ICS / SCADA Проверка за сигурност на: физическа среда, техническа, оперативна и организационна сигурност (мерки)

(Примерен списък с позиции за проверка и попълване относно различните среди и организацията на киберсигурността на производствени системи. Без претенции за изчерпателност и подлежи на допълване или съкращаване при необходимост)

№	НАИМЕНОВАНИЕ	ДА/НЕ	ОПИСАНИЕ НА ЕЛЕМЕНТИТЕ	КОМЕНТАРИ / РЕФЕРЕНЦИИ
	Система: TEST-SYSTEM *(Name Sysytem)*			
	Физическа сигурност			
1.	Налични ли са процедури за физическа сигурност на оборудването на ICS/SCADA			
2.	Местонахождение на компютри/сървъри/бази данни подходящо ли е за сигурността на ICS/SCADA			
3.	Предвидени ли са устройства/карти или комбинации от заключващи устройства, които да ограничават достъпа до помещението с компютърнтото / сървърно оборудване			
4.	Налични ли са процедури за временен достъп от служители, посетители или външни лица изпълнители		например те се придружават по време на изпълнение на дейностите им или се използват пропуски за идентификация и т.н.	
5.	Налични ли са процедури и устройства за осигуряване на чувствително оборудване към риск от природни бетствия			
6.	За други чувствителни зони, освен сървърно помещение като помещение с UPS оборудване или други, предвидени ли са адекватни контроли			
	Технически и оперативни мерки			
1.	Име на индустриална система ICS/SCADA		TEST-SYSTEM.DOMAIN.BG	
2.	Производител на системата ICS/SCADA (внедрил, обслужващ)			
3.	Брой мрежови карти, които ползва системата ICS/SCADA			
3.1.	ИП адрес, Маска, Гейтуей, ДНС (описанието се прави за всяка налична карта) / MAC		IP: xxx.xxx.xxx.xxx	
			MASK: 255.255.255.0	
			GATEWAY: xxx.xxx.xxx.001	
			MAC: 78e3b3356404	
			DNS:	
3.2.	ИП адрес, Маска, Гейтуей, ДНС (описанието се прави за всяка карта)			
3.3.	ИП адрес, Маска, Гейтуей, ДНС (описанието се прави за всяка карта)			
4.	Изолирана ли е системата ICS/SCADA (от други мрежови връзки, системи)			
5.	Свързаност с други системи (ако да, да се опишат системите)			
5.1.	от адрес към адрес, TCP / UDP порт № , предаваи/или приема данни			
6.	Налична ли е директна интернет свързаност (ако е да, защо е необходима)			
7.	Налична ли е директна свързаност към мрежови устройства (модел устройство)			
8.	Ползва ли се ДМЗ, Proxy, Firewall			
9.	Системата е зад защитна стена (ако е да, да се опише модела - софтуерна, хардуерна…)			
10.	Ползва се системи за откриване на проникване IDS (модел, …)			
11.	Поставени ли са IDS (софтуерни и/или физически) на стратегически места (входни точки)			
11.	Системата е инсталирана върху ВМ			
12.	Извършен ли е анализ на мрежовата свързаност към други мрежи (Ако да, да се предостави)			
13.	Системата е върху физическа машина			
14.	ICS/SCADA е върху операционна система Windows OS (версия)			
15.	ICS/SCADA е върху друг тип отворена и/или търговска ОС (да се посочи)			
16.	Премахнати са/деактивирани са неизползваните услуги /функции(ако да, да се опишат кои са изключени)		(автоматично абновяване, електронна поща, интернет, отдалечен достъп,...)	
17.	Налични ли са вградени защитни елементи от производител в самата система (ако да, да се опишат кои са, ползват ли се, или са изключени)			
18.	Налична ли е скрита (задна врата) за влизане от производителя (доставчика) в системата (ако да, защо е необходима)			
19.	Ако е налична, по каква комуникация е предоставена (да се опише, на какви портове, тип свързаност)			
20.	Налична ли е антивирусна система / софтуер (ако да, да се опиша какъв е софтуера, да се опише и останалия софтуер)			

21.	Колко съоръжения имат физическа свързаност към производствената система (ако има, да се опишат)			
22.	Налични физически точки на достъп до системата ICS/SCADA:			
22.1.	дистанционна телефонна линия			
22.2.	компютърна мрежа			
22.3.	оптични кабели			
22.4.	радио(или други) връзки			
22.5.	компютърни терминали			
22.6.	безжични устройства за достъп до мрежата			
22.7.	USB на системата			
23.	Налична ли е (внедрена ли е) система за вътрешно(външно) откриване на проникванията, 24 часово наблюдение на инциденти (ако има, да се опишат)			
24.	Налични ли са резервни копия на системата и план за възстановяването ѝ при евентуални инциденти, бедстствия или др. събития, нарушаващи работоспособността ѝ (ако да, да се предоставят плановете, да се опишат начините за резервно копиране)			
25.	Налично ли е разграничаване на администраторската и потребителска роли (профили)			
26.	Ползват ли се пароли (сложност на паролите)			
27.	Налична ли е политика за ползване на външни / преносими носители			
28.	Налична ли е организация за управлението на кръпки, фиксове и подобрения в софтуера			
29.	Налична ли е политика за свързване на мобилни устройства, лаптопи, телефони, смарт устройства и др.			
30.	Налична ли е политика и/или реална организация за контрол на промените в конфигурациите			
31.	Налична ли е симулационна среда, различна от производствената за извършване на тестове			
Организационни мерки				
1.	Налична ли е политика за сигурност, която се прилага за ICS/SCADA			
2.	Налични ли са процедури за реагиране при инциденти (ако има, се предоставят, описват се)			
3.	Оторизиран персонал с достъп до системата (брой, длъжност, начин на достъп)			
4.	Роли, отговорности, правомощия на персонала с достъп до системата			
5.	Налична ли е организационна структура за кибер сигурност (да се предостави, опише)			
6.	Наличен ли е ред за ескалация на проблеми и /или инциденти (да се предостави процедура и/или друг тип документ)			
7.	Налична ли е мрежова документация за идентифициране на системата, ако да, къде се съхранява, кой има достъп до нея			
8.	Налична ли е оценка на рисковете за системата (ако да, да се пердостави)			
9.	До каква степен е сведено до минимум "Социалното инженерство"			
10.	Налични ли са разписани изисквания за сигурност, които обхващат целия цикъл на разработване, закупуване, управление, поддръжка и подмяна на елементи и/или ICS/SCADA системи, контрол.			
11.	Налични ли са разписани и контролирани правила отнносно обучуния и осведомяване за сигурността на ICS/SCADA на служителите. (ако има от производител и/или локално да се посочат периодика и самите правила.)			
12.	Наличен ли е отговорен служител и/или екип отговорен за сигурността на системите ICS/SCADA. (ако да, се посочва)			

Дата:

Изготвил: