UNISTAR PRO

Kibernetski varnostno operativni center kot storitev SOCaaS

Marko Zavadlav, Vodja oddelka PRO.Astec Security Team

Kdo smo

- Top 3 sistemski integrator v Sloveniji
- 27 let uspešnega poslovanja
- Preko 100 zadovoljnih odjemalcev v Sloveniji, 225 aktivnih vzdrževalnih pogodb, ki upravljajo s preko 40k končnimi uporabniki
- Preko 500 uspešno zaključenih projektov v Sloveniji in tujini
- 70 inženirjev s skupno preko 300 certifikati s področja informacijske tehnologije in projektnega vodenja
- V lasti Alterna d.d.
- V skupini so 4 organizacije, 130 zaposlenih in preko 35 mio EUR letnih prihodkov
- Certificirani po standardih ISO/IEC 9001 and ISO/IEC 27001

Unistar profesionalne storitve

PRO.cloud

PRO.poslovna analitika

PRO.podatkovni center

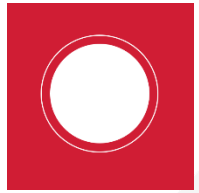
PRO.poslovni procesi

PRO.upravljanje IT sredstev

PRO.varnost

PRO.virtualizacija

PRO.komunikacije



PRO.napredno komuniciranje

PRO.EVT

