



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Situation awareness

Handreiking

Situation awareness

Situation awareness – ook wel situational awareness genoemd – is een term die vaak de revue passeert in het cyber security domein. Zo wordt het vaak gebruikt in de context van het verhogen van cyberweerbaarheid. Desondanks is er geen eenduidige consensus over wat het precies is. Deze handreiking heeft als doel duidelijk te maken wat situation awareness is en hoe dit kan bijdragen aan een verhoogde cyberweerbaarheid.

Wat is situation awareness?

Op dit moment is er geen specifieke definitie van situation awareness in cyber security. Mica Endsley heeft hier veel over geschreven vanuit haar rol als wetenschapper bij de Amerikaanse Luchtmacht. Zij heeft een model voor situation awareness ontwikkeld dat ze toeschrijft naar een dynamische omgeving.¹ Dat is het cyberdomein bij uitstek en maakt dit model geschikt om situation awareness in ons vak te definiëren en te begrijpen.

Situation awareness wordt door Endsley² beschreven als een interactief proces, bestaande uit drie niveaus:

1. *Perceptie van elementen in de huidige situatie* – Om je heen kijken en observeren wat er gebeurt. Het behelst onder andere het verzamelen van informatie, zoals logbestanden, accounts met meerdere foutieve inlogpogingen en ontwikkelingen in het nieuws.
2. *Begrip van de huidige situatie* – De impact van een incident kunnen inschatten. Dit heeft betrekking op de ernst van de kwetsbaarheid en het effect die potentiële mitigerende maatregelen erop kunnen hebben.
3. *Projectie van de toekomstige status* – Het voorspellen van hoe een security incident zich zal ontwikkelen, door voort te bouwen op de twee eerdere niveaus. Ervaring uit eerdere situaties speelt hierbij een belangrijke rol.

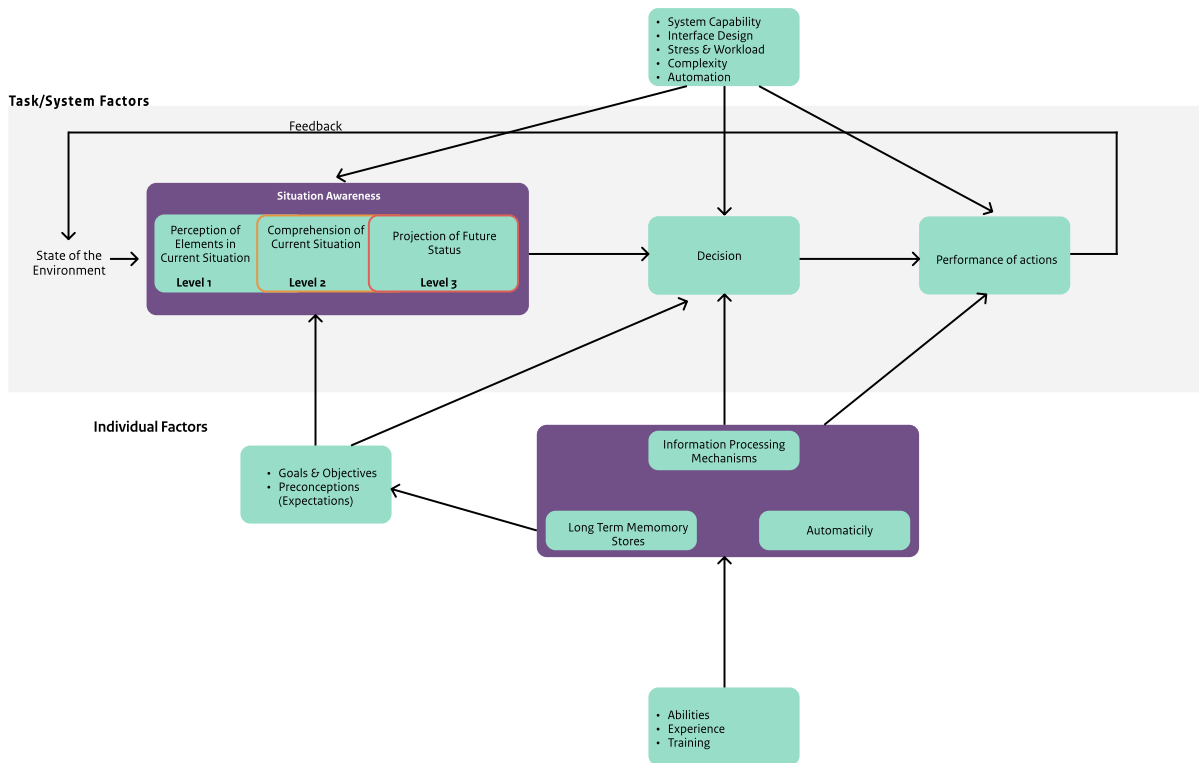
Hoe werkt situation awareness?

