axians

E-BOOK

SOC-diensten uitbesteden? Dit zijn de 6 voordelen!

Axians
Rivium Boulevard 41
2909 LK Capelle aan den IJssel
Tel: +31 88 988 96 00
axians.nl/cybersquad

The best of ICT with a human touch

VINCI ENERGIES

SOC-diensten uitbesteden? Dit zijn de 6 voordelen!

"Wat is het nut van het kunnen signaleren van kwaadaardige activiteiten als je de meldingen niet monitort en opvolgt?"

Wat is het nut van het kunnen signaleren van kwaadaardige activiteiten als je de meldingen niet monitort en opvolgt? De periode tussen het eerste contactmoment en het overgaan op een aanval duurt nog slechts enkele maanden of soms dagen. Wil je voorkomen dat de digitale veiligheid van jouw organisatie in het gedrang komt, dan is het essentieel om de situatie actief te blijven monitoren.

Laten we beginnen met het beantwoorden van de vraag: wat is een Security Operations Center, oftewel SOC? Het verkeer dat je IT-infrastructuur binnenkomt kan kwaadaardig blijken. Wanneer dit gebeurt, is het van belang dat je er direct bij bent. In een SOC houdt een toegewijd team van cyber security-specialisten de omgeving nauwlettend voor je in de gaten. Ze identificeren en analyseren beveiligingsmeldingen en beoordelen op potentieel gevaar. Indien nodig komt het SOC vervolgens met een passend mitigatie-advies en wordt de detectie uiteraard gerapporteerd. Is er daadwerkelijk sprake van een beveiligingsincident, dan initiëren de specialisten ook een onderzoek naar hoe dit heeft kunnen plaatsvinden.

Wat gemonitord en welke forensische informatie verzameld kan worden, is uiteraard afhankelijk van de gekozen EDR-, NDR-, en/of SIEM-oplossing. Maar wie is bij jouw organisatie de professional die de SOC-dienstverlening uitvoert? Een eigen SOC is vaak enkel weggelegd voor organisaties met een grote IT-afdeling die over voldoende middelen beschikken. Ontbreekt het hieraan? Dan kiezen de meeste organisaties voor rust, zekerheid én flexibiliteit door de SOC-diensten uit te besteden, en hiermee in één klap externe skills en expertise in huis te halen.

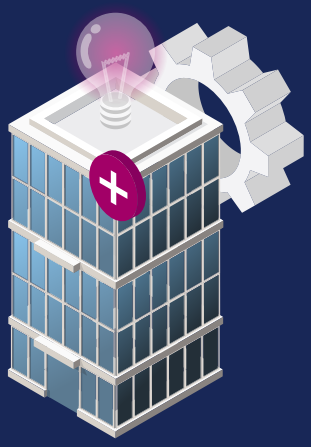
Het uitbesteden van je SOC-diensten zorgt om deze 6 redenen voor rust, zekerheid en flexibiliteit

Je weet dat de bewaking van jouw IT-landschap in de handen ligt van de beste security-specialisten

Het werven en vasthouden van gekwalificeerd personeel blijft een uitdaging. Het opereren van een SOC is daarnaast een complexe en specialistische opdracht, die er vaak niet even bij gedaan kan worden. En dan hebben we het nog niet gehad over de tijd die het vraagt van IT-personeel om de kennis up-to-date te houden. Ook op het gebied van cyberaanvallen staan de ontwikkelingen immers niet stil.

Wanneer je de keuze maakt om de SOC-diensten uit te besteden, ligt de bewaking van jouw IT-landschap in de handen van specialisten. Zij zijn dagelijks bezig met inzicht krijgen op je IT-omgeving en het monitoren van de meldingen die hieruit voortkomen. En zij kunnen in het geval van een daadwerkelijke cyberaanval snel en adequaat reageren. Helaas zien we vaak genoeg gebeuren dat, door onderbezetting of het niet goed beoordelen van de prioriteit, een melding pas een paar weken later wordt opgepakt. En dat is niet zonder risico. De kans is groot dat de schade dan al is aangericht. Dit probleem ondervang je wanneer je beroep doet op een partner.

Je groeit automatisch mee met onze nieuwe technologieën



Voor de gemiddelde IT-afdeling blijft het een uitdaging om alleen al de dagelijkse gang van zaken bij te benen. Laat staan dat er tijd vrij is om bezig te zijn met de toekomst. Terwijl voor de continuïteit van de organisatie een veilige IT-infrastructuur onmisbaar is. Want wanneer een hacker jouw organisatie platlegt, leidt dit niet alleen tot financieel verlies, maar ook tot imagoschade. Door automatisch mee te groeien met de nieuwe technologieën die in het SOC gebruikt worden, voldoe je aan de juiste eisen om de ambities van jouw organisatie te realiseren. Je beschikt zo altijd over de nieuwste functionaliteiten en de laatste updates, zonder extra vergoedingen of licenties aan te hoeven schaffen.

