

Security Indicators Quick Reference Card (v1.1.2)

For ETSI and Club R2GS, designed and edited by [Axel Rennoch](#) (Fraunhofer FOKUS) and [G rard Gaudin](#) (G²C).

This Quick Reference Card summarizes Information Security Indicator components to support users. The document stems from the ETSI GS ISI 001 standard. Further information: https://en.wikipedia.org/wiki/Information_security_indicators.

1.1. Indicators related to security incidents (Ixx)

CLASS	FAMILY	COMPONENT AND IDENTIFIER	PARAMETERS	F	S	D	M
IEX intrusions and external attacks	FGY Website forgery	1 Forged domain or brand names	#ev[30d], #addresses.legitimate, �month[90d]	+	1	3	6
		2 Forged websites	#ev[30d], #org.websites, �month[90d]	+	2-3	2	6
	SPM Spam	1 Not requested received bulk messages	#ev[30d], #messages[30d], �month[90d]	+++	3	3	-
		PHI Phishing	1 Targeting customers' workstations	#ev[30d], #series.unique[30d], const(exposure.media)	+	3	2
	INT Intrusion	2 Targeting organisation's users	#ev[30d], #messages[30d]	++	3	3	6,7
		1 Attempt on externally accessible servers	#ev.day.unique[30d], #servers	+++	1-2	2	-
	DFC Website defacement	2 Success on externally accessible servers	#ev.unique[30d], #servers, �month[90d]	+	3-4	1	5-8
		3 Intrusions on internal servers NEW	#ev.unique[30d], #servers, �month[90d]	++	4	1	5-8
	MIS Misappropriation of resources	1 Obvious and visible website defacements	#ev[30d], #org.websites, �month[90d]	+	3	3	5-7
	DOS Denial of Service	1 Servers resources misappropriation (by external attackers)	#ev[30d], �month[90d]	sig	2	1	5-7
MLW Malware	1 DoS and DDoS attacks on websites	#ev[30d], #org.websites	+	4	3	5-7	
		1 Attempts to install malware on workstations	#ev[30d], #attempt.mw.unique(#types.mw)	+++	1	3	5-7
		2 Attempts to install malware on servers	#ev[30d], #attempt.mw.unique(#types.mw)	++	1	3	3,5-8
		3 Installations on workstations	#ev[30d], �month[90d]	++	1-4	1-3	3,5-8
PHY Physical intrusion or action	4 Installations on internal servers	#ev[30d], �month[90d]	+	2-4	1-3	3,5-8	
	1 Human intrusion into organizations perimeter	#ev[30d], �month[90d]	+	3	1	6	

IMF mal-functions	BRE Accidental breakdowns or malfunctions	1 Workstations breakdowns or malfunctions	#ev[30d], �month[90d]	++	~	3	6,7
		2 Servers breakdowns or malfunctions	#ev[30d], �month[90d]	+	~	3	6,7
		3 Mainframes breakdowns or malfunctions	#ev[30d], �month[90d]	+	~	3	6,7
		4 Networks breakdowns or malfunctions	#ev[30d], �month[90d]	++	~	3	6,7
	MDL Misdelivery content	1 Delivery of email to wrong recipient NEW	#users.concerned.detected[30d], #ev[30d], #users	+	1-4	1	6
	LOM Loss or theft of mobile devices	1 Mobile devices belonging to org.	#ev[30d], #org.devices, �month[90d]	+	3	3	6
LOG Logging malfunction	1 Downtime / malfunction of log production	2 Absence of possible tracking of involved person	#ev[30d], #org.systems, �month[90d]	++	3-4	3	5,6
		3 Downtime/malfunction of log production for recordings with evidential value	#ev[30d], #org.systems, �month[90d]	+	1-2	2	5,6
		#ev[30d], #org.systems.value, �month[90d]	+	3-4	3	5,6	

