathering](http://www.pentest-standard.org/index.php/Intelligence_Gathering)
* [Threat Modeling](http://www.pentest-standard.org/index.php/Threat_Modeling)
* [Vulnerability Analysis](http://www.pentest-standard.org/index.php/Vulnerability_Analysis)
* [Exploitation](http://www.pentest-standard.org/index.php/Exploitation)
* [Post Exploitation](http://www.pentest-standard.org/index.php/Post_Exploitation)
* [Reporting](http://www.pentest-standard.org/index.php/Reporting)

### Predictive Model Markup Language (PMML)

“The Predictive Model Markup Language (PMML) is an XML-based file format developed by the Data Mining Group to provide a way for applications to describe and exchange models produced by data mining and machine learning algorithms.” Wikipedia

<https://en.wikipedia.org/wiki/Predictive_Model_Markup_Language>

<http://www.dmg.org/>

### RID: Real-time Inter-network Defense protocol

IETF

“Real-time Inter-network Defense (RID) outlines a proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident-handling solution.”

<http://tools.ietf.org/html/rfc6545>

RFC 6545 (Moriarty, 2012), RFC 6546 (Trammell, 2012)

### Risk Taxonomy (O-RT)

“This document provides a standard definition and taxonomy for information security risk, as well as information regarding how to use the taxonomy.” The Open Group

Reference C13K   
US ISBN 1-937218-42-3

<https://www2.opengroup.org/ogsys/catalog/C13K>

### SCAP (Security Content Automation Protocol)

“The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality.” NIST

<http://scap.nist.gov/>

### Security Description and Exchange Format (SecDEF)

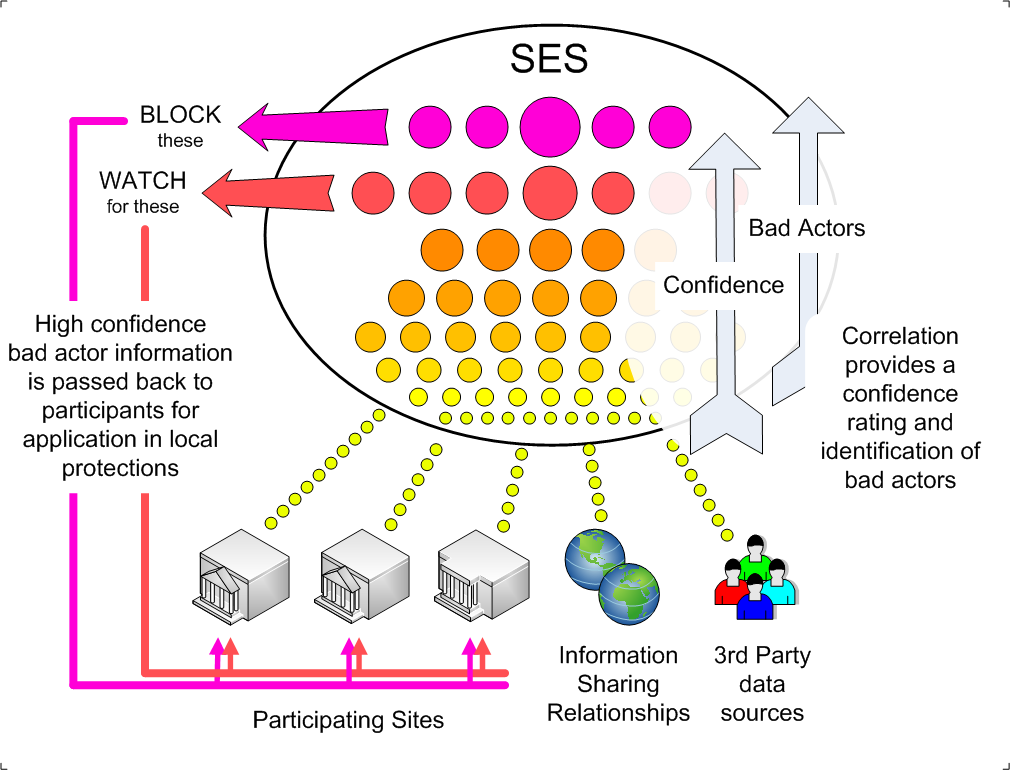
<http://www.enisa.europa.eu/activities/cert/background/inv/cert-activities/standardisation/standard-ii/>

### SES - Security Event System

REN-ISAC (Research and Education Networking Information Sharing and Analysis Center)

“Objective: Improve timely local protection against cyber security threat, by sharing security event information, in near-real time, within a trusted federation, and among federations.”

<http://www.ren-isac.net/ses/>



*Source: REN-ISAC* [*http://www.ren-isac.net/ses/*](http://www.ren-isac.net/ses/)

### Situational Awareness Reference Architecture (SARA)

ICS ISAC

<http://ics-isac.org/sara/>

### Software Assurance (SwA) Competency Model

<http://www.sei.cmu.edu/library/abstracts/reports/13tn004.cfm>

“This Software Assurance (SwA) Competency Model was developed to create a foundation for assessing and advancing the capability of software assurance professionals. To help organizations and individuals determine SwA competency across a range of knowledge areas and units, this model provides a span of competency levels 1 through 5, as well as a decomposition into individual competencies based on knowledge and skills. This model also provides a framework for an organization to adapt the model's features to the organization's particular domain, culture, or structure.” CMU

### Software Defined Perimeter (SDP)

Cloud Security Alliance (CSA)

<https://downloads.cloudsecurityalliance.org/initiatives/sdp/Software_Defined_Perimeter.pdf>

“This document explains the software defined perimeter (SDP) security framework and how it can be deployed to protect application infrastructure from network-based attacks. The SDP incorporates security standards from organizations such as the National Institute of Standards and Technology (NIST) as well as security concepts from organizations such as the U.S. Department of Defense (DoD) into an integrated framework. The Cloud Security Alliance (CSA) intends to create a public standard that is freely available for use without license fees or restrictions.” CSA

### STAR (Security, Trust & Assurance Registry)

Cloud Security Alliance (CSA)

<https://cloudsecurityalliance.org/star/>

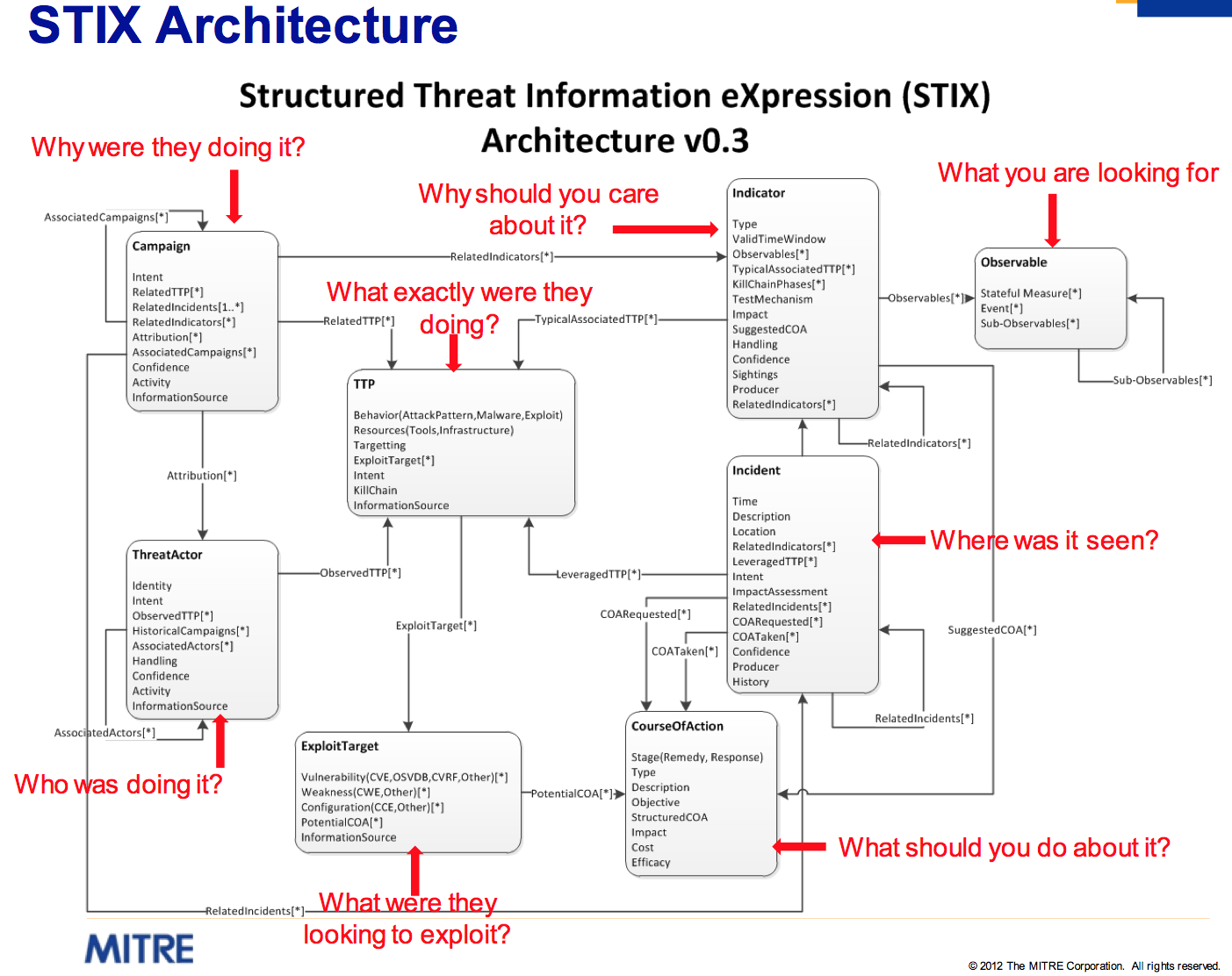
### STIGs: Defense Information Systems Agency Security Technical Implementation Guides

<http://iase.disa.mil/stigs/index.html>

### STIX (Structured Threat Information eXpression)

<http://stix.mitre.org/>

“STIX is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible.” MITRE



*Source:* [*http://www.cyber.st.dhs.gov/wp-content/uploads/2012/10/Day-1.02-NPPD-NPPD-Jarzombek.pdf*](http://www.cyber.st.dhs.gov/wp-content/uploads/2012/10/Day-1.02-NPPD-NPPD-Jarzombek.pdf)

### STRIDE Threat Model

Microsoft

<https://en.wikipedia.org/wiki/STRIDE_(security>)

<http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx>

“STRIDE is derived from an acronym for the following six threat categories:

**Spoofing identity**. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.

**Tampering with data**. Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.

**Repudiation**. Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Nonrepudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.

