PETROL

Izkušnje Petrola pri upravljanju z informacijsko varnostjo v luči ZInfV-1

Dr. Andrej Rakar, Vodja informacijske varnosti (CISO)

ZinfV-1 ključne zahteve

- samoregistracija zavezancev
- obvezno usposabljanje najvišjega vodstva vsaka 4 leta
- obvezno letno usposabljanje zaposlenih in skrbnikov IKT
- zagotavljanje integritete kadrov (lastnih in pogodbenih izvajalcev)
- izvajanje dolžnega nadzorstva nad ključnimi dobavitelji
- opredelitev varnostnih zahtev za ključne dobavitelje
- preverjanje izpolnjevanja in učinkovitosti varnostnih ukrepov
- ocena in samoocena skladnosti (najmanj na dve leti)

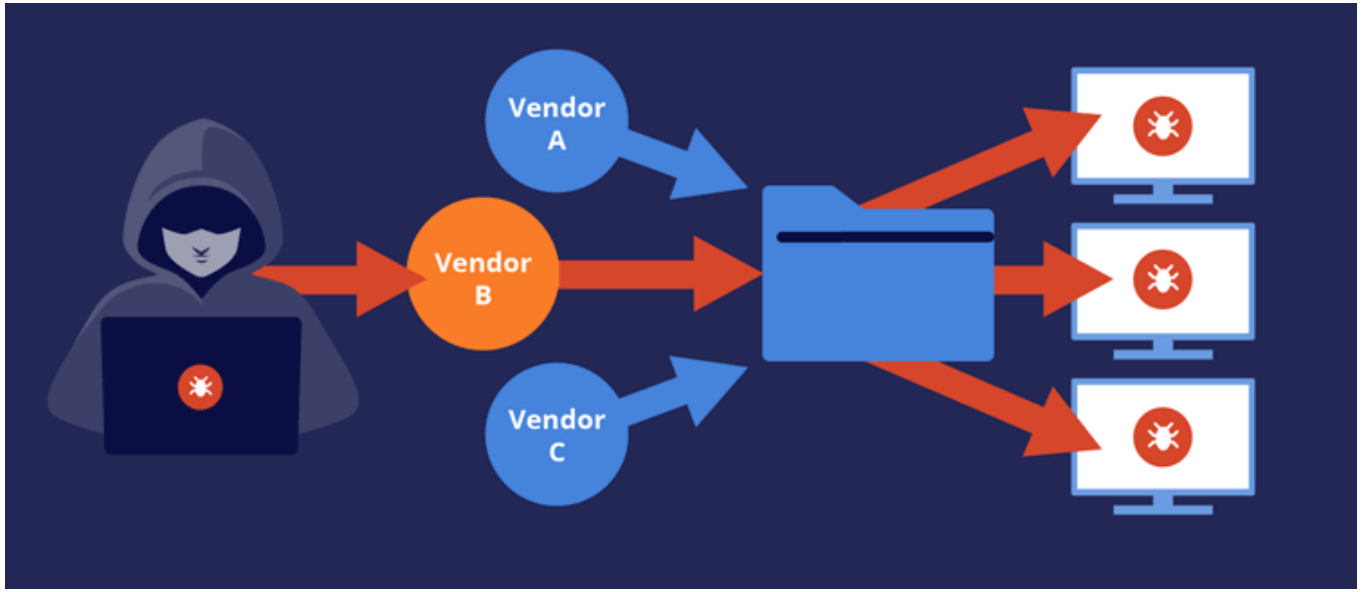
Izzivi

- Varnost dobavne verige
- Nadzor dostopov
- Varnostni ukrepi
- Odziv na incidente
- Preverjanje učinkovitosti

Varnost dobavne verige

Zahteva obvladovanje:

- programske opreme
- strojne opreme
- ljudi in procesov



Ranljivosti dobavne verige

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Malware Infection	Pre-existing Software
Social Engineering	Software Libraries
Brute-Force Attack	Code
Exploiting Software Vulnerability	Configurations
Exploiting Configuration Vulnerability	Data
Open-Source Intelligence (OSINT)	Processes
	Hardware
	People
	Supplier

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199]	Data
Drive-by Compromise [T1189]	Personal Data
Phishing [T1566]	Intellectual Property
Malware Infection	Software
Physical Attack or Modification	Processes
Counterfeiting	Bandwidth
	Financial
	People

