Version: 2019-07-02 - a

Vad innebär Security Analytics?

Korta svaret:

Ökad effektivitet och minskad risk för Dig och Ditt företag!

Det något längre svaret:

Flera saker, men framförallt är Security Analytics**:**

1. En möjlighet till radikalt förbättrad effektivitet i säkerhetsarbetet genom att minska ledtider och underlätta för den personal som ansvarar för jobbet.
2. En metod och ett verktyg för att väsentligt underlätta framtagandet av den information som behövs genom att kombinera Business Intelligence med säkerhetsdata (i vid bemärkelse) i sitt sammanhang.
3. Analyser och rapporter som underlättar förståelse, anpassade till olika beslutsfattare såsom VD/ledningsgrupp, säkerhetsansvariga och systemägare.
4. Rapporter anpassade för övrig/utförande verksamhet.

Tillvägagångssättet för att förbättra hanteringen av sårbarheter och avvikelser är kortfattat:

- Ta reda på och dokumentera det verkliga nuläget.
- Tillse att ledningen får info om, förstår läget samt efterfrågar fortsatt uppföljning.
- Inventera befintlig hantering/process, normalt saknas den eller behöver förbättras.
- Skapa eller förbättra verktyg som underlättar rapportering till ledningen samt, inte minst, anpassade rapporter till de tekniker som ska göra jobbet.
    - Rådata + BI-verktyg = anpassade rapporter till respektive målgrupps behov -> förenklat mottagande av informationen och effektivare hantering…!

Security Analytics kan användas till inte bara avvikelser utan även till mycket annat som t.ex. IAM/behörighetshantering när man behöver inventera och styra upp behörigheter, kontinuerligt och automatiskt säkerställa segregation of duty, matcha avvikelser mot loggar.
Det går också att direkt spara pengar genom att underlätta hantering av programvarulicenser, till exempel ringa in användare som *inte* loggats med att använda programmet.

Det (mycket) längre svaret:

Skälet till att denna text framförallt handlar om effektiv hantering av sårbarheter och avvikelser beror på att många företag släpar efter med att stänga/patcha avvikelser, vilket kan kosta pengar…

En enda sårbarhet/avvikelse ledde t.ex. till kostnader för Maersk på mer än 2 miljarder kronor. (källa: https://www.youtube.com/watch?v=Tqe3K3D7TnI&feature=youtu.be, tid: 2:25 – 7:36)

Då Dataskyddsförordningen/GDPR började tillämpas 25 maj 2018 tillkom risken att drabbas av kostnader relaterade till GDPR. Ekonomiskt tillkom därmed ytterligare incitament genom att även dataläckage kan generera avsevärda kostnader.

Ganska många svenska och nordiska företag har en flora av tusentals för att inte säga tiotusentals olika datorer, operativsystem, programvaror, applikationer etc.

Normalt använder alla företag ett antivirusverktyg som kontinuerligt uppdaterar en central databas med larm om att dator x har smittats och behöver åtgärdas.

Många kör även sårbarhetsscanningar med verktyg som letar efter kända säkerhetshot.

Man använder också verktyg som scannar utrustning och applikationer för att hitta avvikelser från hur det borde vara enligt respektive godkänd standard för säker konfiguration (IT Security Baselines).

Gemensamt för dessa olika verktyg är att de genererar listor, normalt långa med hundra- till tiotusentals rader beroende på storleken på företagets it-miljö. Varje rad i en lista innehåller som ett minimum alltid ip-adress och en beskrivning på sårbarheten.

Exempel på en rapporterad sårbarhet:

IP-adress	CVE ID	Allvarlighetsgrad:	Beskrivning
192.168.5.16	CVE-2018-8347	7.8 HIGH	An elevation of privilege vulnerability exists in Microsoft Windows when the Windows kernel fails to properly handle parsing of certain symbolic links, aka "Windows Kernel Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows 10 Servers.

Scannern ger oss data om vad det är för sårbarhet. Däremot kan den **inte** ge oss den övriga tillkommande information som behövs för att åtgärda avvikelsen.

Ytterligare arbete med insamling av fakta behövs för att kunna avgöra prioritering, hur, när och vem som ska åtgärda avvikelsen. Detta är både tidsödande och omfattande, och stjäl därmed effektivitet från säkerhetsarbetet.

Ett exempel på vilka uppgifter som brukar vara nödvändiga.