**Information disclosure**. Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

**Denial of service**. Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.

**Elevation of privilege**. In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.” Microsoft

### SQUARE (Security Quality Requirements Engineering)

CERT.org

<http://www.cert.org/sse/square/>

Requirements Engineering for Improved System Security and Privacy.

“Requirements problems are the primary reason that projects are significantly over budget and past schedule have significantly reduced scope deliver poor-quality applications that are little used once delivered, or are cancelled altogether.

One source of these problems is poorly expressed or analyzed quality requirements, such as security and privacy. Requirements engineering defects cost 10 to 200 times more to correct during implementation than if they are detected during requirements development. Moreover, it is difficult and expensive to significantly improve the security of an application after it is in its operational environment.

Security Quality Requirements Engineering (SQUARE) is a [nine-step process](http://www.cert.org/sse/square/square-ninesteps.html) that helps organizations build security into the early stages of the production life cycle. We have extended the process to consider privacy.

Using SQUARE can enable your organization to develop more secure, survivable software and systems, more predictable schedules and costs, and achieve lower costs.

An enhanced robust tool to help you easily use the SQUARE process for security, privacy, or both is now available as a [free downloadable application](http://www.cert.org/sse/square/square-tool.html).

Organizations that are acquiring software have the same security concerns as those that are developing software, but they usually have less control over the actual development process.” CERT.org

### SWID Tags

<https://en.wikipedia.org/wiki/ISO/IEC_19770>

### TAXII (Trusted Automated eXchange of Indicator Information)

“TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols, and message exchanges to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats.” MITRE

<http://taxii.mitre.org/>

### TOGAF

The Open Group

“TOGAF®, an Open Group Standard, is a proven enterprise architecture methodology and framework used by the world's leading organizations to improve business efficiency.”

<http://www.opengroup.org/togaf/>

### Traffic Light Protocol (TLP) Matrix

<https://www.us-cert.gov/tlp/>

|  |  |  |
| --- | --- | --- |
| **Color** | **When should it be used?** | **How may it be shared?** |
| **RED** | Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. | Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed. |
| **AMBER** | Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved. | Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information. |
| **GREEN** | Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. | Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. |
| **WHITE** | Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. | TLP: WHITE information may be distributed without restriction, subject to copyright controls. |

### Trust Model for Security Automation Data (TMSAD)

<http://scap.nist.gov/specifications/tmsad/>

“TMSAD describes a common trust model that can be applied to specifications within the security automation domain, such as Security Content Automation Protocol (SCAP). Since information in the security automation domain is primarily exchanged using Extensible Markup Language (XML), the focus of this model is on the processing of XML documents. The trust model is composed of recommendations on how to use existing specifications to represent signatures, hashes, key information, and identity information in the context of an XML document within the security automation domain.” NIST

### VERIS: Vocabulary for Event Recording and Incident Sharing

Verizon

<http://www.veriscommunity.net>

### Web Application Security Evaluation Criteria

“The Web Application Security Evaluation Criteria is a set of guidelines to evaluate web application security scanners on their identification of web application vulnerabilities and its completeness.” WASC

<http://www.webappsec.org/projects/wassec/>

### Web Application Firewall (WAF) Evaluation Criteria

“The goal of this project is to develop a detailed web application firewall (WAF) evaluation criteria; a testing methodology that can be used by any reasonably skilled technician to independently assess the quality of a WAF solution.” WASC

<http://www.webappsec.org/projects/wafec/>

### XCCDF: Extensible Configuration Checklist Description Format

“XCCDF is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices.” NIST

<http://scap.nist.gov/specifications/xccdf/>

### XEP-0268: Incident Handling

<http://xmpp.org/extensions/xep-0268.html>

### XML Encryption

“XML Encryption specifies a process for encrypting data and representing the result in XML.” W3C

<http://www.w3.org/TR/xmlenc-core/>

## XORCISM Tools

To illustrates and demonstrates the possibilities and usability offered by XORCISM, some tools have been made available (including source code under [GNU GPL License](#_License_2)).

These are available at:

<https://github.com/athiasjerome/XORCISM>

### XORCISM Database conversion script

An SQL script and example is available to convert the XORCISM Database Schema for use with different Database Management Systems (DBMS).

<https://github.com/athiasjerome/XORCISM/tree/master/XORCISMModel>

### XORCISM DLL

Library that can be use to interact with a XORCISM database.

Note: this library can be used as an API to interact with all the XORCISM objects.

<https://github.com/athiasjerome/XORCISM/tree/master/XORCISMModel_DLL>

NB: The classes used in the DLL can be obtained, for example, by using a XORCISM database (created using the available schema <https://github.com/athiasjerome/XORCISM/tree/master/XORCISMModel>) in Microsoft SQL Server (even the free Express version), and then manipulated under Microsoft Visual Studio.

**The obtained classes can furthermore be manipulated or modified in various programming languages.**

PS: The above manipulation can also be used to obtain the XORCISM Data Model under Microsoft Visual Studio Model Editor/Entities Browser, and can be exported to Microsoft Visual Studio, or other tools such as DbVisualizer (i.e. to generate a poster).

### XORCISM Import\_capec

<https://github.com/athiasjerome/XORCISM/tree/master/XORCISMCAPEC>

A tool to import a CAPEC repository in a XORCISM database.

### XORCISM Import\_cpe

<https://github.com/athiasjerome/XORCISM/tree/master/XORCISMCPE>

A tool to import a CPE repository in a XORCISM database.

### XORCISM Import\_cve

<https://github.com/athiasjerome/XORCISM/tree/master/XORCISMCVE>

A tool to import a CVE repository in a XORCISM database.

### XORCISM Import\_cwe

<https://github.com/athiasjerome/XORCISM/tree/master/XORCISMCWE>

A tool to import a CWE repository in a XORCISM database.

More to come (i.e. Import/Export) in a near future.

## Other Security Tools

XORCISM allows the users to store information about security [Tools](#_Tool).

XORCISM makes a distinction between **Attack Tools** and **Defense Tools** (where some could be in both [Categories](#_Category_2)).

**The following list of tools is provided “as is”, the author does not provide any warranty of the item whatsoever, whether express, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item will be error-free.**

**In no respect shall the author(s) incur any liability for any damages, including, but limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or any way connected to the use of the item, whether or not based upon warranty, contract, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by the author.**

### Tools Repositories

Here are some **Tools Repositories**:

<https://github.com/CybOXProject/Tools>

<https://github.com/MAECProject/utils>

<https://github.com/STIXProject/Tools>

<https://cloudsecurityalliance.org/>

<http://benchmarks.cisecurity.org/downloads/audit-tools/>

<http://web.nvd.nist.gov/view/ncp/repository>

<http://www.toolswatch.org/>

<https://github.com/vz-risk/veris>

### AbuseHelper

<http://abusehelper.be>

“AbuseHelper is an open-source project initiated by [CERT.FI](http://www.cert.fi/) (Finland) and [CERT.EE](http://www.cert.ee/) (Estonia) with [ClarifiedNetworks](http://www.clarifiednetworks.com/) to automatically process incidents notifications.

This tool is being developed for [CERTs](http://en.wikipedia.org/wiki/Computer_emergency_response_team) and [ISP's](http://en.wikipedia.org/wiki/Internet_Service_Provider) to help them in their daily job of following and treating a wide range of high-volume information sources. It is interesting to note that the framework can also be used for automatically processing (standardised) information from a wide range of sources.”

### Apache Lucene

<https://lucene.apache.org/>

“Apache LuceneTM is a high-performance, full-featured text search engine library written entirely in Java. It is a technology suitable for nearly any application that requires full-text search, especially cross-platform.”

### Appcmd.exe

Microsoft

Command-line tool for IIS settings management.

### AppLocker

Microsoft

### Aqueduct

<https://fedorahosted.org/aqueduct/>

“The Aqueduct project provides automated changes to Red Hat Enterprise Linux based systems to meet security guidelines established by various agencies. These changes are in the form of Bash scripts and Puppet manifests. Each change is specific to the agency's auditing criteria and granular enough to allow the system owner to decide on changes at the line item level.”