Daarnaast komen er elke dag nieuwe kwetsbaarheden (vulnerabilities) bij. Het missen of te laat doorvoeren van een update vergroot de kans op een veiligheidsincident. De SOC-analist helpt je om deze kwetsbaarheden in je omgeving inzichtelijk te maken en geeft je advies hoe je de kwetsbare systemen kunt patchen (fysiek of virtueel). Hierdoor heb je altijd een actueel overzicht, weet je wat je moet patchen, welke patches er beschikbaar zijn en welke kwetsbaarheden prioriteit moeten krijgen. En omdat jouw IT-personeel dit niet zelf hoeft te monitoren, bespaar je bovendien kostbare tijd.

Je gaat van het managen van incidenten en alarmen, naar tijd voor het ondersteunen van de business

Om een veilige IT-infrastructuur te behouden, is het essentieel om continu te monitoren wat er zich afspeelt binnen de systemen. Denk daarnaast ook aan het analyseren, verdedigen en rapporteren van de detectie. Een tijdrovende klus waarvoor het wederom bijna onmogelijk is om zelf alle specialistische kennis in huis te hebben. Kies je voor het uitbesteden van je SOC-diensten dan krijgen eigen IT'ers veel meer tijd om de business te ondersteunen. Ze hoeven immers niet langer incidenten en alarmen te managen. Hiermee kan je dus optimaal gebruik maken van de tijd en skills van je eigen personeel, terwijl de specialisten jouw IT-landschap veilig houden.

Dankzij ‘as a service’ heb je relatief gezien geen grote investeringen én kan je eenvoudig op- en afschalen

Natuurlijk zijn er kosten verbonden aan een extern SOC. Deze kosten liggen wel aanzienlijk lager, dan wanneer je zelf een eigen SOC wilt opstarten. Dit zijn niet alleen de materialen, maar je moet ook je eigen personeel opleiden of specialisten in dienst nemen. En die zijn schaars. Wanneer je bovendien de investeringskosten afzet tegen de herstelkosten bij schade, is de investering slechts een fractie daarvan. Denk bijvoorbeeld aan dataverlies, reputatieschade en business continuïteit.

Organisaties moeten daarnaast snel met de markt kunnen meebewegen. De mogelijkheid om te kunnen op- en afschalen is hierbij cruciaal. Dankzij 'as a service' betaal je alleen voor wat je gebruikt en nodig hebt. Stel door een overname wordt je IT-infrastructuur 20% groter en je krijgt aanzienlijk meer netwerkverkeer dat gemonitord moet worden, dan kan je eenvoudig je SOC-diensten hierop laten aanpassen. Door snel op- en afschalen voorkom je overbodige resources, wat leidt tot een kostenvoordeel. Wanneer je een eigen SOC hebt, ben je hier minder flexibel in. Een collega waar tijdelijk geen werk voor is, moet je toch betalen. En andersom: een (tijdelijke) extra security-specialist in dienst nemen is tegenwoordig bijna een onmogelijke opgave.

Jouw organisatie wordt beschermd door experts die ook zicht hebben op de technieken die cybercriminelen inzetten bij andere bedrijven

Cybercriminelen hanteren steeds slimmere en snellere aanvallen. Zelfs artificial intelligence (AI) en machine learning (ML) behoren voor hen tot de dagelijkse kost. Bijhouden welke technieken ze inzetten is voor de meeste organisaties onbegonnen werk. Zij hebben immers niet direct zicht op de technieken die worden ingezet bij andere bedrijven. De specialisten in het SOC wel. Ze kunnen de aanvallen sneller herkennen, de juiste verdediging implementeren én deze kennis inzetten om vervolgens ook jouw organisatie te beschermen.

Je hebt altijd zicht op de securitystatus van je infrastructuur, apps en data

Wil je de schade bij een cyberaanval zo klein mogelijk houden of zelfs voorkomen, dan is inzicht een van de belangrijkste factoren, zo niet de belangrijkste. Zicht op je netwerk, op kwetsbaarheden en op gaten in de verdediging. In het SOC worden de meest geavanceerde technologieën gecombineerd om te komen tot volledige end-to-end visibility op het applicatie-, data- en serverlandschap. Op basis van maandelijkse rapportage wordt je op de hoogte gehouden van de securitystatus, welke activiteiten hebben plaatsgevonden en hoe daarop is gereageerd. Zo bespaar je tijd omdat je niet zelf de situatie hoeft te monitoren én houd je grip op de securitysituatie van je infrastructuur, apps en data.

Get in touch

Kies ook voor rust, zekerheid én flexibiliteit door de SOC-diensten uit te besteden, en haal hiermee in één klap externe skills en expertise in huis. Van het identificeren waar de risico's voor jouw organisatie liggen tot aan het monitoren van het verkeer in je IT-infrastructuur. Elke stap die je neemt, draagt bij aan een veilige organisatie. Welke wensen heeft jouw organisatie?

Neem vrijblijvend contact op en we kijken samen naar waar je staat, waar je naartoe wil, hoe je daar komt én hoe je daar blijft.

Guido Eschbach
Client Manager Security
+31 6 5362 9465
guido.eschbach@axians.com

The best of ICT with a human touch

axians

Rivium Boulevard 41
2909 LK Capelle aan den IJssel
Tel: +31 88 988 96 00
axians.nl/cybersquad