Meer inzicht, minder concessies

De SOC die wél alles ziet

Elke organisatie is anders en heeft – in grote lijnen – andere behoeften op het gebied van cybersecurity. Dat klopt. Maar betekent dat meteen dat elk bedrijf compleet verschillende SOC use cases nodig heeft? Nee.

In de praktijk is er altijd overlap in de use cases die organisaties gebruiken. Dus waarom keer op keer use cases die al lang bestaan opnieuw ontwikkelen?

De SOC zonder blinde vlekken

De SOC van IP4Sure maakt gebruik van InsightIDR software van Rapid7. Daarmee heeft u toegang tot meer dan 100 pre-built use cases. Waar u niets extra voor betaalt. Kies zorgeloos en onbeperkt use cases uit voor uw organisatie en krijg relevante meldingen.

Een use case nodig die er niet tussen staat? Dan is maatwerk altijd mogelijk. Bel voor meer informatie naar 040-2444666 of mail naar info@ip4sure.nl

Pre-built use cases

FASE 0: VISIBILITY	
Pre-built detectie:	Notificatie wanneer:
ACCOUNT LEAK	De inloggegevens van een gebruiker zijn mogelijk gelekt.
EXPLOITABLE MOBILE DEVICE	Een gebruiker gebruikt een verouderd besturingssysteem op een mobile device.
NEW MOBILE DEVICE	Een gebruiker verkrijgt vanaf een nieuw mobile device toegang tot het netwerk.
STALE MOBILE DEVICE	Een “watchlist” gebruiker krijgt voor het eerst in 30 dagen toegang tot het netwerk met een mobile device.

FASE 1: INFILTRATION & PERSISTENCE	
Pre-built detectie:	Notificatie wanneer:
ACCOUNT ENABLED	Een account dat eerder uitgeschakeld was, is opnieuw geactiveerd door een admin.
ACCOUNT PASSWORD RESET	Een gebruiker reset het wachtwoord van een account.
ACCOUNT PRIVILEGE ESCALATED	Een admin geeft een account meer rechten.
ACCOUNT RECEIVED SUSPICIOUS LINK	Een gebruiker ontvangt een email met een link die geregistreerd staat als malafide.
ACCOUNT VISITS SUSPICIOUS LINK	Een gebruiker gaat naar een link die geregistreerd staat als malafide.
ADVANCED MALWARE ALERT	Een geavanceerd malwaresysteem genereert een melding.
AUTHENTICATION ATTEMPT FROM DISABLED ACCOUNT	Een gebruiker probeert in te loggen met een account dat uitgeschakeld is.
DETECTION EVASION - EVENT LOG DELETION	Een gebruiker verwijdert event logs van een apparaat.
DETECTION EVASION - LOCAL EVENT LOG DELETION	Een local account verwijdert event logs van een apparaat.
DNS QUERY TO NEWLY REGISTERED DOMAIN	Een gebruiker doet een DNS-query bij een nieuw geregistreerd internetdomein.
FLAGGED HASH ON ASSET	Een flagged process hash wordt voor de eerste keer uitgevoerd op een apparaat.
FLAGGED PROCESS ON ASSET	Een flagged process name wordt voor de eerste keer uitgevoerd op een apparaat.

HARVESTED CREDENTIALS	Meerdere accounts proberen in te loggen vanaf een ongebruikelijke locatie.
INGRESS FROM ACCOUNT WHOSE PASSWORD NEVER EXPIRES	Een account met een wachtwoord dat nooit verloopt, verkrijgt toegang tot het netwerk vanaf een externe locatie.
INGRESS FROM COMMUNITY THREAT	Een gebruiker logt in op het netwerk met een IP-adres dat gemarkeerd staat als onbetrouwbaar.
INGRESS FROM DISABLED ACCOUNT	Een gebruiker logt in op het netwerk (of monitored cloud service) met een account dat uitgeschakeld is.
INGRESS FROM DOMAIN ADMIN	Een domain administrator account verkrijgt toegang tot het netwerk vanaf een externe locatie.
INGRESS FROM SERVICE ACCOUNT	Een service account verkrijgt toegang tot het netwerk vanaf een externe locatie.
INGRESS FROM THREAT	Een gebruiker verkrijgt toegang tot het netwerk vanaf een IP-adres dat staat gemarkeerd als onbetrouwbaar.
MALICIOUS HASH ON ASSET	Een kwaadaardige hash is gedetecteerd op een apparaat.
MULTIPLE COUNTRY AUTHENTICATIONS	Een gebruiker verkrijgt vanuit verschillende landen toegang tot het netwerk binnen een onnatuurlijk kort tijdsbestek.
MULTIPLE ORGANIZATION AUTHENTICATIONS	Een gebruiker verkrijgt vanuit meerdere externe locaties toegang tot het netwerk binnen een onnatuurlijk kort tijdsbestek.
NETWORK ACCESS FOR THREAT	Een gebruiker verkrijgt toegang tot een domein of IP-adres dat gemarkeerd staat als onbetrouwbaar.
SPEAR PHISHING URL DETECTED	Een gebruiker bezoekt een domein dat gekoppeld is aan phishing-praktijken.
WIRELESS MULTIPLE COUNTRY AUTHENTICATIONS	Een gebruiker verkrijgt vanaf een mobiel apparaat vanuit verschillende landen toegang tot het netwerk binnen een onnatuurlijk kort tijdsbestek.
WIRELESS MULTIPLE ORGANIZATION AUTHENTICATIONS	Een gebruiker logt met een wireless device in op het netwerk vanuit verschillende organisaties. Dit binnen een onnatuurlijk kort tijdsbestek.