IDB Internal deviant behaviour	UID Identity usurpation	1 User impersonation	#ev[30d], �month[90d]	+	2-4	1	4-7	
		RGH Rights (or privileges) usurpation or abuse	1 Privilege escalation by exploitation of software or config vul.	#ev[30d], �month[90d]	+	4	2	4-8
			2 Privilege escalation by social engineering	#ev[30d], �month[90d]	sig	3	2	4-8
			3 Use of admin rights illicitly granted by admin	#ev[30d], �month[90d]	sig	3	3	4-8
			4 Use of time-limited rights after period	#ev[30d], �month[90d]	sig	3	2	4-8
			5 Abuse of privileges by admin	#ev[30d], #admins.mis[30d], �month[90d]	sig	3-4	2	4-8
			6 Abuse of privileges by operator or user	#ev[30d], #applications, �month[90d]	sig	2-3	3	4-8
	7 Illicit use of rights not removed (after departure or position change)	#users.mis[30d], �month[90d]	sig	3	2	4-8		
	MIS Misappropriation of resources	1 Server resources misappropriation by an internal source	#users.mis(remote)[30d], �month[90d]	sig	1	1	4-7	
	IAC Illicit access to Internet	1 Access to hacking website (from internal workstation)	#inc[30d], �month[90d]	+	4	1	5,6	
LOG Deactivating of logs recording	1 Deactivating of logs recording by an admin	#admins.performing.detected[30d], �month[90d]	sig	2-3	3	5,6		

1.2. Consolidated indicators of the previous IEX, IMF, IDB security incidents

IWH whole incident class	VNP Non-patched or poorly patched vul. exploitation	1 Exploitation of sw vul. w/o available patch	#ev[30d], #inc.categorized.detected, �month[60d]	key	3	3	3-6
		2 Exploitation of non-patched sw vul.	#ev[30d], #inc.categorized.detected, �month[60d]	key	3	3	3-6
		3 Exploitation of poorly-patched sw vul.	#ev[30d], #inc.categorized.detected, �month[60d]	key	3	3	3-6
	VCN Conf. vul. exploitation	1 Exploitation of config flaw	#ev[30d], #inc.categorized.detected, �month[60d]	key	3	2	2,4-6
	UKN Unknown incidents	1 Not categorized sec incidents	#ev[30d], #inc.categorized.detected, �month[90d]	key	3-4	2	4-6
UNA Incidents on not addressed assets	1 Sec. inc. on non-inventoried/not-managed assets	#ev[30d], #inc.categorized.detected, �month[90d]	key	3-4	3	1,5,6	

Conventions: F (frequency rate: +/++/+++; sig=significant; key to know; ?=undefined), S (severity level: 1[low]-4[highest]; ~[depend on sensitivity]), D (detection rate: 1[very difficult]-3[easy]), M (maturity KPSI) "#" number (quantitative amount); "[30d]" time interval (e.g. 30 days); " " average; " " sum over all incidents; " month" average value of this indicator in last month; "org.xx" xx in the organization

Abbreviations: AP (access point), ev (event), FW (firewall), inc (incident), mis (misbehaving), mw (malware), org (company or organisation), OS (oper.sys.), sec (security), sw (software), vul (vulnerability)

Copyright 2013-2015. Forwarding and copying of this document is permitted for personal and educational purposes provided that authorship is retained and that the content is not modified. This work is not to be distributed for commercial advantage.

2. Indicators related to vulnerabilities (Vxx)

CLASS	FAMILY	COMPONENT AND IDENTIFIER	PARAMETERS	F	S	D	M
VBH Behaviour vulnerabilities	PRC Dangerous protocols used	1 Server accessed by an admin with unsecure protocols	#ev[30d], #admins.system[30d], Ømonth[90d]	sig	2-3	1	4-6
		2 P2P client in a workstation	#users.installing[30d], Ømonth[90d]	++	3	2	5,6
		3 VoIP client in a workstation	#users.installing[30d], Ømonth[90d]	++	1	2	5,6
		4 Outbound connection dangerously set up	#users.installing[30d], Ømonth[90d]	++	2	2	5,6
		5 Not compliant lap top computer used to establish a connection	#users.connecting[30d], #laptops, Ømonth[90d]	++	3	2	2,5,6
		6 Other unsecure protocols used	#ev[30d], Ømonth[90d]	+	2-3	1-2	5,6
	IAC Internet illicit access	1 Outbound controls bypassed	#users.performing[30d], Ømonth[90d]	sig	2-4	1	5,6
		2 Anonymisation site used	#users.performing[30d], Ømonth[90d]	sig	3	3	5,6
	FTR File illicit transfer with outside	1 File recklessly downloaded	#ev[30d], Ømonth[90d]	++	2-3	2	5,6
		2 Personal public instant messaging account used (for business file exchanges)	#users.performing[30d], Ømonth[90d]	+	3	2	5,6
		3 Personal public messaging account used (for business file exchanges)	#users.performing[30d], Ømonth[90d]	sig	2	2	5,6
	WTI Workstation used w/o relevant usual security	1 Workstations accessed in admin mode	#users.performing[30d], Ømonth[60d]	+	2-3	2	2,4-6
		2 Personal storage devices used	#ev[30d], Ømonth[90d]	++	3	1	2,4-6
		3 Personal devices used w/o compartmentalization (BYOD)	#users.performing[30d], #devices.personal, Ømonth[90d]	++	2	1	2,4,6
		4 Not encrypted sensitive files exported	#ev[30d], Ømonth[90d]	++	4	1	5,6
		5 Personal software used	#users.performing[30d], Ømonth[60d]	+	2-3	3	2,5,6
		6 Mailbox/internet access admin mode NEW	#users.concerned[30d], Ømonth[60d]	+	3	3	2,4-6
	PSW Passwords illicitly handled or managed	1 Weak passwords used	#ev[30d], #accounts.users, Ømonth[90d]	sig	3	2	2,4,6
2 Passwords not changed		#ev[30d], #accounts.users, Ømonth[90d]	sig	2	2	2,4,6	
3 Admin passwords not changed		#ev[30d], #accounts.admins, Ømonth[90d]	sig	3	2	2,4,6	
RGH Access rights illicitly granted	1 No compliant user rights granted by admin	#admins.performing[30d], #admins, Ømonth[90d]	+++	3	2	2,4-6	
HUW Human weakness	1 Exploited by phishing message exchanges	#users.performing[month], #users, Ømonth[90d]	+	3	2	6,7	
	2 By exchanges secrets through online media	#users.performing[month], #users, Ømonth[90d]	+	1	1-2	6,7	
VSW Software vul.	WSR Webserver sw. vul.	1 Web applications sw vul.	#ev[30d], #applications.web, Ømonth[90d]	+	3-4	3	3,6
	OSW OS sw. vul.	1 OS sw vul. regarding servers	#ev[30d], #server.ext.visible, Ømonth[90d]	+	2-3	3	3,6
	WBR Webbrowser sw. vul.	1 Webbrowser sw. vul.	#ev[30d], #workstations, Ømonth[90d]	++	2-4	3	3,6
VCF Configuration vul.	DIS Dangerous or illicit services	1 Dangerous or illicit services on externally accessible servers	#ev[30d], #server.ext.visible, Ømonth[90d]	+	2-3	2	1,2,5,6
		LOG Log production shortcomings	1 Insufficient size of the space allocated for logs	#ev[30d], #org.systems, Ømonth[90d]	sig	1	2
	FWR Weak FW config.	1 Weak FW filtering rules	#ev[30d], #FW, Ømonth[90d]	sig	2	1	2,6
	WTI Workstation wrong configured	1 Workstation with bad AV/FW NEW	#users.concerned[30d], Ømonth[60d], #workstations	++	4	3	2,5,6
		2 Autorun feature enabled on workstations	#ev[30d], #workstations, Ømonth[60d]	+	2-3	3	2,6
	UAC User accounts wrongly configured	1 Access rights configuration not compliant with security policy	#users.detected[30d], Ømonth[60d]	+	3	3	2,4-6
2 Not compliant access rights on logs		#ev[30d], #servers, Ømonth[60d]	+	2-3	2/3	2,4-6	
3 Generic and shared admin account		#ev[30d], #OS+#DB+#applications, Ømonth[60d]	sig	2-3	3	2,4,6	
4 Accounts w/o owners		#ev[30d], #OS+#DB+#applications, Ømonth[60d]	+	3	2/3	2,6	
5 Inactive accounts		#ev[30d], #OS+#DB+#applications, Ømonth[60d]	+	2	2	2,4,6	
VTC General sec. technical vul.	BKP Back-up malfunction	1 Malfunction server hosted safeguards NEW	#ev[30d], #servers.safeguards, Ømonth	sig	3	3	6,7
	IDS IDS/IPS malfunction	1 Full unavailability of IDS/IPS	#ev[30d], #IDS/IPS, Ømonth[90d]	sig	3	3	5,6
	WFI Illicit Wi-Fi access points	1 Wi-Fi devices installed on the network w/o any official authorisation	#ev[30d], #APs.WiFi, Ømonth[180d]	sig	4	3	2,6
	RAP Illicit remote access	1 Remote access points used to gain unauthorised access	#ev[30d], #AP.authorized, Ømonth[180d]	?	3	1	5
	NRG Illicit network connections	1 Devices or servers connected to org. network w/o being reg./managed	#ev[30d], #equipment.authorized, Ømonth[90d]	sig	3	2/3	1
	PHY Physical access control	1 Not operational phy. access control means	#ev[30d], #areas.protected, Ømonth[90d]	sig	2-3	2	-
VOR General sec. org. vul.	DSC Discovery of attacks	1 Excessive time to discovery NEW	#ev[30d], #inc.detected [30d],	sig	4	1	6
		2 Excessive time of windows of risk exposure	time.risk(>limit.policy.sec), Ømonth[90d]	+	3-4	2	3
	VNP Not patched vul.	2 Rate of not patched systems	#ev[30d], #systems, Ømonth[90d]	sig	2	2	3
	VNR Not reconfigured systems	1 Rate of not reconfigured systems	#ev[30d], #systems.reconfigured, Ømonth[90d]	sig	2	3	2
	RCT Reaction plans	1 Reactions plans launched w/o experience feedback	#ev[30d], #reactionplans.launched, Ømonth[90d]	sig	2	3	6,7
		2 Reaction plans unsuccessfully launched	#ev[30d], # reactionplans.launched, Ømonth[90d]	sig	4	3	6,7
	PRT Security in IT projects	1 Launch of new IT projects w/o information classification	#ev[30d], #projects.launched, Ømonth[90d]	+	3	3	6
2 Launch of new specific IT projects w/o risk analysis		#ev[30d], #projects.launched, Ømonth[90d]	+	3	3	6	
3 Launch of new IT projects of a standard type w/o identification of vul. and threats		#ev[30d], #projects.launched, Ømonth[90d]	+	3	3	6	