Situation awareness wordt niet bereikt door bovengenoemde punten simpelweg af te gaan. Het is een dynamisch proces, waarop verschillende factoren van invloed zijn. Dit is terug te zien in het model van Endsley, *figuur 1*. Deze factoren kunnen situation awareness op verschillende niveaus

¹Endsley, M.R. (1995), "Toward a Theory of Situation Awareness in Dynamic Systems", *Human Factors Journal* 37(1), pp. 32-64.

²Endsley, M.R. (1995), "Toward a Theory of Situation Awareness in Dynamic Systems", *Human Factors Journal* 37(1), pp. 32-64.

beïnvloeden. Dit betekent dat ze effect kunnen hebben op iemands begrip van een situatie, en dus ook op de besluiten die erover gemaakt worden.



Figuur 1: Model Endsley

In deze handreiking bespreken we niet alle factoren die van invloed zijn op situation awareness. Wel besteden we aandacht aan cognitieve factoren, omdat deze bij uitstek van invloed zijn op besluitvormingsprocessen en beeldvorming.³ Denk hierbij aan de hoeveelheid informatie die iemand kan verwerken. Bijvoorbeeld, een SOC-medewerker die de hele dag door veel verschillende rapporten krijgt toegestuurd, kan niet altijd alles met evenveel aandacht doornemen. Laat staan dat diegene de impact van alles wat in de rapporten staat goed kan inschatten. Als er sprake is van een overload aan informatie kan de situation awareness dus negatief beïnvloed worden.

Ook zogeheten *mental models* spelen een rol. Een mental model is een systemisch begrip van hoe iets werkt. Zo ontwikkelen systeembeheerders bijvoorbeeld een begrip van wanneer hun systeem abnormaal gedrag vertoont en er mogelijk sprake is van een security incident. Dit begrip helpt mensen ook bij het bepalen welke informatie er al dan niet relevant is en is op deze manier ook van invloed op de verschillende niveaus van situation awareness.

Mental models hangen nauw samen met de doelen die iemand beoogt. Op basis van een doel bepaalt iemand namelijk wat wel of niet belangrijk is, en dus hoe en waarover besluiten worden

³Banbury, S., & Tremblay, S. (2017). *A cognitive approach to situation awareness: Theory and application*. Routledge.

genomen. Een doel kan bijvoorbeeld het in de lucht houden van een specifiek systeem zijn, of het voorkomen van lekken van klantgegevens.

Op basis van een duidelijk doel zal die persoon aandacht besteden aan de hiervoor relevante informatie. Dit betekent dat informatie die betrekking heeft op het behalen van een specifiek doel meer aandacht zal krijgen en dus zal worden meegenomen in de impactbepaling. Daartegenover staat dat informatie die niet lijkt bij te dragen aan het behalen van dit doel, vaak niet met dezelfde aandacht wordt bekeken. Dit kan ertoe leiden dat relevante input niet wordt meegenomen. Op deze manier beïnvloedt het eveneens situation awareness op verschillende niveaus.

Naast de bovengenoemde, zijn er veel andere factoren van invloed op situation awareness. Hierbij kan je denken aan systemen waarmee mensen werken, stress en de complexiteit van een omgeving.

Op wie is situation awareness van toepassing?

Situation awareness is van toepassing op verschillende lagen. Denk hierbij aan individuen, teams en organisaties. Elk individu heeft diens eigen situation awareness in diens eigen rol. Gezamenlijk vormen de individuen de situation awareness van hun team, dat weer afhankelijk is van het type team en de verantwoordelijkheid dat het heeft. De teams samen vormen op hun beurt weer de situation awareness van de organisatie. Zo zou je kunnen stellen dat volledige situation awareness voor een bepaald doel bereikt kan worden door de situation awareness van alle betrokken organisaties samen te brengen. Bijvoorbeeld op sectoraal of landelijk niveau. Hierbij is het delen van de juiste informatie met elkaar ontzettend belangrijk.