PRO.varnost

IT varnost in skladnost

UNISTAR PRO

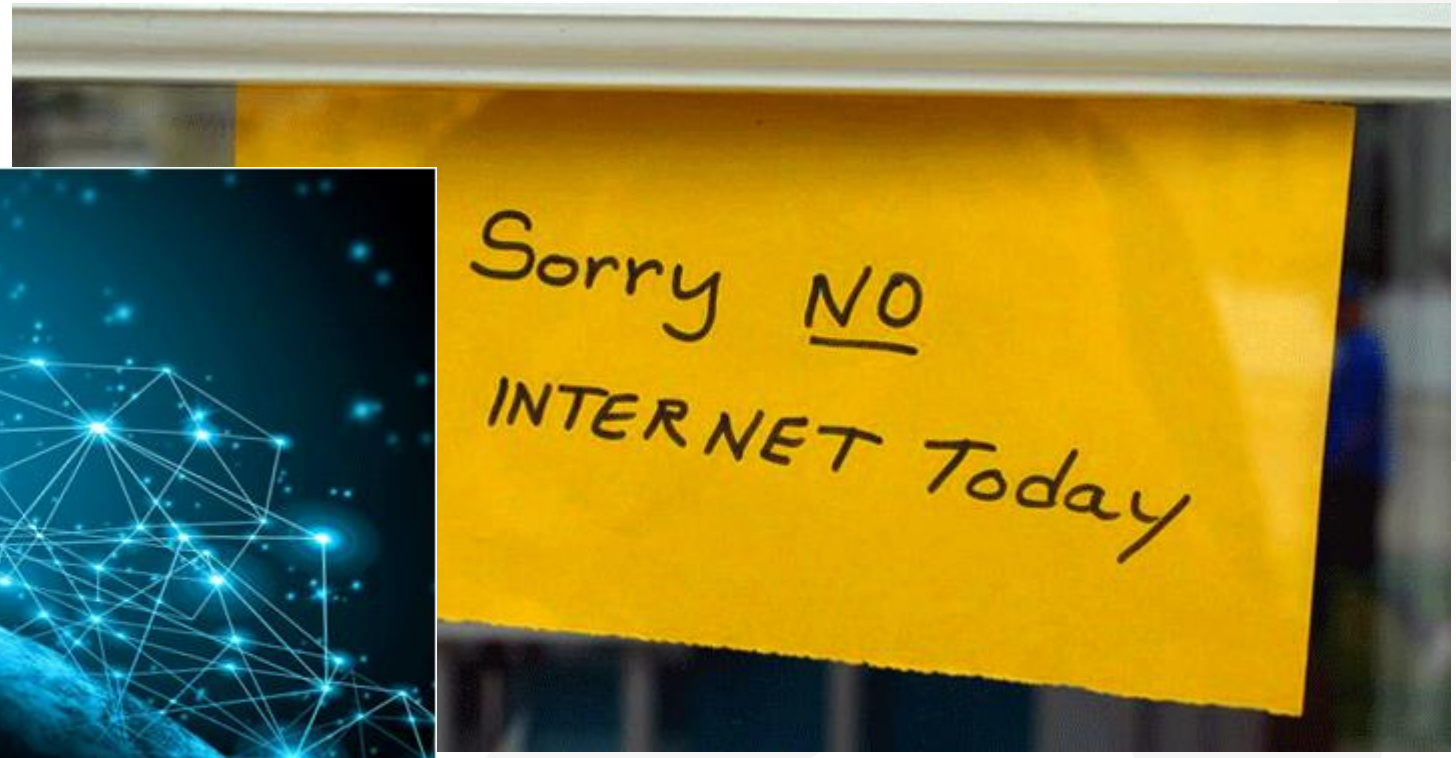
Kibernetski napadi - realnost

Hackers Steal Millions From European ATMs Using Malware That Spit Out Cash

Someone is Using Mirai Botnet to Shut Down Internet for an Entire Country

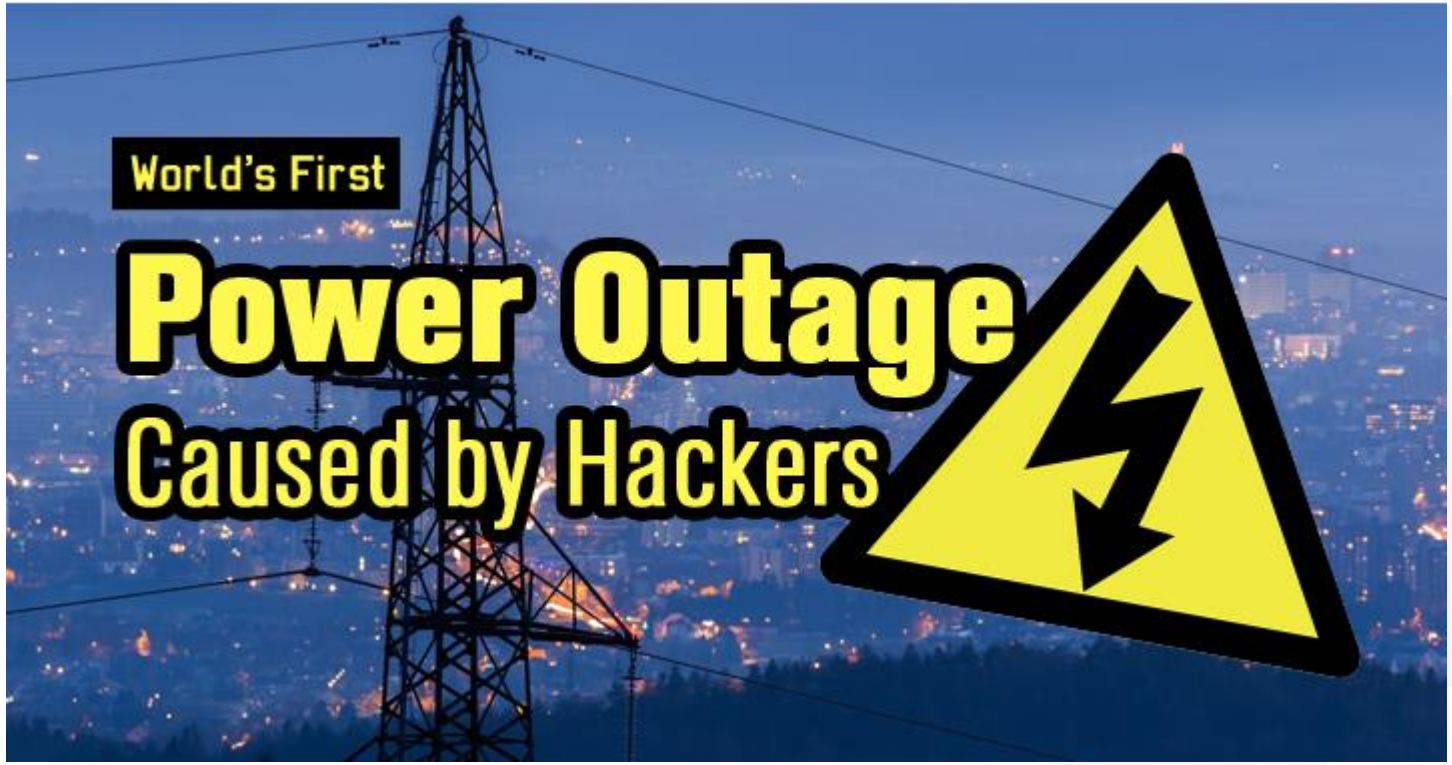
Kibernetski napadi - realnost

An Army of Million Hacked IoT Devices Almost Broke the Internet Today



Kibernetski napadi - realnost

Hackers Cause World's First Power Outage with Malware

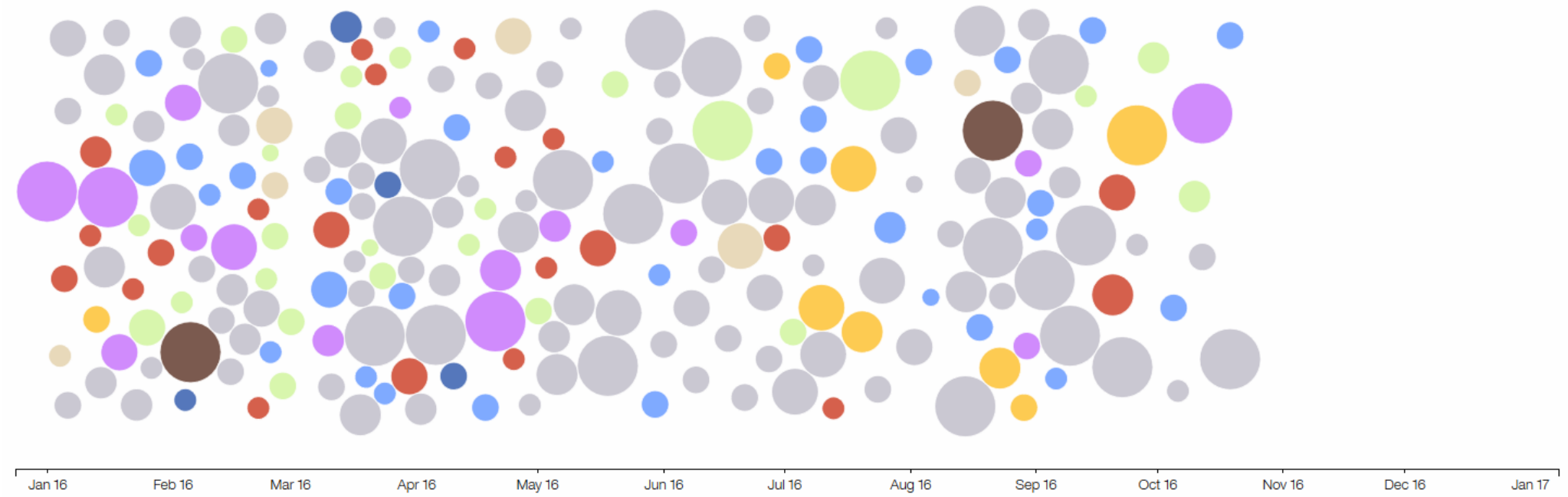


Kibernetski napadi - realnost

Even A Single Computer Can Take Down Big Servers Using BlackNurse Attack

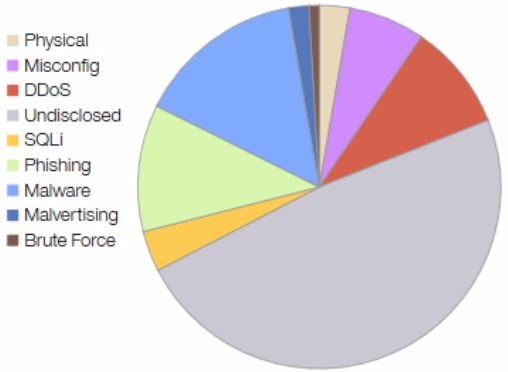
Kibernetski napadi - realnost

Kibernetski napadi



Attack Types (reset)

Click to view incidents for a specific attack type.



Industries (reset)

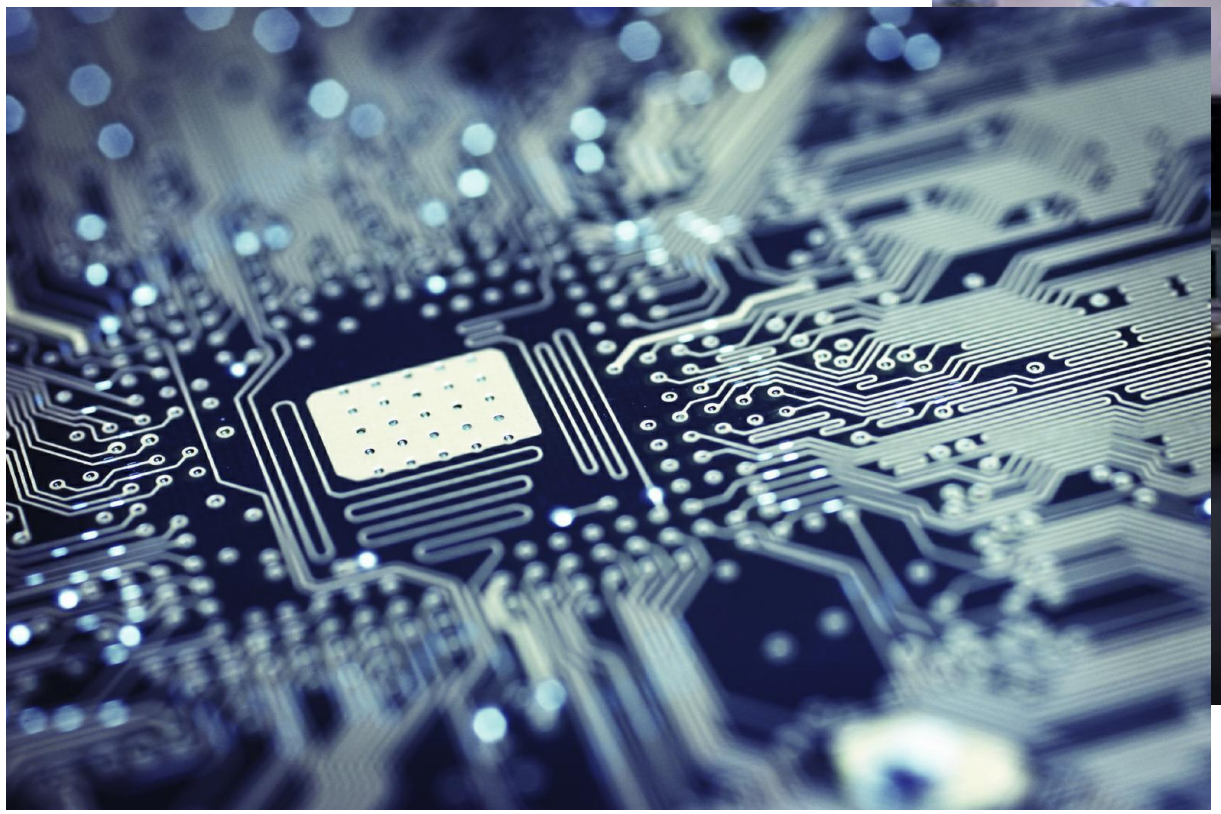
Click below to view incidents from a specific industry.

