Version	Datum	Ändring
1.3	2018-10-26	CIS Controls version 7 - Åtgärd 3 införd.
1.4	2018-10-05	CIS Controls version 7 - Åtgärd 4 införd.
1.4	2018-10-05	CIS Controls version 7 - Åtgärd 5 införd.

Version: 1.4	Ansvarig: Christoffer Strömblad (https://cstromblad.com/)							
Funktionsområde	*Org ID*	*CSF ID*	*Kategori*	*Förmåga*	*Kommentar*	*Specifika åtgärder*	*Metric*	*ATT&CK Ref*
Identifiera	ORG-1	ID.AM-1	Tillgångshantering (Asset Management)	Inventera och hantera hårdvarutillgångar	Att veta vilka enheter som finns på nätverket är en utgångspunkt för många andra typer av åtgärder. 1. Börja exepelvis med att utnyttja de verktyg ni har, exempelvis DHCP-servrar. De flesta enheter i nätverket behöver en IP-adress vilket innebär att detta ger en relativt god bild av vilka enheter som finns på nätverket. När ni väl etablerat en förmåga att inventera enheter finns det många vägar att gå hur ni utnyttjar den här informationen. Nya enheter skulle exempelvis kunna placeras på ett särskilt VLAN som endast tillåter att man ansluter till vissa begränsade resurser. Först efter att enheten har godkänts av exempelvis IT-avdelningen kan enheten "flyttas" till andra VLAN med fler behörigheter. Det finns som sagt många vägar att gå om hur ni väljer att använda informationen från inventeringen. Kanske väljer ni att automatiskt genomföra en enklare port-scanning av nya enheter för att säkerställa en grundläggande nivå av skydd.	1	Så här skulle du kunna mäta förmågan: 1. Anslut en dator till nätverket och mät hur lång tid det tar innan ansvarig organisation uppmärksammar enheten. 2. Hur lång tid tar det för organisationen att godkänna en nyligen ansluten enhet? 3. Vi kan urskilja godkända från icke-godkända enheter.	N/A
Identifiera	ORG-2	ID.AM-2	Tillgångshantering (Asset Management)	Inventera och hantera mjukvarutillgångar	Du ska dels känna till vilka mjukvaror som finns i organisationen, vilka som behövs och aktivt arbeta för att endast tillåta godkända programvaror att exekvera och installeras. 1. Börja med att dokumentera vilka programvaror som behöver finnas, vilka verksamheter som använder vad och hur ni vill hantera icke-godkända programvaror. 2. Börja inventera. 3. Fortsätt införande av mer specifika åtgärder som exempelvis vitlistning.	Enligt CIS finns tio specifika åtgärder vilka bland annat omfattar: - Inventera programvaror - Säkerställ att godkända programvaror supporteras av leverantörer - Hantera icke-godkända programvaror - Använd vitlistning - Separera, antingen fysiskt eller logiskt, affärskritiska applikationer som samtidigt innebär särskilt mycket risk (kanske programvaror som inte längre stöds och innehåller sårbateter men av affärsmässiga skäl inte ännu kan ersättas)	1. Har organisationen förmåga att identifiera och inventera installerade programvaror? 2. Hur lång tid tar det för organisationen att upptäcka installation av nya programvaror? 3. Har organisationen förmåga att avgöra vilka programvaror som är nödvändiga för verksamheten och inte? 4. Hur lång tid tar det att godkänna en ny programvara? 5. Hur många otillåtna programvaruinstallationer sker varje dag? 6. Har organisationen förmåga att hantera icke-godkända programvaror?	N/A
Upptäcka	ORG-3	DE.CM-8	Kontinuerlig säkerhetsövervakning	Kontinuerlig hantering av sårbarheter	Identifiera sårbarheter inom ramen för organisationens ansvar (system, applikationer, plattformar etc.) Se till att dessa också hanteras med hjälp av riskbedömningar om hur sårbarheterna påverkar organisationens olika verksamheter. 1. Dokumentera en process/plan för att hantera information om sårbarheter som kräver aktiva åtgärder. 2. Skaffa verktyg för sårbarhetsscanning 3. Inloggningsuppgifter till scanningsverktyget för autentiserad scanning 4. Verktyg för automatisk uppdatering av operativsystem och tredjepartsprodukter 5. Process för att genomföra riskbedömningar avseende sårbarheter för att kunna prioritera	Det finns totalt 7 specifika åtgärder vilka bland annat omfattar: - Verktyg för automatisk sårbarhetsscanning - Processer för riskbedömningar avseende sårbarheter - Verktyg för automatisk uppdatering av operativsystem och tredjepartsprodukter.	1. Från det datum då en patch finns tillgänglig för en sårbarhet hur lång tid tar det för er organisation att bedöma risken för sårbarheten? 2. Från det datum då en patch finns tillgänglig hur lång tid tar det innan den är applicerad, testad och inflyttad till produktionsmiljö? 3. Hur många identifierade kritiska sårbarheter är äldre än 30 dagar? 4. Hur många identifierade sårbarheter, som bedömts enkla att exploatera, kan kopplas till er externa miljö? (E.g. publika hemsidor, applikationer eller andra typer av system, brandväggar, routrar osv.) 5. Hur många sårbarheter påverkar, av verksamheten bedöma, kritiska system eller applikationer?	N/A
Skydda	ORG-4	PR.AC-4 PR.PT-1	Identitetshantering, autentisering och behörighetskontroll (PR.AC) Skyddande teknologier (PR.PT)	- Åtkomsträttigheter och behörighetskontroller är hanterade och använder sig utav principen för *least privilege*. - Logghändelser genereras och följs upp på relevanta händelser	1. Beskriv en övergripande plan på målsättning och kriterier för att uppnå denna. 2. Analysera och dokumentera nuvarande arbete med administrativa behörigheter, förstå problembilden innan lösningar och åtgärder införs. 3. Inför flerfaktors-autentisering på administratörs konton 4. Installera och använd särskilda datorer/servrar som är särskilt ämnade för administrativa arbetsuppgifter	Det finns totalt 9 specifika åtgärder vilka bland annat omfattar: - Inventering av administrativa konton - Användning av flerfaktors-autentisering för administrativa konton - Generea logghändelser och följ upp dessa kring användningen av administrativa konton - Använd särskilda datorer/servrar för administrativa uppgifter	- Vi kan, vid ett givet ögonblick, visa exakt hur många som har möjlighet att använda administrativa behörigheter; lokalt på datorer så väl som i nätverket i stort. - Hur stor andel av våra administratörs-konton, jämfört med förra månaden, använder flerfaktors-autentisering? - Vi har förmåga att genom logg-händelser se vem som gjort vad i egenskap av systemadministratör.	https://attack.mitre.org/techniques/T1075 https://attack.mitre.org/techniques/T1097

Skydda	ORG-5	PR.IP-1 PR.IP-3	Processer, och rutiner för skydd av information (PR.IP)		1. Förstå Cyber Kill Chain och formulera några tänkta angreppsvägar mot verksamheten. 2. Bygg säker konfiguration utifrån de "steg" som en angripare behöver genomföra för att utföra ett angrepp.	Det finns totalt 5 specifika åtgärder vilka bland annat omfattar: - Etablera säkra konfigurationer - Lagra OS-images på ett säkert sätt - Installera centralt verktyg för system konfiguration	- Hur många gånger har vi förhindrat att ett PowerShell-script exekverar? - Hur många gånger har ett program förhindrats att exekvera med anledning av konfiguration av AppLocker?	Många beroende på vilken konfiguration som genomförs.