### BitLocker

BitLocker Drive Encryption is a full disk encryption feature included with some versions of Microsoft Windows.

<https://en.wikipedia.org/wiki/BitLocker_Drive_Encryption>

### BitMail

<http://sourceforge.net/projects/bitmail/>

### Bitmessage

<https://bitmessage.org/>

“Bitmessage is a P2P communications [protocol](https://bitmessage.org/wiki/Protocol_specification) used to send encrypted messages to another person or to many subscribers. It is decentralized and trustless, meaning that you need-not inherently trust any entities like root certificate authorities. It uses strong authentication which means that the sender of a message cannot be spoofed, and it aims to hide "non-content" data, like the sender and receiver of messages, from passive eavesdroppers like those running warrantless wiretapping programs.”

[MIT License](#_License_1)

### Bro-IDS

### capirca

Multi-platform ACL generation system

“Developed internally at Google, this system is designed to utilize common definitions of networks and services and high-level policy files to facilitate the development and manipulation of network access control filters (ACLs) for various platforms.”

<https://code.google.com/p/capirca/>

### CIS-CAT

<http://benchmarks.cisecurity.org/downloads/audit-tools/>

### Cuckoo Sandbox

“In three words, Cuckoo Sandbox is a malware analysis system.”

<http://www.cuckoosandbox.org/>

Note that significant efforts are made to have it *compatible* with MAEC.

### EMET (Enhanced Mitigation Experience Toolkit)

“The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET achieves this goal by using security mitigation technologies. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited. However, they work to make exploitation as difficult as possible to perform.” Microsoft

<http://www.microsoft.com/emet>

### ESAPI (OWASP Enterprise Security API)

“ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications.” OWASP

<https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API>

### File Vault

“FileVault is a method of using encryption with volumes on Mac computers.”

<https://en.wikipedia.org/wiki/FileVault>

### Forensic Toolkit (FTK)

“FTK is a court-accepted digital investigations platform built for speed, stability and ease of use.” AccessData

<http://www.accessdata.com/products/digital-forensics/ftk>

### GnuPG (GPG) / PGP

<https://en.wikipedia.org/wiki/GNU_Privacy_Guard>

<https://en.wikipedia.org/wiki/Pretty_Good_Privacy>

### hadoop-pcap

Hadoop library to read packet capture (PCAP) files

<https://github.com/RIPE-NCC/hadoop-pcap>

### IOCExtractor

“IOC (Indicator of Compromise) Extractor: a program to help extract IOCs from text files.”

<https://github.com/stephenbrannon/IOCextractor>

### Malware Hash Registry

<http://www.team-cymru.org/Services/MHR/>

### MANTIS

Cyber Threat Intelligence Management Framework

<http://django-mantis.readthedocs.org/en/latest/>

### Microsoft System Center Configuration Manager (SCCM)

### MISP

Malware Information Sharing Platform

<https://github.com/MISP/MISP>

### Minion

“Minion is an open source Security Automation platform. The 0.3 release of Minion allows Development, QA, and Security team members to perform automated web security scans with a set of tools, and re-execute those scans as needed.”

<https://wiki.mozilla.org/Security/Projects/Minion>

### Moloch

“Moloch is a open source large scale IPv4 full PCAP capturing, indexing and database system.”

<https://github.com/aol/moloch>

### Moon Secure Antivirus

“Moon Secure Antivirus aims to be the best Free Antivirus for Windows under GPL license. It offers multiple scan engines, Net shield, Firewall, On access, on Exec scanner and rootkits preventions plus features from Commercial Antivirus applications.”

License: [GNU General Public License version 2.0 (GPLv2)](http://sourceforge.net/directory/license:gpl/)

<http://sourceforge.net/projects/moonav/>

### Nfsight

“Nfsight is a Netflow processing and visualization application designed to offer a comprehensive network awareness solution. It is developed as a Nfsen plugin to provide client/server identification and intrusion detection capabilities.”

<http://sourceforge.net/projects/nfsight/>

### Nmap

“Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.”

GNU General Public License

<http://nmap.org/>

### OCIL Interpreter

“The OCIL Interpreter is a standalone Java GUI implementation that demonstrates how an OCIL document can be evaluated. It guides the end user in completing questionnaires (one question at a time), viewing and computing results.”

<http://sourceforge.net/projects/interactive/?abmode=1>

### OpenDNS (DNSCrypt)

<http://www.opendns.com/technology/dnscrypt/>

### OpenSCAP

<http://www.open-scap.org/page/Main_Page>

### OpenVAS (Open Vulnerability Assessment System)

“OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.”

<http://www.openvas.org/>

### OpenVPN

<http://openvpn.net>

### OSSIM

Open Source SIEM

<http://www.alienvault.com/open-threat-exchange/projects#ossim>

### OTR (Off-the-Record Messaging)

<https://otr.cypherpunks.ca/>

### OVAL Interpreter (ovaldi)

“The OVAL Interpreter is a freely available reference implementation that demonstrates the evaluation of OVAL Definitions. Based on a set of OVAL Definitions the interpreter collects system information, evaluates it, and generates a detailed OVAL Results file. “

<http://sourceforge.net/projects/ovaldi/>

### OWASP Projects and Guides

<https://www.owasp.org/index.php/Category:OWASP_Project>

<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>

<https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project>

<https://www.owasp.org/index.php/Automated_Audit_using_SKIPFISH>

<https://www.owasp.org/index.php/Automated_Audit_using_WAPITI>

<https://www.owasp.org/index.php/Automated_Audit_using_W3AF>

<https://www.owasp.org/index.php/Automated_Audit_using_SQLMap>

### pfSense

“pfSense is a free, open source customized distribution of FreeBSD tailored for use as a firewall and router.”

<http://www.pfsense.org/>

### Request Tracker (RT)

“RT is a battle-tested issue tracking system which thousands of organizations use for bug tracking, help desk ticketing, customer service, workflow processes, change management, network operations, youth counseling and even more.”

<http://www.bestpractical.com/rt/>

### RIPS

“RIPS is a static source code analyser for vulnerabilities in PHP webapplications.”

<http://sourceforge.net/projects/rips-scanner/>

### RTIR (RT for Incident Response)

“RTIR is the premier open source incident handling system targeted for computer security teams. We worked with over a dozen CERT and CSIRT teams around the world to help you handle the ever-increasing volume of incident reports.”

<http://www.bestpractical.com/rtir/>

### scap-security-guide

<https://fedorahosted.org/scap-security-guide/>

<https://git.fedorahosted.org/cgit/scap-security-guide.git/>

### Secpod Saner

<http://www.secpod.com/index.html#prod>

### Secunia PSI

<https://secunia.com/vulnerability_scanning/personal/>

### Shodan

<http://www.shodanhq.com>

### Silent Phone / Silent Text

<https://silentcircle.com/web/technology/>

### Snort

“Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide.”

<http://www.snort.org>

### Splunk

<http://www.splunk.com>

### Spybot 2 Search & Destroy

<http://www.safer-networking.org/mirrors/>

### sshuttle

“Transparent proxy server that works as a poor man's VPN. Forwards over ssh. Doesn't require admin. Works with Linux and MacOS. Supports DNS tunneling.”

<https://github.com/apenwarr/sshuttle>

### Suricata

“Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.”

<http://suricata-ids.org>

### ThreadFix

“ThreadFix is a software vulnerability aggregation and management system that helps organizations aggregate vulnerability data, generate virtual patches, and interact with software defect tracking systems.”

ThreadFix is licensed under the Mozilla Public License (MPL) version 2.0.

<https://github.com/denimgroup/threadfix>

### ThreatModeler

<http://myappsecurity.com/threatmodeler/>

### Tor

<https://en.wikipedia.org/wiki/Tor_(anonymity_network>)

### TrueCrypt

“Free open-source disk encryption software”

<http://www.truecrypt.org/>

### VirusTotal

<https://www.virustotal.com>

### XCCDF Interpreter

“An open-source Java-based XCCDF reference implementation.”

<http://sourceforge.net/projects/xccdfexec/>

### YARA

*The pattern matching swiss knife for malware researchers*

“YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic.”

<http://plusvic.github.io/yara/>

### YETI

“YETI is a [TAXII](#_TAXII_(Trusted_Automated_1) implementation”

<https://github.com/TAXIIProject/yeti>

### Wireshark

<http://www.wireshark.org>

See also tcpdump

### WP-CLI

“A command line interface for WordPress”

<http://wp-cli.org/>

## Acronyms/Terms/Definitions/Abbreviations/Symbols

List provided “as is”, without intent to be exhaustive.

Note: The author recommends to store and extend this list in the [Acronym](#_Acronym) table of a XORCISM database.

### A&I database: Abstracting and Indexing database

### ABAC: Attribute Based Access Control

<http://csrc.nist.gov/projects/abac/index.html>

### ACL: Access Control List

### AI: [Asset Identification](#_Asset_Identification_(AI)) [5]

### AI: Artificial Intelligence

### AM: Asset Management

### ANSI: American National Standards Institute

<http://www.ansi.org/>

### ANSSI: Agence Nationale de la Sécurité des Systèmes d’Information (France)

<http://www.ssi.gouv.fr/>

### AppSec: Application Security

### APT: Advanced Persistent Threat

### ARF: [Asset Reporting Format](#_Asset_Reporting_Format_1) [6]

### ASN: Autonomous System Numbers

### ASVS: Application Security Verification Standard Project

<https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project>

### Bloom filter

“A Bloom filter is a space-efficient probabilistic data structure, conceived by Burton Howard Bloom in 1970, that is used to test whether an element is a member of a set.” Wikipedia

<https://en.wikipedia.org/wiki/Bloom_filter>

### BSIMM: Building Security In Maturity Model

<http://bsimm.com/>

### BYOD: Bring Your Own Device

<http://www.zdnet.com/10-steps-for-writing-a-secure-byod-policy-7000006170/>

### C2: Command and Control

### CADF: Cloud Auditing Data Federation Working Group

<http://www.dmtf.org/standards/cadf>

### CAESARS: Continuous Asset Evaluation, Situational Awareness, and Risk Scoring architectural reference

<http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf>

### CAI: Consensus Assessments Initiative

<https://cloudsecurityalliance.org/research/cai/>

### CAP: Common Alerting Protocol

<https://www.oasis-open.org/committees/download.php/14759/emergency-CAPv1.1.pdf>

### CC: Common Criteria

<http://www.commoncriteriaportal.org/>

### CERT: Cyber Emergency Response Team

### CIA: Confidentiality, Integrity, Availability or Authenticity

### CIS: Center for Internet Security

<http://www.cisecurity.org>

### CNIL: Commission Nationale de l’Informatique et des Libertés (France)

<http://www.cnil.fr/english/>

### COTS: Commercial-off-the-shelf

### CS&C: U.S. Office of Cybersecurity and Communications

<http://www.dhs.gov/office-cybersecurity-and-communications/>

### CSA: Cloud Security Alliance

<https://cloudsecurityalliance.org/>

### CCM: Cloud Controls Matrix

Security Controls Framework for Cloud Providers and Consumers

<https://cloudsecurityalliance.org/research/ccm/>

### CCS: Council on CyberSecurity

<http://www.counciloncybersecurity.org/>

### CCSA: Collaborative Cyber Situational Awareness

### CCV: Cybersecurity Compliance Validations

### CEE: Common Event Expression

### CERT: Computer Emergency Response Team

### CIA: Confidentiality, Integrity, Availability

### CIF: Collective Intelligence Framework

<https://code.google.com/p/collective-intelligence-framework/>

### CIQ: Customer Information Quality Committee

OASIS

### CIS: Center for Internet Security

### CLASP: Comprehensive, Lightweight Application Security Process

<https://www.owasp.org/index.php/Category:OWASP_CLASP_Project>

### CMRS: Continuous Monitoring and Risk Scoring

### CMU: Carnegie Mellon University

<https://www.cmu.edu/>

### CNCI: U.S. Comprehensive National Cybersecurity Initiative

### CNE: Computer Network Espionage

### COA: Course of Action

### COBIT: Control Objectives for Information and Related Technology

### COL: Course of Law

### CPE: Common Platform Enumeration

<https://nvd.nist.gov/cpe.cfm>

### CPNI: United Kingdom's Centre for the Protection of National Infrastructure

<http://www.cpni.gov.uk>

### CSIC: Computer Security Incident Coordination

<http://csrc.nist.gov/projects/csic/>

### CSIRT: Computer Security Incident Response Team

### CSRC: Computer Security Resource Center

<http://csrc.nist.gov/index.html>

### C-TIP: Cyber Threat Intelligence Program

### CTP: Cloud Trust Protocol

<https://cloudsecurityalliance.org/research/ctp/>

### CVE: Common Vulnerabilities and Exposures

<https://cve.mitre.org/>

### CVSS: Common Vulnerability Scoring System (CVSS-SIG)

<http://www.first.org/cvss>

### CWE: Common Weaknesses Enumeration

<http://cwe.mitre.org/>

### CWRAF: Common Weakness Risk Analysis Framework

<http://cwe.mitre.org/cwraf/>

### CWSS: Common Weakness Scoring System

<http://cwe.mitre.org/cwss/>

Cybersecurity Framework [7]

<http://www.nist.gov/cyberframework/>

### CybOX: Cyber Observable eXpression

<http://cybox.mitre.org/>

DGB: Data Governance Board

DHS: U.S. Department of Homeland Security

### DISA: U.S. Defense Information Systems Agency

### DLP: Data Loss Prevention

### DMG: Data Mining Group

<http://www.dmg.org/>

### DMZ: Demilitarized zone

### dnsSinkhole

### DNS Amplification

### DoD: U.S. Department of Defense

### DRM: Digital Rights Management

### DSS: Defense Security Service (U.S. Department of Defense)

### ECPA: Electronic Communications Privacy Act

### ENISA: European Union Agency for Network and Information Security

<http://www.enisa.europa.eu>

### ESAPI: OWASP Enterprise Security API

<https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API>

### FIDO: Fast Identity Online

*Simpler, Stronger Authentication*

<http://fidoalliance.org/fido-standards.html>

### FINE: Format for Incident Information Exchange

### FIPS: U.S. Federal Information Processing Standards

<http://csrc.nist.gov/publications/PubsFIPS.html>

### FISM: Federal Information Security Memorandum

### FISMA: Federal Information Security Management Act

<https://en.wikipedia.org/wiki/FISMA>

### GHDB: Google Hacking Database

### Google Dork

### GPO: Microsoft Group Policy

### GRC Stack: Governance, Risk Management and Compliance

<https://cloudsecurityalliance.org/research/grc-stack/>

### HMI: Human-Machine Interface

### HOST: Homeland Open Security Technology

<http://www.dhs.gov/csd-host/>

### hpfeeds: Honeynet Project generic authenticated datafeed protocol

<https://github.com/rep/hpfeeds>

### IATF: Information Assurance Technical Framework

<http://www.iatf.net/>

### ICS: Industrial Control System

### ICS-ISAC: Industrial Control System Information Sharing and Analysis Center

<http://ics-isac.org/>

### IDS: Intrusion Detection System

### IEEE: Institute of Electrical and Electronics Engineers

<http://www.ieee.org/>

### IETF: Internet Engineering Task Force

<http://www.ietf.org/>

### IOC: Indicator of Compromise

IODEF: Incident Object Description Exchange Format

### IP: Internet Protocol

### IPS: Intrusion Prevention System

### ISA: International Society of Automation

<http://www.isa.org/>

### ISACA: Information Systems Audit and Control Association

<http://www.isaca.org/>

ISF: Information Sharing Framework

ISO: Information Security Office

IISLoB: Information Systems Security Line of Business

<https://www.dhs.gov/information-systems-security-line-business>

IT: Information Technology

ITIL: Information Technology Infrastructure Library

<http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library>

ITL: Information Technology Laboratory at the National Institute of Standards and Technology (NIST)

### ITSM: IT Service Management

### ITU: International Telecommunication Union

### Jammer

### JSON: JavaScript Object Notation

<https://en.wikipedia.org/wiki/JSON>

### KISS: Keep it Simple, Stupid

### KNOX: Samsung KNOX

Samsung KNOX is a set of business focused enhancements to the Android mobile environment for selected Samsung mobile devices. One of the most important new enterprise features provided with KNOX is the ability for KNOX devices to be joined, secured and managed by a Microsoft Active Directory infrastructure.

### MAEC: Malware Attribute Enumeration and Characterization

<http://maec.mitre.org/>

### MACCSA: Multinational Alliance for Collaborative for Cyber Situational Awareness

### MAPP: Microsoft Active Protections Program

<http://blogs.technet.com/b/bluehat/archive/2013/07/29/new-mapp-initiatives.aspx>

### MARS: Microsoft Active Response for Security

### MCC: Motor Control Center

### Megatron

### MISP: Malware Information Sharing Platform

### MSRC: Microsoft Security Response Center

### MTPIS: Managed Trusted Internet Protocol Services

### NAICS: North American Industry Classification System

<http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012>

### NATO: North Atlantic Treaty Organization

### NCCIC: U.S. National Cybersecurity and Communications Integration Center

### NCCoE: U.S. National Cybersecurity Center of Excellence

<http://csrc.nist.gov/nccoe/index.html>

### NCP: U.S. National Checklist Program repository

<http://web.nvd.nist.gov/view/ncp/repository>

### NDA: Non-Disclosure Agreement

### NISPOM: National Industrial Security Program Operating Manual

<http://www.dss.mil/isp/fac_clear/download_nispom.html>

### NIST: U.S. National Institute of Standards and Technology

<http://www.nist.gov/>

### NRF: U.S. National Response Framework

FEMA (Federal Emergency Management Agency)

<http://www.fema.gov/national-response-framework>

### NTP: Network Time Protocol

### NVD: U.S. National Vulnerability Database

<https://nvd.nist.gov/download.cfm>

### OASIS: Organization for the Advancement of Structured Information Standards

<http://www.oasis-open.org>

### OAuth: Open standard for Authorization

<https://en.wikipedia.org/wiki/OAuth>

<http://oauth.net/>

“An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications.” oauth.net

### OCTAVE

<https://www.cert.org/octave/>

### OCIL: Open Checklist Interactive Language

<http://scap.nist.gov/specifications/ocil/>

“The Open Checklist Interactive Language (OCIL) defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. Although the OCIL specification was developed for use with IT security checklists, the uses of OCIL are by no means confined to IT security. Other possible use cases include research surveys, academic course exams, and instructional walkthroughs.” NIST