Wat is het verschil tussen situation awareness en situationeel beeld?

Situation awareness en situationeel beeld zijn termen die veel door elkaar heen worden gebruikt. Hoewel de twee absoluut met elkaar te maken hebben, is er een verschil. Een situationeel beeld is de beschrijving van de huidige situatie met huidige stand van ontwikkelingen. Denk hierbij bijvoorbeeld aan een rapport met de nieuwste ontwikkelingen rondom een bepaalde situatie. Dit kan bijdragen aan een verhoogde situation awareness, omdat het inzicht en informatie voorziet.

Situation awareness is het vermogen om de huidige status te observeren en te bepalen wat er belangrijk is en hoe de situatie zich gaat ontwikkelen. Het kan daarom op zijn beurt van invloed zijn op het situationeel beeld.

Hoe gebruik je situation awareness?

Ieder individu, team, en organisatie heeft een eigen situation awareness. Door onderling informatie te delen, kan je daarom tot een hogere mate van situation awareness komen en kan je een gegeven situatie of incident beter begrijpen. Dit maakt het mogelijk om de juiste besluiten op basis van de juiste informatie te maken. Deze besluiten hebben het potentieel om de koers van een incident te wijzigen, waardoor de impact en de situatie ook veranderen.

In het delen van informatie is het goed om na te gaan wat het doel, de rol en de verantwoordelijkheid is van het betreffende individu, team of organisatie waarmee je informatie deelt of waarvan je informatie ontvangt. Een management team op c-level, heeft waarschijnlijk een ander doel dan een operationeel team en heeft daarom andere informatie nodig.

Door een duidelijk beeld te hebben van het doel en de verantwoordelijkheid van een ander, ben je beter in staat de voor hen nodige informatie te delen. Zo worden ze niet overladen met informatie

en stel je hen in staat betere keuzes te maken. Vooral in complexe en dynamische omgevingen, zoals cyber security, is het namelijk makkelijk om mensen te overbelasten.⁴

Tot slot is het van belang om te benoemen dat simpelweg de juiste informatie met de juiste mensen op het juiste moment te delen niet altijd voldoende is om situation awareness te verhogen.⁵ Minstens zo belangrijk is dat de informatie op een bruikbare manier met de ander wordt gedeeld.

Als de ontvangende partij een ontvangen bestand nog moet converteren en bewerken, kan dit bijvoorbeeld veel tijd in beslag nemen waardoor andere essentiële informatie niet wordt bekeken. Het helpt wederom om het doel van de ander scherp te hebben, zodat je weet welke informatie ze zullen gebruiken en hoe ze dit zullen doen. Bij het delen van informatie is vertrouwen tussen de verschillende informatie-delende partners van essentieel belang.⁶ Immers, als je niet vertrouwt dat een partner zorgvuldig met de gedeelde informatie omgaat, dan ben je terughoudender om die informatie te delen.

Het delen van informatie verhoogt situation awareness. Dit stelt jou en anderen in staat om betere beslissingen te nemen. Hierbij is het van belang dat je je bewust bent van de factoren die van invloed zijn op situation awareness en dat er sprake is van vertrouwen tussen de informatie-delende partners.

⁴Endsley, M.R. (1995), "Toward a Theory of Situation Awareness in Dynamic Systems", *Human Factors Journal* 37(1), pp. 32-64.

⁵Preden, J. S., Motus, L., Pahtma, R., & Meriste, M. (2012, March). Data exchange for shared situation awareness. In *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support* (pp. 198-201). IEEE.

⁶T. Kokkonen, J. Hautamäki, J. Siltanen and T. Hämäläinen, "Model for sharing the information of cyber security situation awareness between organizations," *2016 23rd International Conference on Telecommunications (ICT)*, Thessaloniki, Greece, 2016, pp. 1-5, doi: 10.1109/ICT.2016.7500406.

Uitgave

Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie

www.ncsc.nl
info@ncsc.nl
[@ncsc_nl](https://twitter.com/ncsc_nl)

[april] [2025]