FASE 2: EXPLORE INTERNAL NETWORK	
Pre-built detectie:	Notificatie wanneer:
BRUTE FORCE – ASSET	Veel verschillende accounts proberen in te loggen op hetzelfde apparaat.
BRUTE FORCE - DOMAIN ACCOUNT	Een domain account probeert opvallend vaak en onsuccesvol in te loggen op een apparaat.
BRUTE FORCE - LOCAL ACCOUNT	Een local account probeert opvallend vaak en onsuccesvol in te loggen op een apparaat.
HONEYPOT ACCESS	Er is geprobeerd verbinding te maken met een netwerkhoneypot.
HONEY USER AUTHENTICATION	Er is geprobeerd in te loggen met een honey user account.
LDAP ADMIN ADDED	Een gebruiker is toegevoegd aan de LDAP group en heeft adminrechten verkregen.

FASE 3: LATERAL MOVEMENT	
Pre-built detectie:	Notificatie wanneer:
APPLICATION AUTHENTICATION - NEW SOURCE	Een (permitted) gebruiker logt in op een applicatie vanaf een nieuw bronapparaat.
APPLICATION AUTHENTICATION - NEW USER	Een nieuwe gebruiker logt in op een applicatie.
HONEY CREDENTIAL AUTHENTICATION ATTEMPT – LOCAL	Een “dummy credential” die geïnjecteerd is door de Insight Agent is gebruikt om in te loggen.
HONEY CREDENTIAL AUTHENTICATION ATTEMPT – REMOTE	Een “dummy credential” die geïnjecteerd is door de Insight Agent is gebruikt om in te loggen.
KERBEROS PRIVILEGE ELEVATION EXPLOIT	Een gebruiker misbruikt de Windows Kerberos-Kwetsbaarheid CVE-2014-6324 om toegangsrechten te verhogen.

LATERAL MOVEMENT - ADMINISTRATOR IMPERSONATION	Een gebruiker logt in op een admin account.
LATERAL MOVEMENT - DOMAIN CREDENTIALS	Een domain account probeert toegang te krijgen tot meerdere nieuwe apparaten in een kort tijdsbestek.
LATERAL MOVEMENT - LOCAL CREDENTIALS	Een local account probeert toegang te krijgen tot meerdere nieuwe apparaten in een kort tijdsbestek.
LATERAL MOVEMENT - SERVICE ACCOUNT	Een service account logt in vanuit een nieuw bronapparaat.
LATERAL MOVEMENT - WATCHED USER IMPERSONATION	Een gebruiker logt in op een "watched" account.
NEW ASSETS AUTHENTICATED	Een gebruiker verkrijgt toegang tot opvallend veel nieuwe apparaten in een kort tijdsbestek.
PROTOCOL POISONING DETECTED	Een 'vergiftiging' van een netwerkprotocol wordt gedetecteerd.
ZONE POLICY VIOLATION	Een gebruiker schendt de zone policy (geconfigureerd in InsightIDR).
REMOTE FILE EXECUTION DETECTED	Er is remote file execution gedetecteerd.

FASE 4: MISSION TARGET	
Pre-built detectie:	Notificatie wanneer:
HONEY FILE ACCESSED	Een honey file wordt geopend op een shared file server.
RESTRICTED ASSET AUTHENTICATION - NEW SOURCE	Een (permitted) gebruiker logt in op een 'restricted' apparaat vanuit een nieuw bronapparaat.
RESTRICTED ASSET AUTHENTICATION - NEW USER	Een nieuwe gebruiker logt in op een 'restricted' apparaat.