### OISF: Open Information Security Foundation

<http://www.openinfosecfoundation.org/>

### OpenID

<https://en.wikipedia.org/wiki/OpenID>

### OpenVAS: Open Vulnerability Assessment System

<http://www.openvas.org/>

### OpenSAMM: Software Assurance Maturity Model

<http://www.opensamm.org/>

### OSSTMM: Open Source Security Testing Methodology Manual

<http://www.isecom.org/research/osstmm.html>

### OSVDB: Open Sourced Vulnerability Database

<http://osvdb.org/>

### OVAL: Open Vulnerability and Assessment Language

<http://oval.mitre.org/index.html>

### OWASP: Open Web Application Security Project

### PCS: Process Control System

### PGP: Pretty Good Privacy

### PKE: Public Key Enablement

### PKI: Public Key Infrastructure

### PLC: Programmable Logic Controller

### Plover

### PMML: Predictive Model Markup Language

“The Predictive Model Markup Language (PMML) is an XML-based file format developed by the Data Mining Group to provide a way for applications to describe and exchange models produced by data mining and machine learning algorithms.” Wikipedia

<https://en.wikipedia.org/wiki/Predictive_Model_Markup_Language>

<http://www.dmg.org/>

### PPSM: Ports, Protocols, and Services Management

### Protocol Buffers

“Protocol Buffers are a method of serializing structured data. As such, they are useful in developing programs to communicate with each other over a wire or for storing data. The method involves an [interface description language](https://en.wikipedia.org/wiki/Interface_description_language) that describes the structure of some data and a program that generates from that description source code in various programming languages for generating or parsing a stream of bytes that represents the structured data.” Wikipedia

<https://en.wikipedia.org/wiki/Protocol_Buffers>

<https://code.google.com/p/protobuf/>

<https://developers.google.com/protocol-buffers/>

### PTES: Penetration Testing Execution Standard

<http://www.pentest-standard.org/index.php/Main_Page>

### RACE: Rapid Access Computing Environment

### RFC1392: Internet Users' Glossary

IETF

<http://tools.ietf.org/search/rfc1392>

### RID: Real-time Inter-network Defense protocol

<http://tools.ietf.org/html/rfc6545>

### ROLIE: Resource-Oriented Lightweight Indicator Exchange

### RVA: Risk and Vulnerability Assessment

### SAIR: Situational Awareness and Incident Response

### SCADA: Supervisory Control And Data Acquisition

### SCAP: Security Content Automation Protocol

<http://scap.nist.gov/>

### SCIMP: Silent Circle Instant Messaging Protocol

<https://silentcircle.com/web/technology/>

### SCM: Software Configuration Management

<https://en.wikipedia.org/wiki/Software_configuration_management>

### SDLC: Secure Development Life Cycle

<https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet>

### SDN: Software Defined Networking

<http://www.federaltechnologyinsider.com/software-defined-networking-heres-what-you-need-to-know/>

### Shredder

### SIEM: Security Information & Event Management solution

### SOC: Security Operation Center

### SQUARE: Security Quality Requirements Engineering

<http://www.cert.org/sse/square/>

### STAR: Security, Trust & Assurance Registry

<https://cloudsecurityalliance.org/star/>

### STIG: Defense Information Systems Agency Security Technical Implementation Guide

<http://iase.disa.mil/stigs/index.html>

### STIX: Structured Threat Information eXpression

<http://stix.mitre.org/>

### SwA: Software Assurance

<http://measurablesecurity.mitre.org/directory/areas/softwareassurance.html>

### TAXII: Trusted Automated eXchange of Indicator Information

“TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols, and message exchanges to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats.” MITRE

<http://taxii.mitre.org/>

### Threatsaurus: “The A-Z of computer and data security threats”

Sophos

<http://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf>

### TPM: Trusted Platform Module

### TTP: Tactics, Techniques and Procedures

### UAC: User Access Control

### URI: Uniform Resource Identifiers

### US-CERT: U.S. Computer Emergency Readiness Team

### USGCB: United States Government Configuration Baseline

<http://usgcb.nist.gov/usgcb_content.html>

### VCDB: VERIS Community Database

### VDM: Vulnerability Data Model

<http://tools.ietf.org/html/draft-booth-sacm-vuln-model-02>

### VERIS: Vocabulary for Event Recording and Incident Sharing

Verizon

<http://www.veriscommunity.net>

### VFD: Variable Frequency Drive

### VLAN: Virtual Local Area Network

### VoIP: Voice over IP

### VoSIP: Voice over Secure Internet Protocol

### VPN: Virtual Private Network

### W3C: World Wide Web Consortium

<http://www.w3.org>

### Waiver

### WAF: Web Application Firewall

### WAPT: Web Application Penetration Test

### WASC: Web Application Security Consortium

<http://www.webappsec.org>

### WHID: Web Hacking Incidents Database

<http://www.webappsec.org/projects/whid/>

### xCIL: extensible Customer Information Language

### xCRL: extensible Customer Relationships Language

### xNAL: extensible Name and Address Language

### XML: Extensible Markup Language

### XVDM: XORCISM Vulnerability Data Model

### Waiver

### Warrant

## Ontologies/Taxonomies/Controlled Vocabularies/Thesauri/Classifications

**List non-exhaustive provided “as is”**

**[TODO] Complete with the missing ones (i.e. found in the Specifications/Standards)**

**Enumerations not provided in this document but SHOULD be stored in XORCISM.**

### BIZEC APP/11

“The BIZEC APP/11 standard comprises the most critical and the most common security defects in SAP ABAP applications. Its purpose is to give companies that plan to conduct ABAP code audits guidance which types of security defects should be covered at minimum by an audit.”

<http://www.bizec.org/wiki/BIZEC_APP11>

### BIZEC TEC/11

“The BIZEC TEC/11 lists the most common and most critical security defects and threats affecting the Business Runtime layer of SAP platforms.”

<http://www.bizec.org/wiki/BIZEC_TEC11>

### CSIRT Case Classification

<http://www.first.org/_assets/resources/guides/csirt_case_classification.html>

### CybOX (Cyber Observable eXpression)

“CybOX provides a common mechanism (structure and content) for addressing cyber observables across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.” MITRE

<http://cybox.mitre.org/>

### HP Fortify Taxonomy: Software Security Errors

HP

<http://www.hpenterprisesecurity.com/vulncat/en/vulncat/index.html>

<http://www.hpenterprisesecurity.com/vulncat/en/docs/Fortify_TaxonomyofSoftwareSecurityErrors.pdf>

### Internet Users' Glossary (RFC1392)

IETF

<http://tools.ietf.org/search/rfc1392>

### IODEF (Incident Object Description Exchange Format)

IETF (MILE Working Group), RFC5070

<http://tools.ietf.org/html/draft-ietf-mile-rfc5070-bis-02>

### ISO 3166 (Country Codes)

<http://www.iso.org/iso/home/standards/country_codes.htm>

### North American Industry Classification System

2012 NAICS

<http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012>

### OWASP Attack Category

“This category is for tagging common types of application security attacks.” OWASP

<https://www.owasp.org/index.php/Category:Attack>

### Risk Taxonomy (O-RT)

“This document provides a standard definition and taxonomy for information security risk, as well as information regarding how to use the taxonomy.” The Open Group

Reference C13K   
US ISBN 1-937218-42-3

<https://www2.opengroup.org/ogsys/catalog/C13K>

### SANS- Twenty Critical Security Controls for Effective Cyber Defense

<https://www.sans.org/critical-security-controls/>

[**20 Critical Security Controls - Version 4.1**](https://www.sans.org/critical-security-controls/guidelines.php)

[Critical Control 1: Inventory of Authorized and Unauthorized Devices](https://www.sans.org/cag/control/1.php)

[Critical Control 2: Inventory of Authorized and Unauthorized Software](https://www.sans.org/cag/control/2.php)

[Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers](https://www.sans.org/cag/control/3.php)

[Critical Control 4: Continuous Vulnerability Assessment and Remediation](https://www.sans.org/cag/control/4.php)

[Critical Control 5: Malware Defenses](https://www.sans.org/cag/control/5.php)

[Critical Control 6: Application Software Security](https://www.sans.org/cag/control/6.php)

[Critical Control 7: Wireless Device Control](https://www.sans.org/cag/control/7.php)

[Critical Control 8: Data Recovery Capability](https://www.sans.org/cag/control/8.php)

[Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps](https://www.sans.org/cag/control/9.php)

[Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches](https://www.sans.org/cag/control/10.php)

[Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services](https://www.sans.org/cag/control/11.php)

[Critical Control 12: Controlled Use of Administrative Privileges](https://www.sans.org/cag/control/12.php)

[Critical Control 13: Boundary Defense](https://www.sans.org/cag/control/13.php)

[Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs](https://www.sans.org/cag/control/14.php)

[Critical Control 15: Controlled Access Based on the Need to Know](https://www.sans.org/cag/control/15.php)

[Critical Control 16: Account Monitoring and Control](https://www.sans.org/cag/control/16.php)

[Critical Control 17: Data Loss Prevention](https://www.sans.org/cag/control/17.php)

[Critical Control 18: Incident Response and Management](https://www.sans.org/cag/control/18.php)

[Critical Control 19: Secure Network Engineering](https://www.sans.org/cag/control/19.php)

[Critical Control 20: Penetration Tests and Red Team Exercises](https://www.sans.org/cag/control/20.php)