(Mycket jobb är det…)

Uppgifter som scannern EJ känner till MEN som behöver utredas för att kunna utföra arbetet med att prioritera och åtgärda avvikelsen samt även för rapportering efter utförd åtgärd		
Org Enhet 1	ACME Kit	Sammanställning av koncernsäkerhetsstatus
Org Enhet 2	Företagskunder	Sammanställning av bolagets säkerhetsstatus
Kostnadsställe	120056	Vem bär kostnaden för arbetet?
Application Owner	Carl Kulander	Problemägare. Beslut om tillfälle för åtgärd.
Application	Prosit	Vad är det för system som körs på maskinen?
Customer Facing	Ja	Vad har applikationen/utrustningen för exponering?
Internet Facing	Ja	Vad har applikationen/utrustningen för exponering?
GDPR	Ja	Hur är skadekostnaden med avseende på GDPR?
Verksamhetskritisk	Ja	Hur är skadekostnaden med avseende på verksamheten?
24/7/365	Ja	Hur är skadekostnaden med avseende på driftstopp?
Fall Back	Nej	Finns det lastväxlande eller backup-maskiner? I så fall vilka (för patchning även av dem)
Application Provider	Anna Larsson	Intressent - behöver känna till patchen så den inte medför oönskade driftstörningar
UtrustningID	45326582	Var finns utrustningen?
Inventarienummer	i16-27401	Hur gammal är utrustningen? Är det bättre att ersätta den?

Tillverkare	Microsoft	Vem är tillverkaren/leverantören?
Produktgrupp	Operativsystem	Vad är det för något? (operativsystem/databas/hårdvara/etc)
Produkt	Windows Server	Vad är det för produkt?
Version	12.8	Vilken version? (Speciellt viktigt/användbart att veta i de fall en Security Advisory från en leverantör anger att version x måste uppdateras)

Den person eller den grupp som är ansvarig för att åtgärda avvikelsen kommer att behöva ta reda på svaren på dessa frågor innan de kan åtgärda och rapportera sårbarheten. (Tänk dig in i arbetsinsatsen för de personer eller grupper som har till uppgift att hantera listorna, dvs resultatet från de olika scanningarna…)

Glöm inte att detta är ETT (1) enda exempel på en (1) ip-adress.

Normalt handlar det om

- Mer än en enstaka avvikelse.
    - Beroende på företagets IT-miljö, 100-tals – 10 000 tals avvikelser
- Olika typer av avvikelser
    - Sårbarheter
    - Avvikelser från korrekt standard/inställning
    - Security Advisories
    - Godkända undantag t.ex. säkerhetsrisker som accepteras tills vidare (men som scannern rapporterar vid varje scanning…)

För att hantera avvikelser effektivt behöver man alltså sammanställa dessa uppgifter i en lista, dela in dem i grupper, prioritera och planera åtgärder.

Inte minst leder detta till att den personal som ska åtgärda behöver lägga mycket tid och möda på att ta reda på fakta som de behöver för att kunna göra sitt jobb. Samt, inte minst, stämma av och förankra åtgärder med olika intressenter som t. ex. applikationsägare (ITIL: application owners).

Då man oftast inte kan koppla en applikation till programvaror, utrustningar etc som används så saknar applikationsägarna ofta eller nästan alltid en helhetsbild av vilka avvikelser som applikationen är behäftad med.

Man kan nog också med mycket gott samvete hävda att företagsledningen normalt också saknar en helhetsbild av läget samt därmed vilka affärsrisker som företaget är utsatt för.

En enda möjlighet för en insider kostade Punjab Bank 1,8 miljarder dollar.

Källa: https://www.darkreading.com/the-6-worst-insider-attacks-of-2018---so-far/d/d-id/1332183?image_number=3

Det är kanske inte så konstigt att många företag släpar efter med att åtgärda avvikelser och sårbarheter men det finns omfattande ekonomiska skäl att visualisera riskerna så man kan ställa dem mot konsekvenserna och fatta väl underbyggda beslut.