Target Geography (reset)

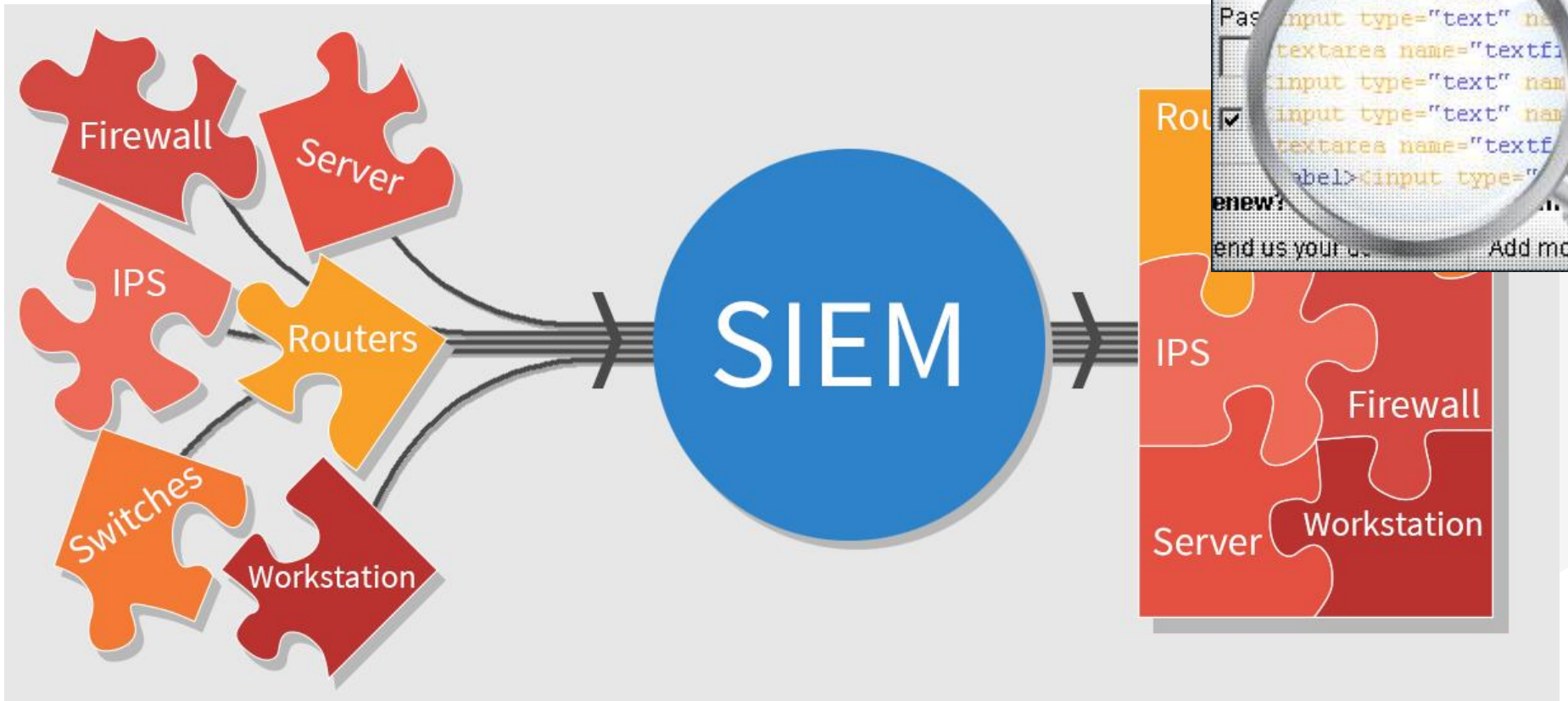
Size of flag indicates higher volume. Click to view incidents for that geography.

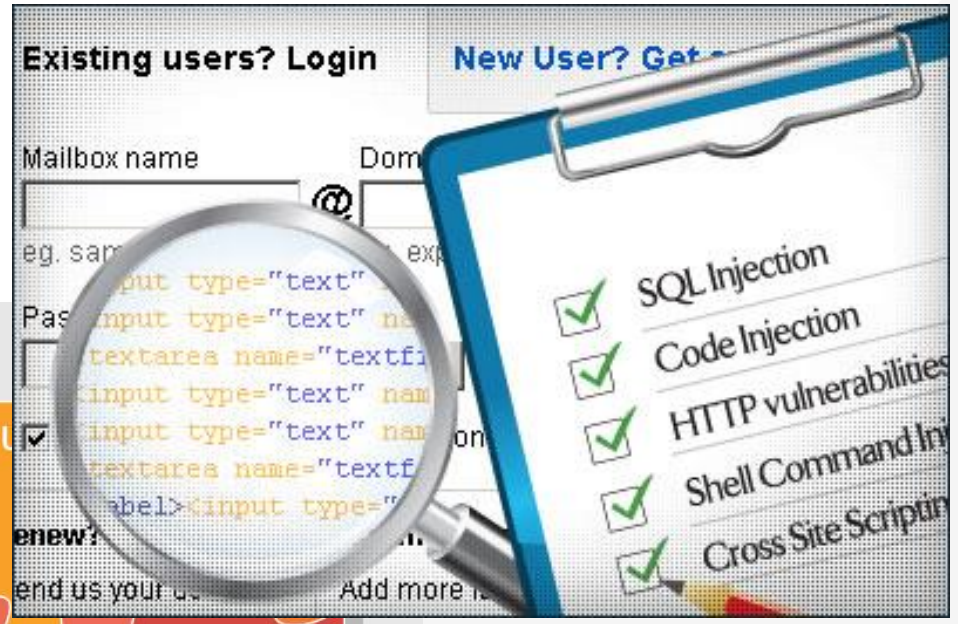
Vir: IBM XForce

Kibernetska varnost – tehnika?

