

Initiële Use Cases SOC-dienstverlening Monitoring en Alarmering

Overzicht minimaal af te dekken use cases voor PA (CSIR 3.0 pagina 82) en KA

Nummer	Use Cases PA	Beschrijving
1	Mislukte autorisatiepogingen	BV een upload/download poging van een PLC met een onjuist wachtwoord
2	Verboden protocollen geconstateerd	BV een telnet sessie opzetten van een ES naar een Switch
3	Poging uitgaand verkeer	BV ping naar www.kpn.com van een PA netwerk
4	Koppeling met KA geconstateerd	BV een connectie van KA naar PA d.m.v. een Ping of Telnet poging
5	Malware Virusmelding	BV een DNS request doen naar een TOR site ('57g7spgrzlojinaz.onion' voorbeeld WannaCry)
6	configuratie wijzigingen in de beveiligingsinstellingen	BV een password wijzigen van een device met een voorspelbaar wachtwoord (password 1234, masterkey)
7	Afwijkend remote gedrag	BV een connectie van een ES binnen KA naar PA of een 4G LTE router verbinden met een PA netwerk
8	software configuratie gewijzigd	BV een upload / download van een PLC met juiste inloggegevens?
Nummer	Use Case KA	Beschrijving
9	Identity and access	Veranderingen aan 'admin'-accounts (bijvoorbeeld wachtwoordwijziging) en afwijkend gebruik van admin accounts (bijv. tijdstip/locatie of vanaf niet logische plek inloggen, abnormaal gedrag). Inclusief Anomalous privilege escalation en wijzigingen van administratieve groepen, zowel op domein- als lokaal op serverniveau.
10	Bewaken belangrijke servers	Veranderingen aan (belangrijke) systemen en programma's detecteren. Inclusief Installeren/stoppen/starten van niet standaard services/ daemons.
11	Netwerkverkeer	Alerts genereren aan de hand van IOC's. Detecteren van het "raken van IOC's", inclusief netwerk intrusion
12	Netwerkverkeer	Detect lateral movement
13	Netwerkverkeer	Onveilige diensten/software/protocollen detecteren. (Netwerkverkeer sniffen). Monitor Network devices - monitoring traffic over time and detecting unusual spikes, non-trusted communication sources, insecure protocols, and other signs of malicious behavior.
14	Accountgebruik	Afwijkend gebruik van accounts over een tijdsbestek van 24 uur, bijvoorbeeld min of meer simultaan gebruik van een account vanuit bijvoorbeeld een Russisch en een Nederlands IP-adres.
15	Accountgebruik	Acties vanuit 1 account, vanuit 1 machine, of vanuit 1 IP-adres richting een hoop gemonitorde servers, bijvoorbeeld het benaderen van shares op vele verschillende servers vanuit 1 adres.
16	End points	Compromised End-points detecteren, inclusief servers/netwerk- componenten
17	Attacks	Detect Phishing en malware attacks, application intrusion attacks
18	Audittrail	Manipulatie van audittrail: een aanvaller kan proberen eigen acties te verbergen door de audittrail van gemonitorde devices te wijzigen of te verwijderen

De kracht van samen