3. Indicators as regards impact measurement (IMP)

IMP	COS costs	1 Average cost to tackle a critical sec. incident	Σcost.inc[30d], Øcost.inc[30d], Øcost.inc(all)[120d]
		2 Due to whole sec incidents	Σtime.inc[30d], Øtime.inc[30d], Øtime[90d]
	TIM Average time of website downtime	2 Due to successful malicious attacks	Σtime.inc[30d], Øtime.inc[30d], Øtime[90d]
3 Due to malfunctions/unintentional sec. incidents		Σtime.inc[30d], Øtime.inc[30d], Øtime[90d]	

Conventions: F (frequency rate: +/+/++/+++; sig=significant; key to know; ?=undefined), S (severity level: 1[low]-4[highest]; ~[depend on sensitivity]), D (detection rate: 1[very difficult]-3[easy]), M (maturity KPSI) "#" number (quantitative amount); "[30d]" time interval (e.g. 30 days); "Ø" average; "Σ" sum over all incidents; "Ømonth" average value of this indicator in last month, "org.xx" xx in the organization
Abbreviations: AP (access point), ev (event), FW (firewall), inc (incident), mis (misbehaving), mw (malware), org (company or organisation), OS (oper.sys.), sec (security), sw (software), vul (vulnerability)

Copyright 2013-2015. Forwarding and copying of this document is permitted for personal and educational purposes provided that authorship is retained and that the content is not modified. This work is not to be distributed for commercial advantage.