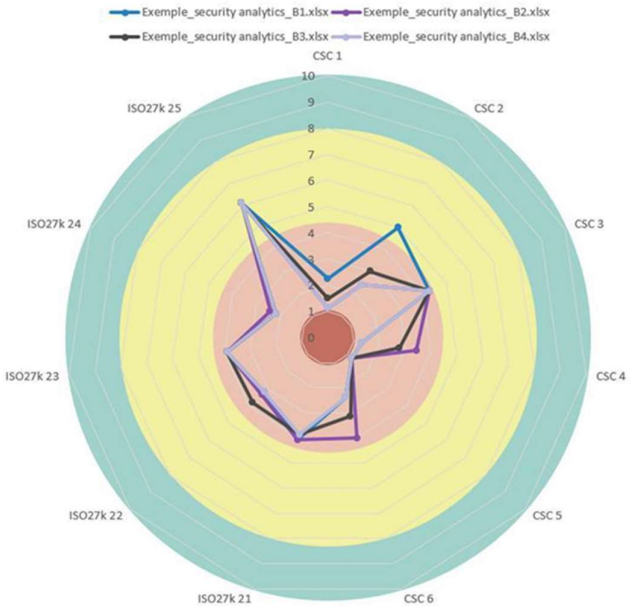
Hur åtgärdar man detta? Hur förebygger vi problem?

- Tillse att de personer/de grupper som arbetar med avvikelser arbetar på samma sätt.
    - Förbättra eller inför ett gemensamt effektivt och standardiserat arbetssätt.
- Använd verktyg/BI för att samla data, analysera och generera anpassade ”rapporter” som möjliggör och underlättar arbetet med att
    - Samla in rådata från olika källor
    - Analysera/Förstå vad data säger
    - Prioritera arbetet
    - Planera arbetet
    - Utföra arbetet med att stänga avvikelser
    - Rapportera utfört arbete
- Följ upp status kontinuerligt.
    - Hur ligger vi till just nu?
    - Hur låg vi till ”igår”?
- Informera företagsledningen.
    - Tillse att denna information visar status på ett effektivt och enkelt sätt.
        - Underlättar radikalt förståelse och därmed möjlighet att få beslut.

Exempel på ”verktyg”
Företagsledningen – endast övergripande rapport

Status Hög risk avvikelser - Företag Acme Kit		
	Denna månad	Föregående månad
Totalt antal hög risk avvikelser	2686	2832
Riskkostnad	450 – 880 Mkr	440 – 1090 Mkr
Genomsnittlig ålder på avvikelser	825 dagar	900 dagar

Inte bara text, även grafik, t.ex. polär/spindeldiagram eller andra typer av diagram som stapel etc



Exempel på ”verktyg”
Enhetschefer – övergripande info avseende deras enhet samt möjlighet att jämföra sig med övriga enheter

	Stora företag	Små och medel	Privatkunder	Offentlig	IT-drift
Totalt antal avvikelser	xxxx	xxxx	xxxx	xxxx	xxxx
Antal hög risk avvikelser	492 (503)	510 (585)	535 (592)	562 (562)	587 (590)
Genomsnittlig ålder på avvikelser	899 dagar	1209 dagar	336 dagar	954 dagar	727 dagar
Applikationer – topp tre - avvikelser	Smurf, Bok, CRM	CRM, Guld, Res	Bok, Privat, Smurf	Inv, px, Res	Nessus, AD, SSO

Exempel på ”verktyg”
Utförarrapport – Till varje grupp, anpassad info med den info de behöver. Detta som en del i processen, det verktyg de behöver för att kunna jobba effektivare och slippa lägga mycket tid på att ta reda på exakt vad som behöver göras.

Ansvar	Ip-adress	Avvikelse	Åtgärd	Tid	Övrigt
Unixgruppen	192.168.1.12 192.168.4.25 192.168.4.26 192.169.4.40 192.163.4.33 etc	CVE-xxxx-xx	Installera uppdatering enligt leverantörens rekommendation xxxx	2018-12-14 03:00 – 2018-12-14 07:00	Kräver omstart
Windowsgruppen	192.168.1.10 192.168.2.25 192.168.2.26 192.169.3.40 192.163.2.33 etc	CVE-xxxx-xx	Ominstallera xyz	ok att göra när som helst.	Kräver ej omstart.
Skrivargruppen	192.232.1.20	Skrivare x sönder	Ta ur hårddisk ur skrivaren. Skicka skrivaren på service hos leverantör Lexmark. Adress: xxxx.		Placerad, hus x, vån 3, rum 12
Databasgruppen	192.168.14.20	CVE-xxxx-xx	Omstart av xxx	2018-12-12 02:00 – 2018-12-12 04:00	

Har du frågor/Vill du veta mer?

Välkommen att kontakta mig!

Per-Erik Eriksson