### STIX

<https://stix.mitre.org/language/version1.0.1/xsddocs/default_vocabularies/1.0.1/stix_default_vocabularies.html>

### Threatsaurus (“The A-Z of computer and data security threats”)

Sophos

<http://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf>

### VERIS: Vocabulary for Event Recording and Incident Sharing

Verizon

<http://www.veriscommunity.net>

“VERIS is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS is a response to one of the most critical and persistent challenges in the security industry - a lack of quality information. VERIS targets this problem by helping organizations to collect useful incident-related information and to share that information - anonymously and responsibly - with others. The overall goal is to lay a foundation from which we can constructively and cooperatively learn from our experiences to better measure and manage risk.” Verizon

### Web Security Glossary

WASC

“The Web Security Glossary is an alphabetical index of terms and terminology relating to web applications security. The purpose of the Glossary is to further clarify the language used within the community.” WASC

<http://www.webappsec.org/projects/glossary/>

### Web Security Threat Classification *(WSTC)*

WASC

“The Web Security Threat Classification is a cooperative effort to clarify and organize the threats to the security of a web site. The members of the Web Application Security Consortium have created this project to develop and promote industry standard terminology for describing these issues. Application developers, security professionals, software vendors, and compliance auditors will have the ability to access a consistent language for web security related issues.” WASC

<http://www.webappsec.org/projects/threat/>

## Repositories/Data Feeds

Of course, XORCISM could be use as a [Repository](#_Repository), or a Repository of Repositories.

**List non-exhaustive provided “as is”.**

**[TODO] Complete**

### CIS Benchmarks

<http://benchmarks.cisecurity.org/>

### Cybercrime tracker

<http://cybercrime-tracker.net>

### DShield

<http://www.dshield.org/>

### FIPS: U.S. Federal Information Processing Standards

<http://csrc.nist.gov/publications/PubsFIPS.html>

### GRC Repository

### Inventory of Standards Relevant to Cloud Computing (NIST)

<http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory>

### National Checklist Program (NCP) repository

### National Vulnerability Database (NVD) (NIST)

<https://nvd.nist.gov/download.cfm>

NVD Overview

<http://csrc.nist.gov/publications/nistbul/itlbul2013_12.pdf>

#### NVD CPE (Common Platform Enumeration) product dictionary

<https://nvd.nist.gov/cpe.cfm>

### Open Sourced Vulnerability Database (OSVDB)

<http://osvdb.org/>

### OVAL Repositories

<http://oval.mitre.org/repository/>

<http://oval.mitre.org/repository/about/other_repositories.html#Altx-Soft>

<http://oval.mitre.org/repository/about/other_repositories.html#Cisco>

<http://oval.mitre.org/repository/about/other_repositories.html#Debian>

<http://oval.mitre.org/repository/about/other_repositories.html#DISA-FSO>

<http://oval.mitre.org/repository/about/other_repositories.html#IT-Security-Database>

<http://oval.mitre.org/repository/about/other_repositories.html#NIST>

<http://oval.mitre.org/repository/about/other_repositories.html#Novell>

<http://oval.mitre.org/repository/about/other_repositories.html#Positive-Technologies>

<http://oval.mitre.org/repository/about/other_repositories.html#Red-Hat>

<http://oval.mitre.org/repository/about/other_repositories.html#Security-Database>

<http://oval.mitre.org/repository/about/other_repositories.html#SecPod>

### SCAP Repositories

<http://www.scaprepo.com>

(CVE, CPE, CCE, XCCDF, OVAL)

### SSL Labs

“SSL Labs is a collection of documents, tools and thoughts related to SSL.” Qualys

<https://www.ssllabs.com/>

### STIGs: Defense Information Systems Agency Security Technical Implementation Guides

<http://iase.disa.mil/stigs/index.html>

### Tools Repositories

<https://github.com/CybOXProject/Tools>

<https://github.com/MAECProject/utils>

<https://github.com/STIXProject/Tools>

<https://github.com/OVALProject>

<http://www.toolswatch.org/>

<https://www.ripe.net/data-tools>

<https://opensource.srlabs.de>

See also: [Other Security Tools](#_Other_Security_Tools)

### VirusTotal

<https://www.virustotal.com/>

### XCCDF Repositories

<https://benchmarks.cisecurity.org/downloads/benchmarks/>

## Communities/Working Groups/Mailing lists

(List provided “as is”, without any particular order)

**[TODO] To be updated**

### BSIMM

<http://bsimm.com/community/>

### Buqtraq

### Center for Internet Security

<https://www.cisecurity.org/>

### Cloud Security Alliance (CSA)

<https://cloudsecurityalliance.org/>

### Communities of Trust

**CERTs**

**ISAC**

Examples: S-ISAC, DSIE (DIB-ISAC), NCI

### Continuous Monitoring Working Group

### DShield

<http://www.dshield.org>

### FIDO (Fast Identity Online)

FIDO Alliance

<http://fidoalliance.org>

### IETF Working Groups

<http://www.ietf.org/>

#### SACM Working Group

#### <https://ietf.org/wg/sacm/charter/>

#### MILE Working Group

<https://datatracker.ietf.org/wg/mile/charter/>

### MITRE/NIST Communities

### Inventory of Standards Relevant to Cloud Computing

<http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory>

### ISACA

<https://www.isaca.org>

### Making Security Measurable

<http://making-security-measurable.1364806.n2.nabble.com/>

### OAuth: Open standard for Authorization

<http://oauth.net/>

### OWASP

<http://www.owasp.org>

#### OWASP Chapters

#### OWASP Breakers Community

<https://www.owasp.org/index.php/Breakers>

#### OWASP Builders Community

<https://www.owasp.org/index.php/Builders>

#### OWASP Defenders Community

<https://www.owasp.org/index.php/Defenders>

### RIPE

<https://www.ripe.net>

### Team Cymru

<http://www.team-cymru.org/>

### The Open Group

<http://www.opengroup.org/>

### VERIS Community

<http://www.veriscommunity.net>

### Web Application Security Consortium (WASC)

<http://www.webappsec.org>

### Web Security Mailing List

Web Application Security Consortium (WASC)

“The Web Security Mailing List is an open information forum for discussing topics relevant to web security. Topics include, but are not limited to, industry news and technical discussions surrounding web applications, proxies, honeypots, new attack types, methodologies, application firewalls, discoveries, experiences, web servers, application servers, database security, tools, solutions, and others.”

<http://lists.webappsec.org/mailman/listinfo/websecurity_lists.webappsec.org>

## Informative References

### Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (France)

<http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf>

### An Algebra for Specifying Valid Compound Terms in Faceted Taxonomies

<http://www.ics.forth.gr/_publications/algebraDKE07_final_pv.pdf>

### ANSI/API Standard 780 methodology

Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

American Petroleum Institute

<http://www.api.org/publications-standards-and-statistics/publications-updates/publication-updates/new-safety-fire-and-scientific-affairs-publications/api_std_780>

### Application Security Architecture

OWASP

<https://www.owasp.org/index.php/Application_Security_Architecture_Cheat_Sheet>

### Application Security Verification Standard Project (ASVS)

OWASP

<https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project>

### Asset Identification (AI)

NIST

<http://scap.nist.gov/specifications/ai/>

### Asset Reporting Format (ARF)

NIST

<http://scap.nist.gov/specifications/arf/>

### Avoiding Social Engineering and Phishing Attacks

US-CERT

<http://www.us-cert.gov/ncas/tips/ST04-014>

### Bitmessage: A Peer‐to‐Peer Message Authentication and Delivery System

<https://bitmessage.org/bitmessage.pdf>

### BIZEC APP11

<http://www.bizec.org/wiki/BIZEC_APP11>

### BIZEC TEC11

<http://www.bizec.org/wiki/BIZEC_TEC11>

### Bloom filters

<https://en.wikipedia.org/wiki/Bloom_filter>

### BSI: Build Security In

<https://buildsecurityin.us-cert.gov/bsi/home.html>

### BSIMM (Building Security In Maturity Model)

<http://bsimm.com/>

### Bug Tracking System

<https://en.wikipedia.org/wiki/Bug_tracking_system>

### C-Based Toolchain Hardening Cheat Sheet

<https://www.owasp.org/index.php/C-Based_Toolchain_Hardening_Cheat_Sheet>

### CAESARS (Continuous Asset Evaluation, Situational Awareness, and Risk Scoring) architectural reference

<http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf>

### CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model (NISTIR-7756)

<http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf>

### CAP: Common Alerting Protocol

<https://www.oasis-open.org/committees/download.php/14759/emergency-CAPv1.1.pdf>

### CAPEC (Attack Patterns)

<http://capec.mitre.org/>

### Center for Internet Security (CIS)

<http://www.cisecurity.org>

### CIP-CSP Mind Map

Adam N. Meyer

<http://www.tripwire.com/state-of-security/wp-content/uploads/2013/11/CIP-CSF-Framework.pdf>

### CIS Benchmarks

Center for Internet Security

<https://benchmarks.cisecurity.org/downloads/benchmarks/>

### CLASP

### CloudAudit

Cloud Security Alliance (CSA)

Automated Audit, Assertion, Assessment, and Assurance

<https://cloudsecurityalliance.org/research/cloudaudit/>

### Cloud Auditing Data Federation Working Group (CADF)

<http://www.dmtf.org/standards/cadf>

### Cloud Controls Matrix (CCM)

Cloud Security Alliance (CSA)

Security Controls Framework for Cloud Providers and Consumers

<https://cloudsecurityalliance.org/research/ccm/>

### Cloud Trust Protocol (CTP)

Cloud Security Alliance (CSA)

Promoting Elements of Transparency in the Cloud

<https://cloudsecurityalliance.org/research/ctp/>

### COBIT

ISACA

<http://www.isaca.org/COBIT/Pages/default.aspx>

### Codes for the representation of currencies and funds (ISO 4217:2001)

### Computer Security: Reducing Risks of Malware Infections

<http://www.sciencedaily.com/releases/2013/12/131216142931.htm>

### Computer Security Incident Coordination (CSIC)

NIST

<http://csrc.nist.gov/projects/csic/>

### Computer Security Resource Center (CSRC)

NIST

<http://csrc.nist.gov/index.html>

### Consensus Assessments Initiative (CAI) Questionnaire (CAIQ)

Cloud Security Alliance (CSA)

<https://cloudsecurityalliance.org/research/cai/>

### CSIRT Case Classification

FIRST

<http://www.first.org/_assets/resources/guides/csirt_case_classification.html>

### Cuckoo Hashing

<https://en.wikipedia.org/wiki/Cuckoo_hashing>

### Cuckoo Sandbox

<http://www.cuckoosandbox.org/>

### CVE: Common Vulnerabilities and Exposures

MITRE

<https://cve.mitre.org/>

### CVSS: Common Vulnerability Scoring System (CVSS-SIG)

FIRST

<http://www.first.org/cvss>

### CWE: Common Weaknesses Enumeration

<http://cwe.mitre.org/>

### CWE/SANS Top 25 Most Dangerous Software Errors

<http://cwe.mitre.org/top25/index.html>

### CWRAF: Weakness Risk Analysis Framework

<http://cwe.mitre.org/cwraf/>

### CWSS: Weakness Scoring System

<http://cwe.mitre.org/cwss/>

### Cybersecurity Assurance (CA)

<https://www.dhs.gov/cybersecurity-assurance>

### Cybersecurity Framework

NIST

<http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf>

### Cyber Security Standards

Wikipedia

<http://en.wikipedia.org/wiki/Cyber_security_standards>

### Cyber Technology and Information Security Laboratory (CTISL)

GTRI (Georgia Tech Research Institute)

<http://gtri.gatech.edu/ctisl/>

### Cyber Threat Landscape Report

ENISA

<http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape>

### CybOX (Cyber Observables)

MITRE

<http://cybox.mitre.org>

### Database Model

Wikipedia

<http://en.wikipedia.org/wiki/Database_model>

### Data Classification

Stanford University

<http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html>

### Data Models

<http://en.wikipedia.org/wiki/Data_model>

### Data Structures

Wikipedia

<https://en.wikipedia.org/wiki/Data_structure>

<http://en.wikibooks.org/wiki/Data_Structures>

### Data Structures/Stacks and Queues

<http://en.wikibooks.org/wiki/Data_Structures/Stacks_and_Queues>

### Date and Time on the Internet: Timestamps (RFC3339)

See also ISO 8601

### Deep learning with word2vec and gensim

<http://radimrehurek.com/2013/09/deep-learning-with-word2vec-and-gensim/>

### Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs

ENISA

<https://www.enisa.europa.eu/media/press-releases/enisa-calls-for-better-data-sharing-and-interoperability-among-certs-to-mitigate-cyberattacks>

### Disk Encryption

<https://en.wikipedia.org/wiki/Full_disk_encryption>

<https://en.wikipedia.org/wiki/Hardware-based_full_disk_encryption>

### Distributed Web Honeypots

<http://projects.webappsec.org/Distributed-Web-Honeypots>

### Dublin Core Metadata

<http://www.dublincore.org/>

### eCSIRT

<http://www.ecsirt.net/>

### Encryption Laws

<https://silentcircle.com/web/encryption-laws/>

### Encryption Using Chaos

<http://www.technologyreview.com/news/405207/encryption-using-chaos/>

### ESAPI: OWASP Enterprise Security API

<https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API>

Exploiting a Thesaurus-Based Semantic Net for Knowledge-Based Search  
[http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.7197&rep=rep1&t  
ype=pdf](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.7197&rep=rep1&type=pdf" \t "_blank)

### FIDO (Fast Identity Online)

FIDO Alliance

*Simpler, Stronger Authentication*

<http://fidoalliance.org/fido-standards.html>

### FileVault

<https://en.wikipedia.org/wiki/FileVault>

### FIPS: U.S. Federal Information Processing Standards

NIST

<http://csrc.nist.gov/publications/PubsFIPS.html>

### FIRST

<http://www.first.org>

### GRC Stack (Governance, Risk Management and Compliance)

Cloud Security Alliance

<https://cloudsecurityalliance.org/research/grc-stack/>

### hpfeeds (Honeynet Project generic authenticated datafeed protocol)

<https://github.com/rep/hpfeeds>

<http://hpfriends.honeycloud.net/>

### Hushmail

<https://www.hushmail.com/>

### IANA Protocol Registries

<http://www.ietf.org/assignments/>

### IETF Vulnerability Data Model (VDM)

<http://tools.ietf.org/html/draft-booth-sacm-vuln-model-02>

Information Systems Security Line of Business (ISSLoB)

<https://www.dhs.gov/information-systems-security-line-business>

### Internet Message Format (RFC2822)

### Internet Users' Glossary (RFC1392)

IETF

<http://tools.ietf.org/search/rfc1392>

### ISO 3166 (Country Codes)

<http://www.iso.org/iso/home/standards/country_codes.htm>

### ISO/IEC 27001

<http://www.27000.org/iso-27001.htm>

<https://en.wikipedia.org/wiki/ISO/IEC_27001:2005>

### ITIL

### ITL Security Bulletins

<http://csrc.nist.gov/publications/PubsITLSB.html>

### ITU Recommendation X.1524 : Common weakness enumeration

<http://www.itu.int/rec/T-REC-X.1524/en>

### IVIL: Intermediary Vulnerability Information Language

<http://www.cupfighter.net/index.php/2010/10/ivil-an-xml-schema-to-exchange-vulnerability-information/>

### Large-scale PCAP Data Analysis Using Apache Hadoop

<https://labs.ripe.net/Members/wnagele/large-scale-pcap-data-analysis-using-apache-hadoop>

### Lumberjack Project

<https://fedorahosted.org/lumberjack/>

### MAEC (Malware)

<http://maec.mitre.org/>

### Making Security Measurable (MSM)

A Collection of Information Security Community Standardization Activities and Initiatives

MITRE

<http://measurablesecurity.mitre.org/>

### MANTIS (Cyber Threat Intelligence Management Framework)

Siemens

<http://django-mantis.readthedocs.org/en/latest/>

### [McAfee Labs 2014 Predictions Report](http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf)

McAfee

<http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf>

### Methodology for Managing Privacy Risks

CNIL

<http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf>

<http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf>

### Minion (Security Automation platform)

Mozilla

<https://wiki.mozilla.org/Security/Projects/Minion>

### Misuses and Code Errors (What you should NOT do)

OWASP

<https://www.owasp.org/index.php/Category:Code_Snippet>

<https://www.owasp.org/index.php/Detail_misuse_cases>

### MSM: Making Security Measurable

<http://measurablesecurity.mitre.org/>

### NIST Computer Security Publications

<http://csrc.nist.gov/publications/PubsSPs.html>

### NISP Library

<http://www.dss.mil/isp/fac_clear/download_nispom.html>

### NIST SP 500-291

NIST

<http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf>

### NIST SP 800-34

NIST

<http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>

### NIST SP 800-53 Rev. 4

NIST

<http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>

<https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53>

### NRF: U.S. National Response Framework

FEMA (Federal Emergency Management Agency)

<http://www.fema.gov/national-response-framework>

### OAuth (Open standard for Authorization), OAuth Framework

<https://en.wikipedia.org/wiki/OAuth>

<http://oauth.net/>

### OpenID

<https://en.wikipedia.org/wiki/OpenID>

### OpenSAMM (Software Assurance Maturity Model)

OWASP

<http://www.opensamm.org/>

### Open Source Licenses

<http://opensource.org/licenses>

### Open Source Security Testing Methodology Manual (OSSTMM)

ISECOM

<http://www.isecom.org/research/osstmm.html>

### OSVDB: Open Sourced Vulnerability Database

<http://osvdb.org/>

### OWASP TOP10

<https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>

### OWASP TOP10 For .NET

<http://www.troyhunt.com/2011/12/free-ebook-owasp-top-10-for-net.html>

### OWASP TOP10 For JavaScript

<http://erlend.oftedal.no/blog/?blogid=125>

<https://www.owasp.org/index.php/Category:OWASP_Video>

### Penetration Testing Execution Standard (PTES)

<http://www.pentest-standard.org/index.php/Main_Page>

### Personal Data Definition

CNIL

<http://www.cnil.fr/english/data-protection/personal-data-definition/>

### pfSense

<http://www.pfsense.org/>

### Plover

### Prince 2

“PRINCE2 is a *de facto*standard developed and used extensively by the UK government and is widely recognised and used in the private sector, both in the UK and internationally. It embodies established and proven best practice in project management.”

<http://www.prince-officialsite.com/>

### Protocol Buffers

“Protocol Buffers are a method of serializing structured data. As such, they are useful in developing programs to communicate with each other over a wire or for storing data. The method involves an [interface description language](https://en.wikipedia.org/wiki/Interface_description_language) that describes the structure of some data and a program that generates from that description source code in various programming languages for generating or parsing a stream of bytes that represents the structured data.” Wikipedia

<https://en.wikipedia.org/wiki/Protocol_Buffers>

<https://code.google.com/p/protobuf/>

<https://developers.google.com/protocol-buffers/>

### Resilience and Cyber Security of Technology in the Built Environment

<http://www.theiet.org/resources/standards/cyber-buildings.cfm>

### Resilient Control Systems

<https://en.wikipedia.org/wiki/Resilient_control_systems>

### Revision Control

<https://en.wikipedia.org/wiki/Revision_control>

### RFC 6189 ZRTP: Media Path Key Agreement for Unicast Secure RTP

<http://zfone.com/docs/ietf/rfc6189bis.html>

<https://silentcircle.com/web/technology/>

### Risk Taxonomy (O-RT)

The Open Group

Reference C13K   
US ISBN 1-937218-42-3

<https://www2.opengroup.org/ogsys/catalog/C13K>

### SCADA Patching recommendations

ENISA

Window of exposure… a real problem for SCADA systems?

<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems>

### SCAP (Security Content Automation Protocol)

<http://scap.nist.gov/>

Scoring Missing Terms in Information Retrieval Tasks  
[http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.85.2896&rep=rep1&t  
ype=pdf](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.85.2896&rep=rep1&type=pdf" \t "_blank)

### Secure Coding Cheat Sheet

<https://www.owasp.org/index.php/Secure_Coding_Cheat_Sheet>

### Secure Development Life Cycle (SDLC)

<https://www.owasp.org/index.php/Secure_SDLC_Cheat_Sheet>

### Security Automation and Continuous Monitoring (sacm)

<https://ietf.org/wg/sacm/>

### Security Battleground

<http://www.mcafee.com/us/campaign/securitybattleground/index.html>

### Security Guidelines

Carnegie Mellon University

<https://www.cmu.edu/iso/governance/guidelines/index.html>

### Security of personal data

CNIL

<http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf>

### Selecting Mathematical Models With Greatest Predictive Power: Finding Occam's Razor in an Era of Information Overload

<http://www.sciencedaily.com/releases/2013/11/131120103619.htm>

### Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors

HP Fortify

<http://www.hpenterprisesecurity.com/vulncat/en/docs/Fortify_TaxonomyofSoftwareSecurityErrors.pdf>

### SimpleRisk

SimpleRisk is Enterprise Risk Management simplified.

<http://simplerisk.org>

### Software Assurance

<http://measurablesecurity.mitre.org/directory/areas/softwareassurance.html>

### Software Configuration Management (SCM)

<https://en.wikipedia.org/wiki/Software_configuration_management>

### Software Defined Networking (SDN)

<http://www.federaltechnologyinsider.com/software-defined-networking-heres-what-you-need-to-know/>

### Software Defined Perimeter (SDP)

Cloud Security Alliance

<https://downloads.cloudsecurityalliance.org/initiatives/sdp/Software_Defined_Perimeter.pdf>

### Software Vulnerability Exploitation Trends

Exploring the impact of software mitigations on patterns of vulnerability exploitation

<http://www.microsoft.com/en-sg/download/details.aspx?id=39680>

### Spamhaus

<http://www.spamhaus.org>

### Spear Phishing - Understanding the Threat

UK CPNI

<http://www.cpni.gov.uk/advice/cyber/spear-phishing/>

### SQL Injection Prevention Cheat Sheet

<https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet>

### SQUARE (Security Quality Requirements Engineering)

CERT.org

<http://www.cert.org/sse/square/>

### SSL Labs

Qualys

<https://www.ssllabs.com/>

### STAR (Security, Trust & Assurance Registry)

Cloud Security Alliance (CSA)

<https://cloudsecurityalliance.org/star/>

### STIG: Defense Information Systems Agency Security Technical Implementation Guide

<http://iase.disa.mil/stigs/index.html>

### STIX (Structured Threat Information)

<http://stix.mitre.org/>

### Supply Chain Assurance

CERT.org

<http://www.cert.org/sse/supplychain.html>

### Supply Chain Risk Management

Enabling Transparency for Informing Decision- Making in Reducing Residual Risk Exposures

DHS

<http://csrc.nist.gov/scrm/documents/workshop_oct2012/jarzombek_ict_supply_chain_workshop_oct-15-2012.pdf>

### Tags for Identifying of Languages (RFC4646)

### TAXII (Trusted Automated eXchange of Indicator Information)

<http://taxii.mitre.org/>

### Taxonomies, Controlled Vocabularies, Thesauri and Ontologies

<http://www.taxonomies-sig.org/about.htm>

### THEMIS

<http://www.sciencedaily.com/releases/2013/11/131107191822.htm>

### ThreadFix

Denim Group

<https://github.com/denimgroup/threadfix>

### Threatsaurus

**The A-Z of computer and data security threats**

Sophos

<http://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf>

### TOGAF

The Open Group

“TOGAF®, an Open Group Standard, is a proven enterprise architecture methodology and framework used by the world's leading organizations to improve business efficiency.”

<http://www.opengroup.org/togaf/>

### Ultimate SANS Pen Test Poster

<http://pen-testing.sans.org/blog/pen-testing/2013/06/20/announcing-the-ultimate-sans-pen-test-poster>

### Uncover Security Design Flaws Using The STRIDE Approach

Microsoft

<http://msdn.microsoft.com/en-us/magazine/cc163519.aspx>

### United States Government Configuration Baseline (USGCB)

<http://usgcb.nist.gov/usgcb_content.html>

### VERIS: Vocabulary for Event Recording and Incident Sharing

Verizon

<http://www.veriscommunity.net>

### Version Control

<http://git-scm.com/book/en/Getting-Started-About-Version-Control>

### W3C: World Wide Web Consortium

<http://www.w3.org>

### Water and wastewater SCADA Cybersecurity

ISA

Strategic approach to water and wastewater network architecture and segmentation

<http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=94401>

### Web Application Firewall (WAF) Evaluation Criteria

WASC

<http://www.webappsec.org/projects/wafec/>

### Web Application Security Consortium (WASC)

<http://www.webappsec.org>

### Web Application Security Evaluation Criteria

WASC

<http://www.webappsec.org/projects/wassec/>

### Web Application Cheat Sheets

<https://www.owasp.org/index.php/Category:Cheatsheets>

### Web Security Threat Classification *(WSTC)*

WASC

<http://www.webappsec.org/projects/threat/>

### What is the exact difference between parallel and concurrent programming?

<http://www.quora.com/What-is-the-exact-difference-between-parallel-and-concurrent-programming>

### Winning the Cybersecurity Battle

<http://www.govloop.com/profiles/blogs/the-govloop-guide-winning-the-cybersecurity-battle>

### X-Frame-Options, or solving the wrong problem

<http://lcamtuf.blogspot.ae/2011/12/x-frame-options-or-solving-wrong.html>

### XML Database

<http://en.wikipedia.org/wiki/XML_database>

### XML Encryption

W3C

<http://www.w3.org/TR/xmlenc-core/>

### XORCISM Database model

<https://github.com/athiasjerome/XORCISM>

### XORCISM Tools

<https://github.com/athiasjerome/XORCISM>

### .NET Security Cheat Sheet

<https://www.owasp.org/index.php/.NET_Security_Cheat_Sheet>

## Acknowledgements

The author would like to thank the various organizations, communities and individuals\* participating in the evolution and improvement, by research and innovation, of the cyberspace’s security.

\* This also includes all not specifically mentioned in this document contributing to Cyber Peacefare.

**The views expressed above are solely those of the author and not those of any corporation, its employees, trustees, or assigns.**

## Appendix A: Threats Taxonomies Examples

Note: Information provided “as is”

**The author(s) recommends to use the standardized/widely used Vocabularies listed in the section** [**Taxonomies/Controlled Vocabularies/Thesauri/Ontologies/Classifications**](#_Taxonomies,_Controlled_Vocabularies,)**.**

See [STIX](#_STIX_2), [VERIS](#_VERIS:_Vocabulary_for_3)

### Cyber Attacks extracted from “Winning the Cybersecurity Battle”

Reference: <http://www.govloop.com/profiles/blogs/the-govloop-guide-winning-the-cybersecurity-battle>

* Cross - site scripting
* Denial-of-service
* Distributed Denial-of-service
* Logic bombs
* Other
* Passive wiretapping
* Phishing
* Structured Query Language injection
* Trojan Horses
* Viruses
* Wardriving
* Worms

### Threat Actors (attackers) extracted from “Winning the Cybersecurity Battle”

Reference: <http://www.govloop.com/profiles/blogs/the-govloop-guide-winning-the-cybersecurity-battle>

* Bot - Network operators
* Business competitors
* Criminal groups
* *Hackers*
* Insiders
* International corporate spies
* Nations
* Phishers
* Spammers
* Spyware or malware authors
* Terrorists

### ThreatModeler Glossary (Threat Library by MyAppSecurity)

<http://myappsecurity.com/threatmodeler-glossary-2/>

“Threat Library is a repository of threats provided by ThreatModeler from MITRE’s CAPEC library, WASC Threat Classification, OWASP, as well as other user defined threats.” MyAppSecurity