Insider Threat Modenhedsmodel (Baseret på "Insider Threat Program Maturity Model Report af Veriato. Se note")

Dedike A/S
Your Security is our Passion

Modenhedsscore (60%)	60%

Expand for English Texts...

Forklaringer på modenhedsscorer >>			Ikke eksisterende	Reaktiv	Proaktiv	Forudseende	Optimeret
			Organisationen har intet program eller teknologi på plads til at opdage og reagere på insider -trusler, og den er ikke klar over risikoen ved en insider trussel.	Organisationen har ikke noget program på plads, men er klar over, at der findes insider -trusler. IT er ansvarlig for at reagere på eventuelle realiserede trusselshandlinger.	Organisationens fokus er på brugen af teknologier (og den nødvendige kommunikation mellem afdelinger for at lette brugen), der hjælper med at få øje på alle insider-trusler inden for en kernegruppe af højrisiko-brugere.	Organisationen har et formelt program på plads, der søger at identificere potentielle eller aktive trusler så tidligt som muligt. Programdefinitioner, politikker, processer og overvågning er på plads i hele organisationen.	Organisationens ITP (Insider Threat Program) er dynamisk og adaptivt og tager løbende fat på skiftende risiko og ændringer i forretningsdriften, der påvirker den nødvendige politik, proces og teknologi.
Score (0-100%)	**Emne (9)**	**Start herunder i C9. Vælg estimeret modenhedsniveau for hvert emne. (Udfyldt af 5/9)**					
50%	**#1: Mål og og formål**	**3. Proaktiv**	Ingen	Svar på problemer, når de opstår. Undersøg efter behov for at identificere, hvilke handlinger der fandt sted (hvis det er muligt).	Overvåg brugere med den største risiko for organisationen for upassende aktivitet.	Etabler passende overvågningsniveauer for alle medarbejdere. Identificer potentielle trusler tidligt. Reager passende på både førende og aktive indikatorer for trusselsaktivitet.	Sørg for, at insider -trusselprogrammet opfylder organisationens skiftende behov gennem gennemgang, tilpasning og optimering af processer, overvågning og svar.
25%	**#2: Awareness**	**2. Reaktiv**	Organisationen har ingen synlighed i medarbejderaktivitet og heller ikke i, om de har været eller er offer for en insider -trussel.	Organisationen er generelt opmærksom på insider-trusler, men får besked fra medarbejdere eller tredjeparter om, at der er sket en handling.	Organisationen er opmærksom på insider-trusler og tager skridt til at overvåge aktivitet i et forsøg på at opdage ondsindede trusler fra brugere, der anses for højrisiko for organisationen.	Organisationen er meget opmærksom på insider -trusler. Mens fokus er på ondsindede insidere, er organisationen fokuseret på at identificere ledende indikatorer for trusler i bestræbelserne på at stoppe trusler, før det sker.	Organisationen har et modent syn på risiko for insider -trusler - ser det som noget, der bevæger sig i hele organisationen, med hver medarbejder som en potentiel trussel. Hver kilde til aktivitetsdetaljer bruges til at give et fuldstændigt billede af medarbejderrisiko.
50%	**#3: Styring og kontrol**	**3. Proaktiv**	Ingen	Ingen	Minimalt etableret regelsæt. Uformel interaktion mellem IT, HR og Executive teams.	Tilsyn etableres med et formaliseret team fra IT, HR, Exec, Legal og Security. Trusseldefinitioner findes. Grundlæggende proces og politikker er på plads.	ITP -teamet indeholder nøglemedarbejdere og en udpeget Senior ITP - embedsmand til at stå i spidsen for teamet. Der findes skriftlige politikker og processer. ITP - teamet mødes ved hjælp af en almindelig kadence.
75%	**#4: Risikovurdering**	**4. Forudseende**	Ingen	Ingen	Identificerede personer med høj risiko og roller, der kræver overvågning.	Risikoniveauer defineres, roller med høj og lav risiko tildeles. Der foretages specifikke engangsvurderinger for enkeltpersoner.	Risikogennemgang, omfordeling af risikoniveauer og tilhørende overvågningsforanstaltninger sker regelmæssigt for både roller og enkeltpersoner.
100%	**#5: Politikker**	**5. Optimeret**	Ingen	Ingen	Enten ingen eller grundlæggende politikker findes for personer med høj risiko, drevet af HR eller IT.	Der findes politikker omkring BYOD, korrekt brug af virksomhedens ressourcer og opretholdelse af fortrolighed.	Politikker undersøges rutinemæssigt for at sikre, at de stemmer overens med andre ændringer i programmet.
	#6: Overvågning		Ingen	Ingen	Aktivitet overvåges for foruddefinerede aktivitetstærskler, organisationen sidestiller som indikatorer for risiko.	Aktivitet overvåges for både ledende og aktive indikatorer for trusler baseret på både statiske definitioner og adfærdsanalyse.	Activity is monitored for both leading and active indicators of threats based on both static definitions and behavioral analysis.
	#7: Processer		Ingen	Ingen	Der findes kun uformelle processer omkring gennemgang af aktivitet og nødvendig reaktion.	Alle medarbejdere overvåges for førende trusselsindikatorer ved hjælp af User Behavior Analytics (UBA) og User Activity Monitoring (UAM). Tydelige og definerede processer er på plads for højrisiko-scenarier.	Alle medarbejdere overvåges for førende trusselsindikatorer ved hjælp af User Behavior Analytics (UBA) og User Activity Monitoring (UAM). Detaljerede processer er på plads for specifikke lav- og højrisiko-scenarier og evalueres og testes rutinemæssigt.
	#8: Kilder til viden		Ingen	Ingen	Identificerede personer med høj risiko og roller, der kræver overvågning.	Risikoniveauer defineres, roller med høj og lav risiko tildeles. Der foretages specifikke engangsvurderinger for enkeltpersoner.	Risikogennemgang, omfordeling af risikoniveauer og tilhørende overvågningsforanstaltninger sker regelmæssigt for både roller og enkeltpersoner.
	#9: Kommunikation og træning		Ingen	Ingen	Grundlæggende acceptabel brugspolitik på plads.	Acceptabel brugspolitik, Formelt program for beskyttelse af børn (CIPA) bruges til alle nyansættelser.	Politik for acceptabel brug, CIPA og sikkerhedserkendelse er alle underskrevet af medarbejdere. Logonbannere bekræfter korrekt brug, fortrolighed og sikkerhed.
60%	**Gennemsnitlig score**						

Dediko A/S
www.dediko.dk
Tel: +45 45 76 20 21