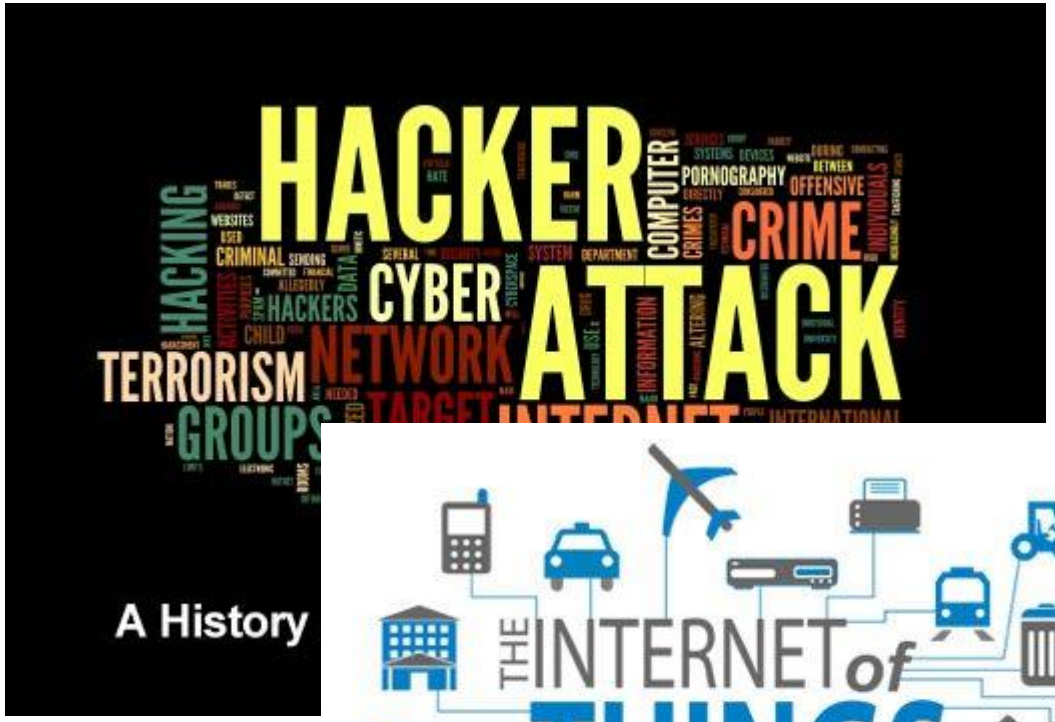


Razvoj kibernetske varnosti





Razvoj kibernetske varnosti

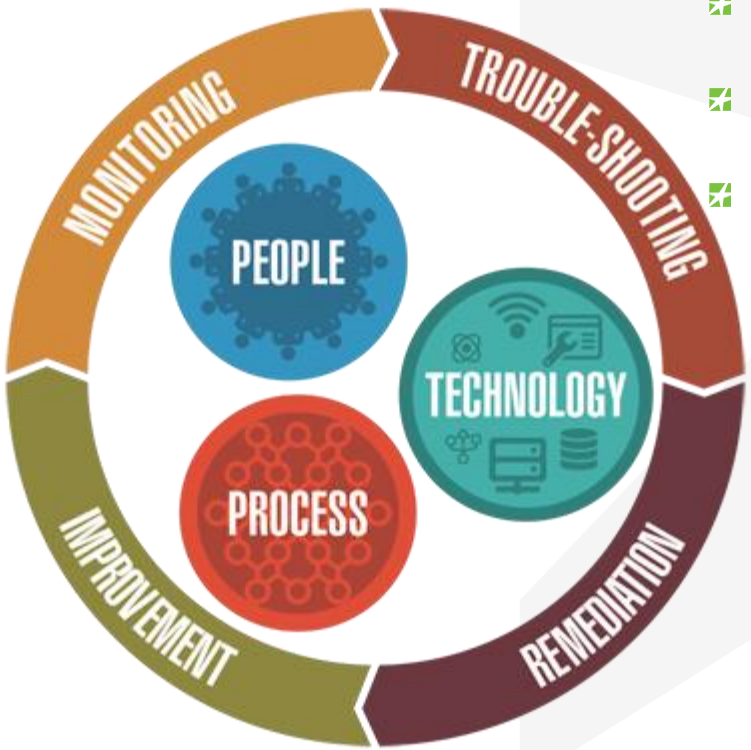


Najprej pa…

- Analiza poslovnih učinkov
- Analiza tveganja
- Analiza razkoraka

SOC procesi

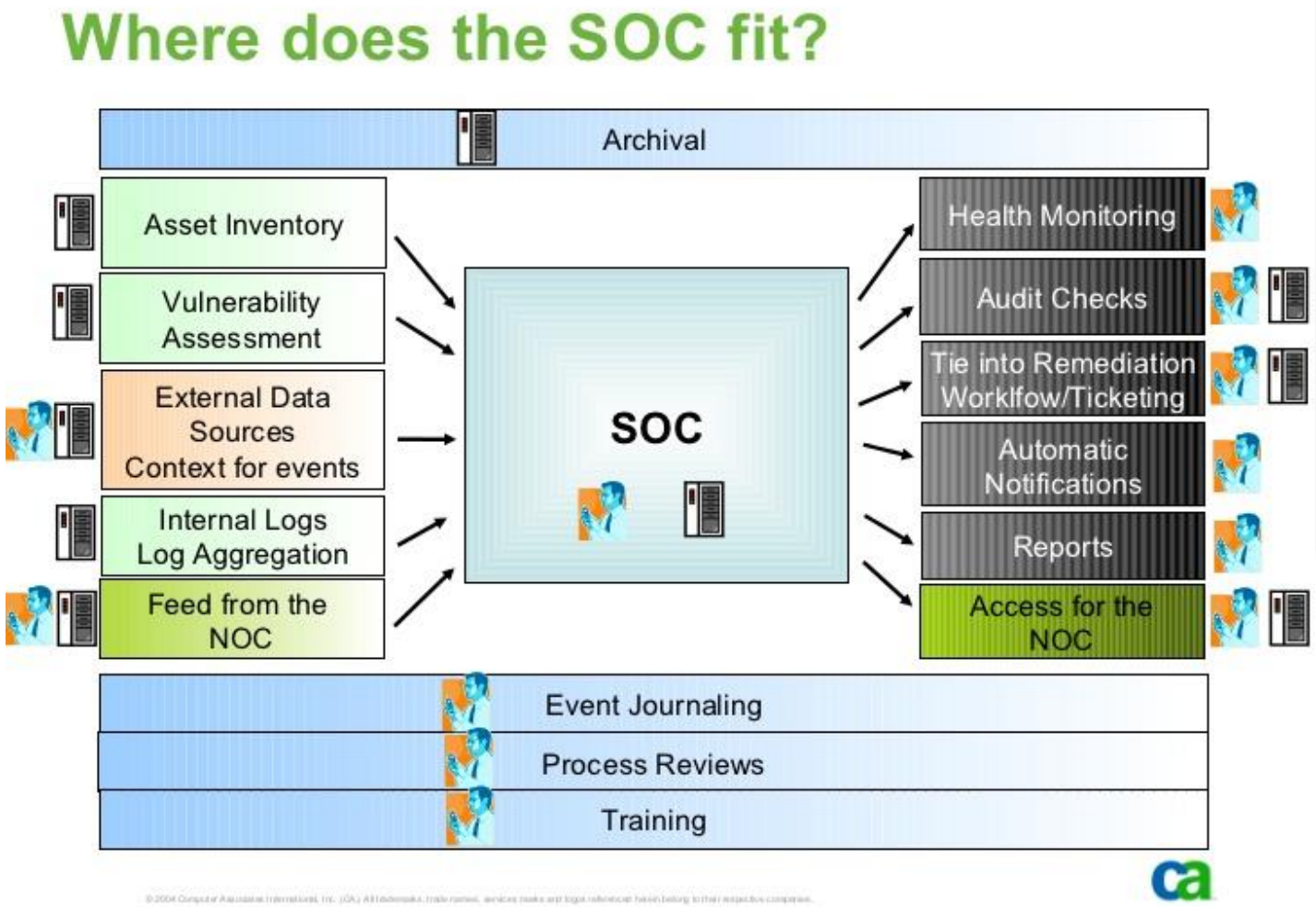
- Priprava in načrtovanje
- Periodično preverjanje ranljivosti
- Preverjanje pred produkcijo
- Monitoring
- Odzivi na zaznane dogodke
- Triaža
- Odzivi na incidente
- Omejevanje
- Poročanje



- Forenzika
- Odpravljanje posledic
- Vzpostavitev normalnega delovanja
- Učenje
- Jačanje varnosti
- Vaje

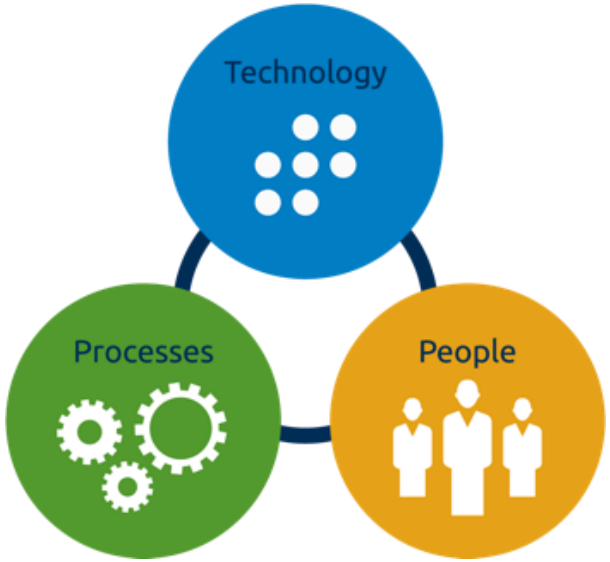
SOC Analiza

- Kaj ščitimo
- Kje smo ranljivi
- Kje bodo naši viri podatkov
- Katere vloge potrebujemo
- Katere kompetence potrebujemo
- Katera pooblastila potrebujemo
- Kako umestimo SOC
- Delovni tokovi in ticketing
- Integracija z obstoječimi sistemi (npr. NOC)



Priprava na SOC

- Pravilni procesi
- Pravilne kompetence
- Učinkovita tehnologija



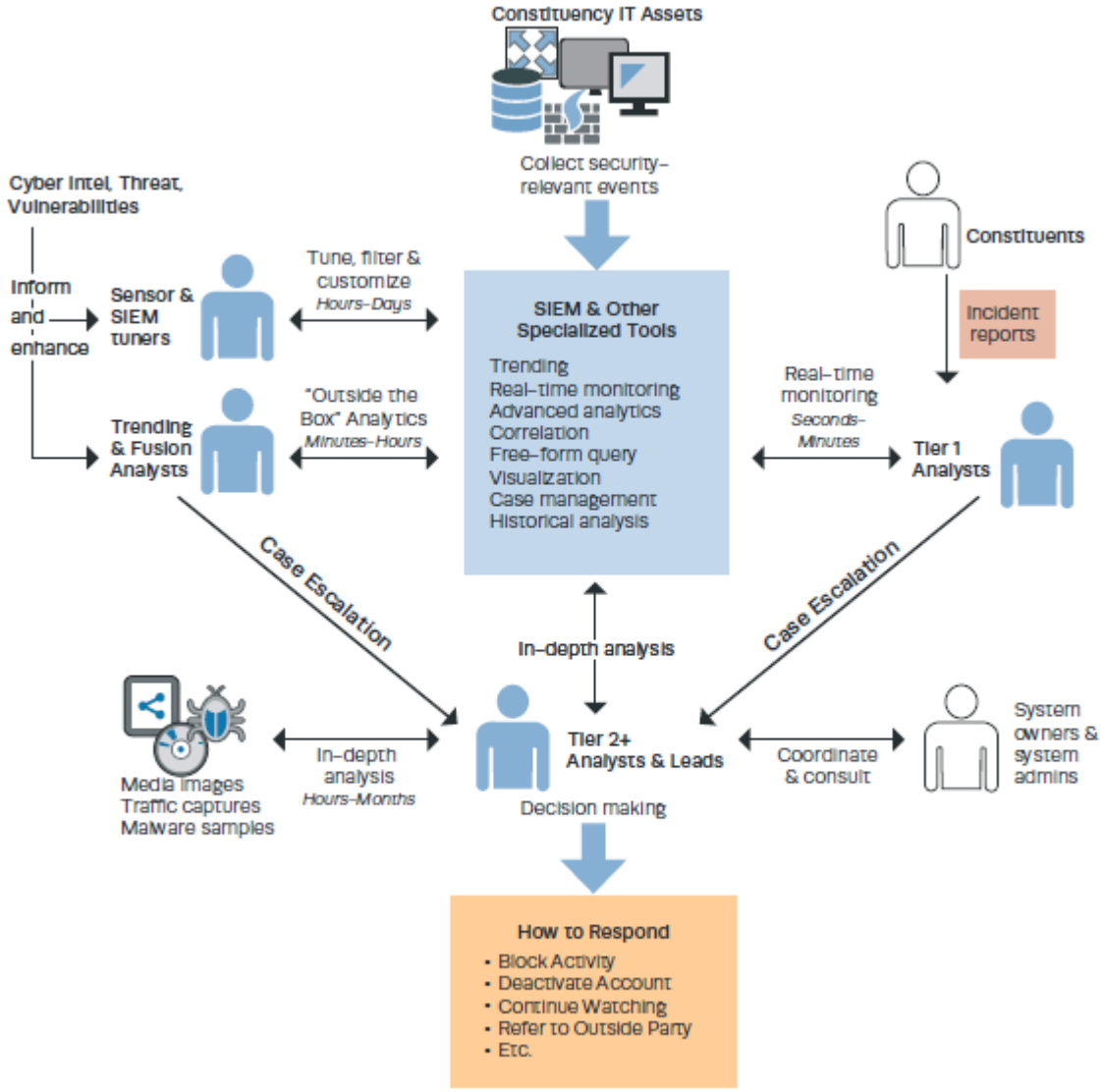
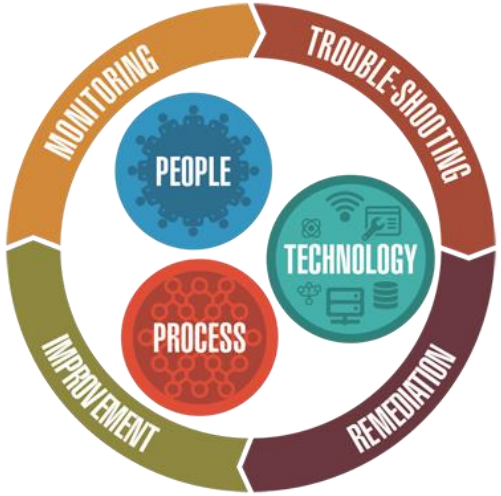


Figure 1. SOC Roles and Incident Escalation

Izbira pravih komponent SOC

- Ljudje (število, kompetence, načrt izobraževanj,…)
- Procesi (priprava, delovanje, izboljševanje)
- Tehnologija (povezave, kapacitete, avtomatizacija)



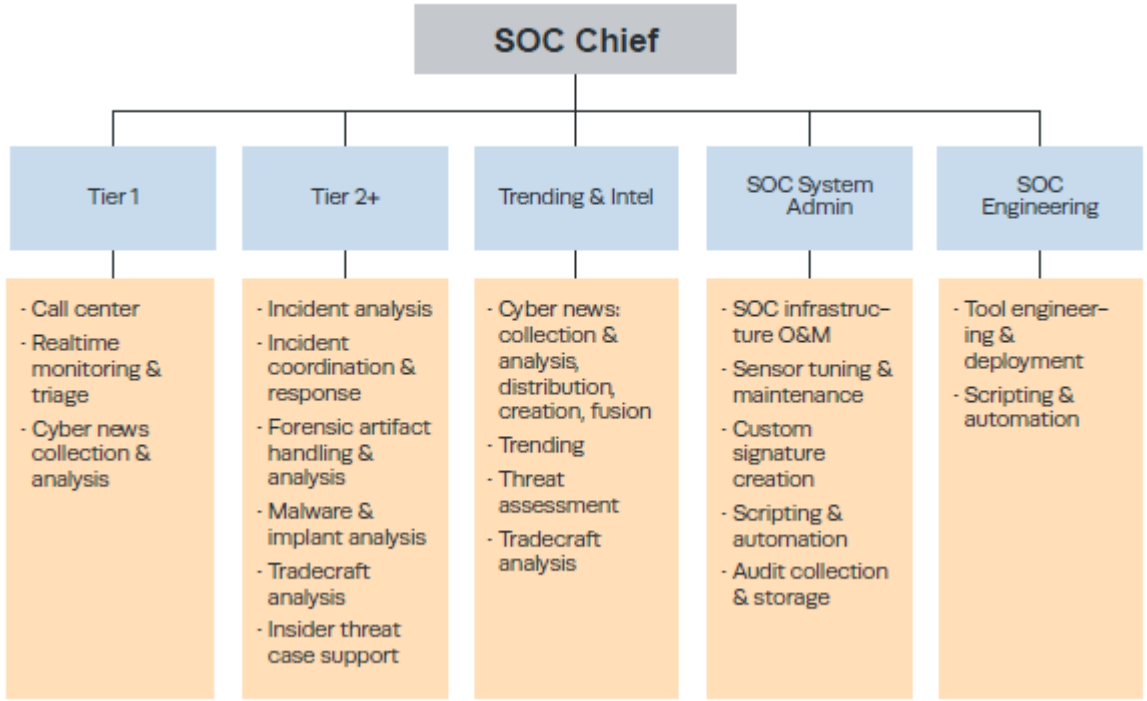
Recept za SOC iz desetih sestavin

1. sestavina – združitev kibernetske obrambe na enem mestu

- Sinhronizacija opravil
- Odkrivanje in odziv na incidente je učinkovit, natančen, relevanten
- Učinkovita izkoriščenost virov
- Podatki o incidentih se pretakajo nazaj za uspešen sistem nenehnega izboljševanja
- Zagotavljanje vidnosti (visibility) vodji odzivnega centra

Rezultat 1. sestavine

- Spremljanje in triaža (Tier 1) na enem mestu
- Analiza incidentov, usklajevanje in odziv (Tier 2 in višje)
- Zbiranje in analiza podatkov (Cyber intel)
- Nastavitve senzorjev in upravljanje SOC infrastrukture
- Uvedba SOC orodij iz enega mesta

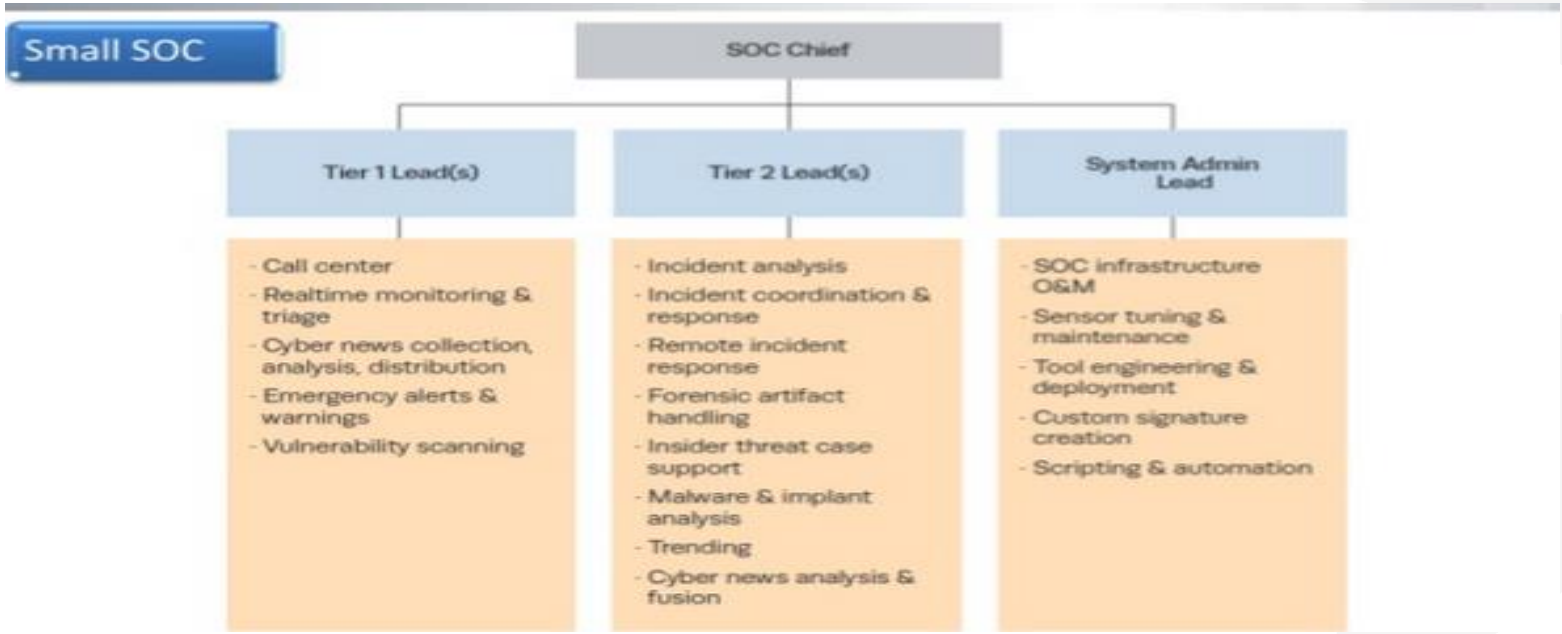


Vir: Mitre, 2014

2. sestavina – pravo razmerje med velikostjo in agilnostjo

Tri zahteve:

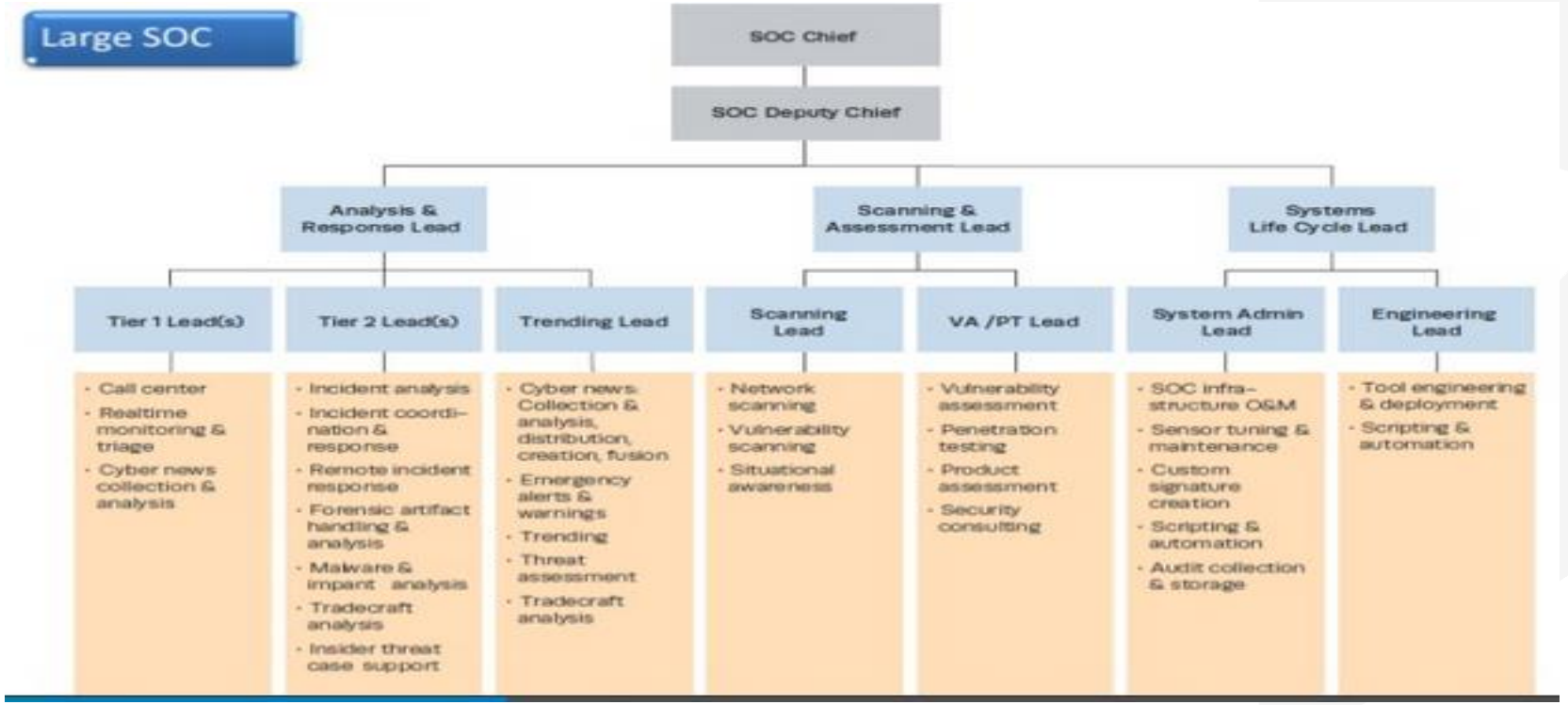
- Potreba po močno povezani ekipi strokovnjakov
- Potreba po ohranjanju logične, fizične ali organizacijske bližine sredstvom, ki se spremljajo
- Finančne in organizacijske omejitve deležnikov (strank)



Rezultati 2. sestavine

Trije odgovori:

- Kateri SOC organizacijski model je pravi?
- Umestitev SOC funkcij v organizacijsko shemo in poveljniška struktura
- Fizična umestitev članov SOC, in uskladitev njihovih aktivnosti



3. sestavina – Ustrezna pooblastila

- Pisna pooblastila
- Podpora vodstva
- Politike

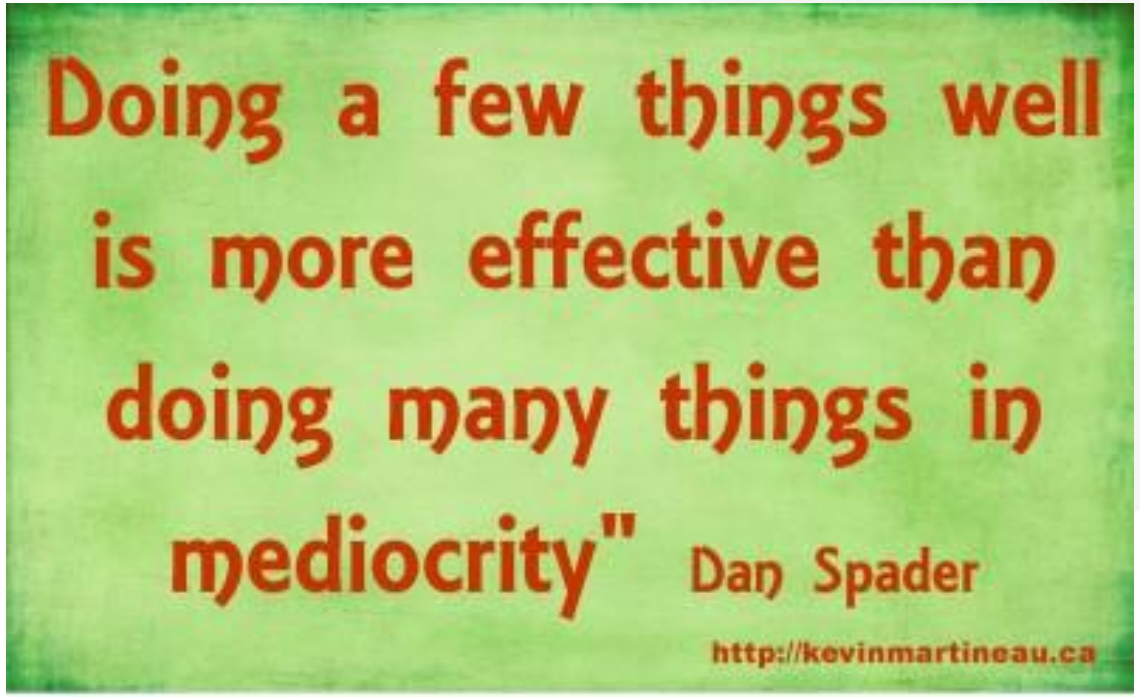
Rezultati 3. sestavine

- SOC, ki se lahko hitro odzove
- SOC, ki ima ustrezne vire za svoje delovanje
- SOC, ki ima jasna pooblastila, naloge in pooblastila za izvedbo procesov

4. sestavina – Delaj malo, a dobro

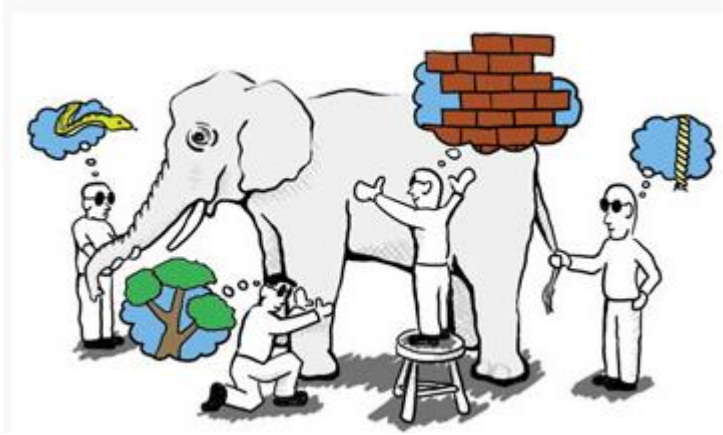
Osnovne funkcije SOC

- Sprejem prijave incidentov s strani uporabnikov
- Pomoč pri odzivu na incidente
- Poročanje o zaznanih incidentih



Rezultati 4. sestavine

- Ustrezno upravljanje pričakovanj uporabnikov,
- Povečanje zaupanja uporabnikov s profesionalno in skrbno obravnavo varnostnih incidentov
- Izogibanje preobremenitvi omejenih virov SOC na račun kakovosti izvajanja osnovnih aktivnosti
- Vpeljava dodatnih aktivnosti in nalog le, če viri, zrelost in fokus organizacije to dovoljujejo



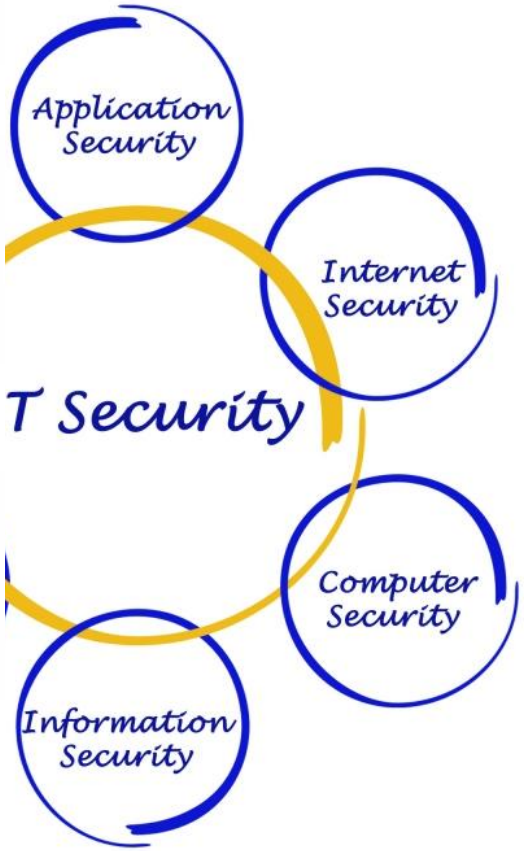
5. sestavina – Prednost naj ima kakovost zaposlenih

- Mnogo bolj pomembna je kakovost analitikov, kot njihovo število
- Analiza ne bo in ne more biti nikoli uokvirjen ponovljiv postopek, ki se ga da natančno opisati

Rezultati 5. sestavine

- Ekipa, ki ve, kaj dela
- Ekipa, ki ima željo in strast

6. sestavina – Maksimirajmo učinkovitost tehnologije

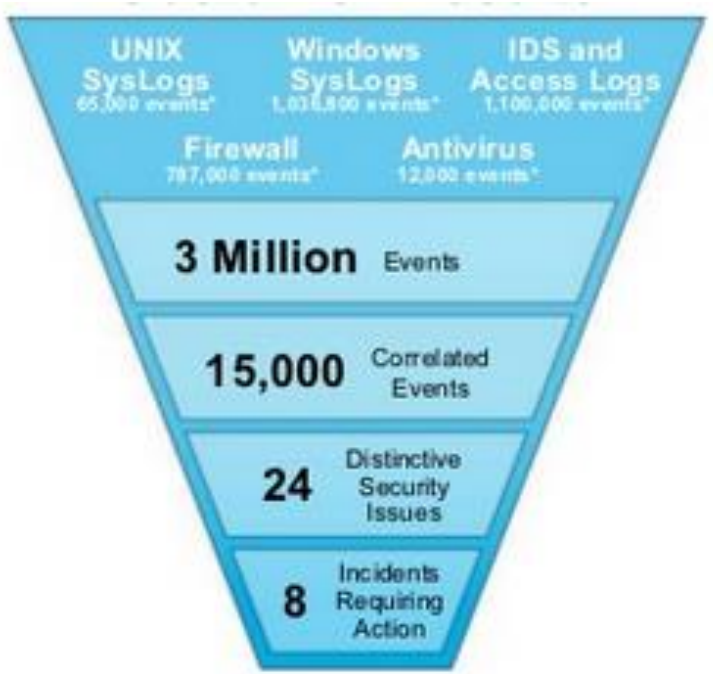


Rezultati 6. sestavine

- Stroškovno učinkovit sistem
- Sistem, ki se da upravljati
- Sistem, ki pozna svoje prednosti in omejitve

7. sestavina – Pazljivo izberi vire in količino zbiranih podatkov

- Kam postavimo senzorje
- Kateri sistemi nam lahko posredujejo relevantne podatke



Rezultati 7. sestavine

- Optimiziran sistem
- Manj overheada informacij
- Hitrejša izvedba analitike nad podatki in s tem hitrejši odziv
- Ni podvajanja informacij

8. sestavina – Zavaruj SOC

- SOC je ranljiv
- SOC lahko natančno izvršuje svoje naloge, ker nasprotnik ne ve, kje se nahaja in kakšne zmožnosti spremljanja in odzivanja ima.

Rezultati 8. sestavine

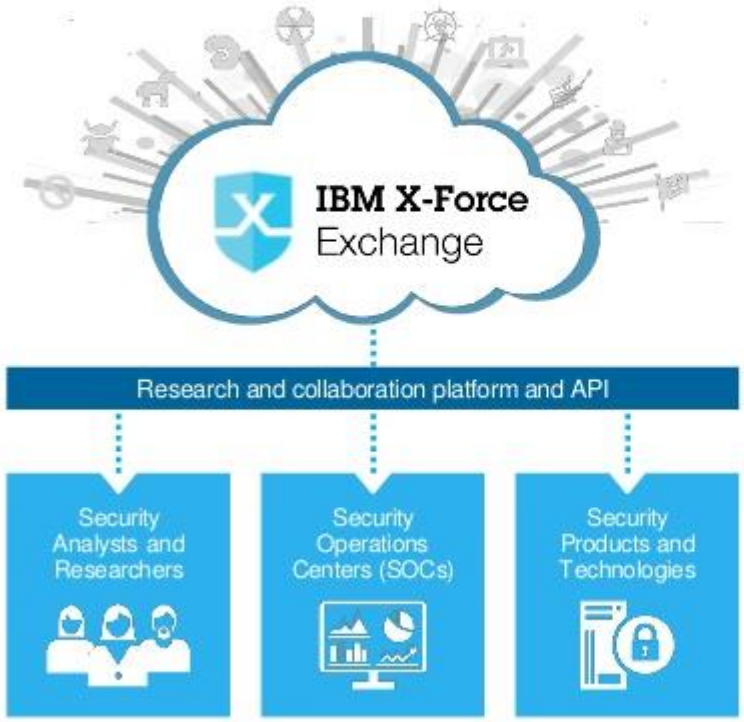
- Ločen avtonomen sistem
- Ni viden navzven
- Ni član poslovnih domen

9. sestavina – Izmenjuj podatke

IBM Security

IBM

Introducing IBM X-Force Exchange



A new platform to consume, share, and act on threat intelligence

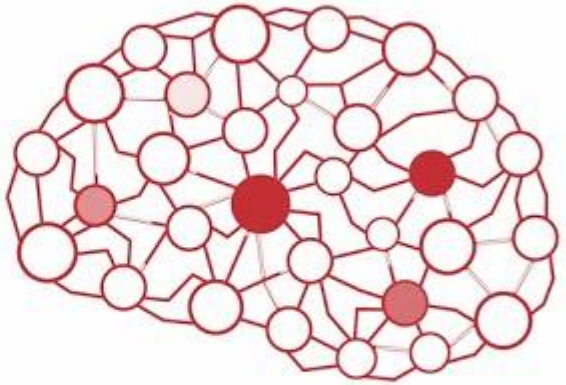
IBM X-Force Exchange is:

OPEN
a robust platform with access to a wealth of threat intelligence data

ACTIONABLE
an integrated solution to help quickly stop threats

SOCIAL
a collaborative platform for sharing threat intelligence

Backed by the reputation and scale of IBM X-Force



McAfee®
Threat Intelligence Exchange

Rezultati 9. sestavine

- Več znanja
- Boljša preventiva
- Dobre prakse

10. sestavina – Premisli

- Ustavi se
- Premisli
- Odreagiraj

UMIRJENO!!!

Rezultati 10. sestavine

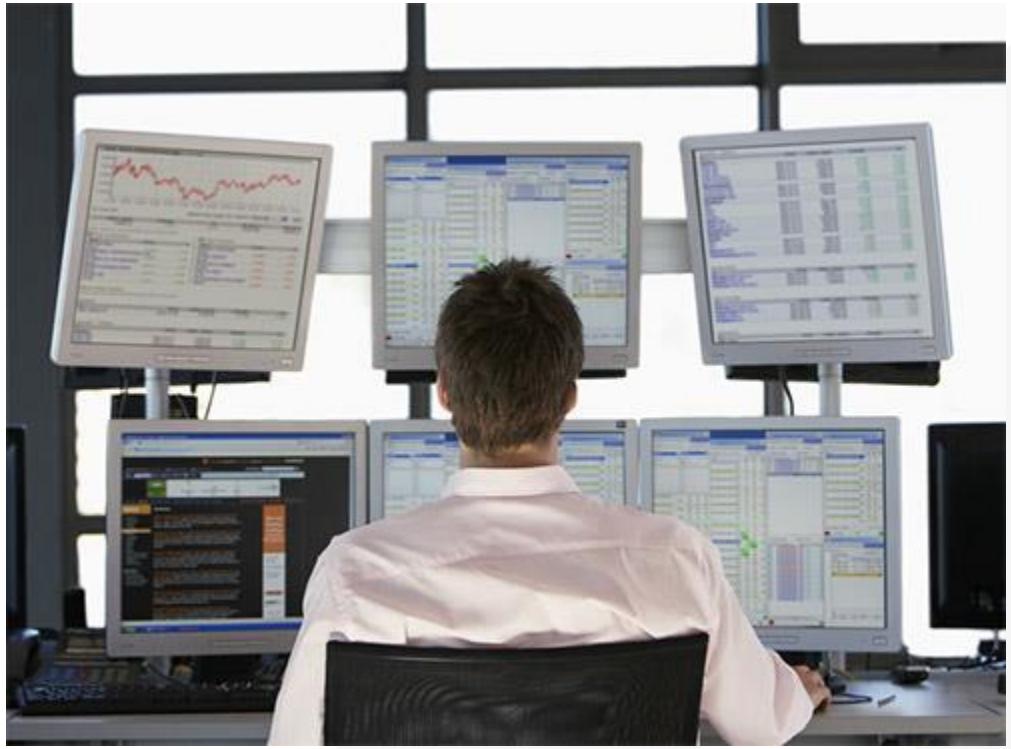
- Pravilen odziv
- Minimiziran vpliv incidenta
- Jasne posledice in skupen odziv
- Zaupanje pri uporabnikih
- Zaupanje v javnosti

Večno vprašanje

- Lasten SOC
- Upravljane storitve

Omejenost virov

- Ljudje
- Kompetence
- Stroški opreme
- Optimalni procesi
- Pooblastila
- Izmenjava podatkov
- Utilizacija
- Skladnost poročanja



Hvala!

info@unistarpro.si

UNISTAR PRO