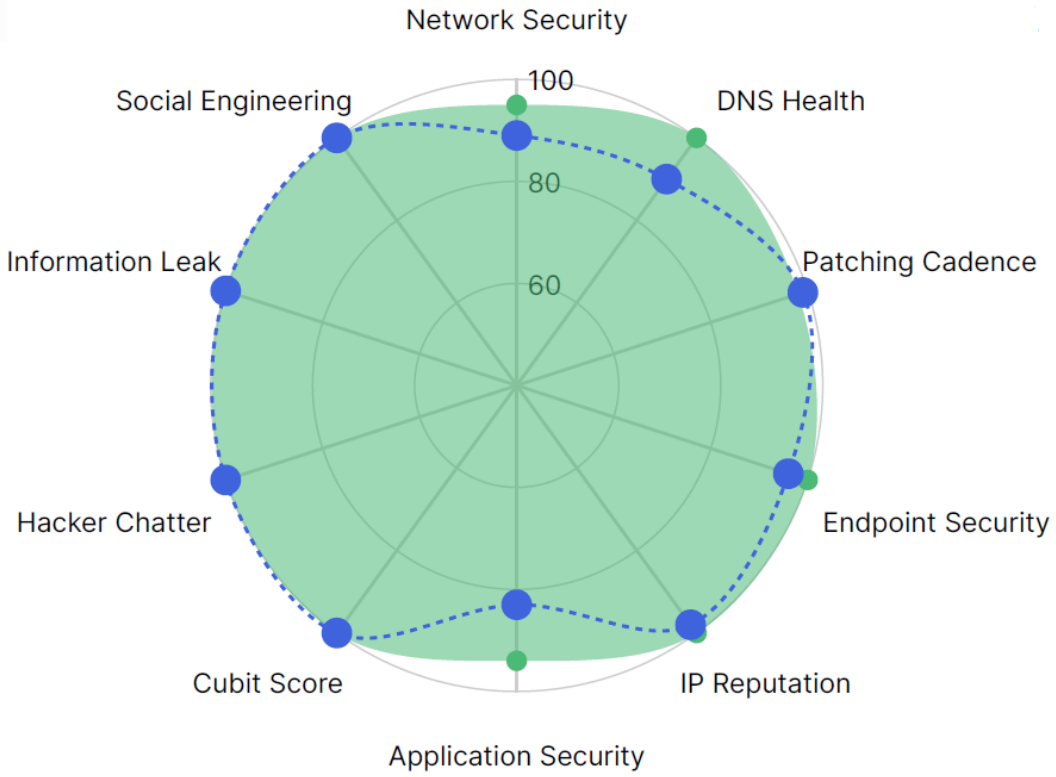
Potencialna tveganja

- Programska oprema po naročilu, brez dokumentacije in validacije
- Neupoštevanje varnostnih priporočil pri implementaciji rešitev
- Nevzdrževanje, zlasti varnostno
- Nadzor oddaljenih dostopov
- Priklop tuje opreme

Ukrep: varnostno ocenjevanje

- Orodje za varnostno ocenjevanje ključnih dobaviteljev:
  - ✓ avtomatizirano
  - ✓ pravno ustrezno
  - ✓ cenovno sprejemljivo
  - ✓ ocena na osnovi javno dostopnih informacij
  - ✓ ni obdelave osebnih podatkov tretjih strank

Faktorji ocenjevanja:



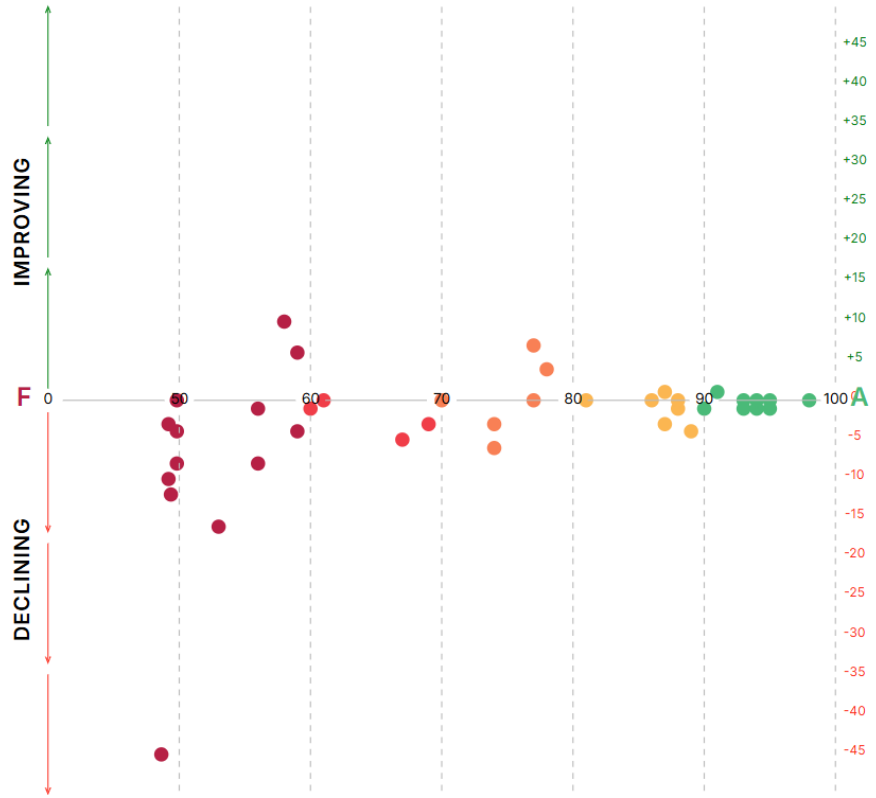
Ključni dobavitelji skupine Petrol

Overall Vendor Risk Brief for petrol.si

Prepared on Jun 06, 2025

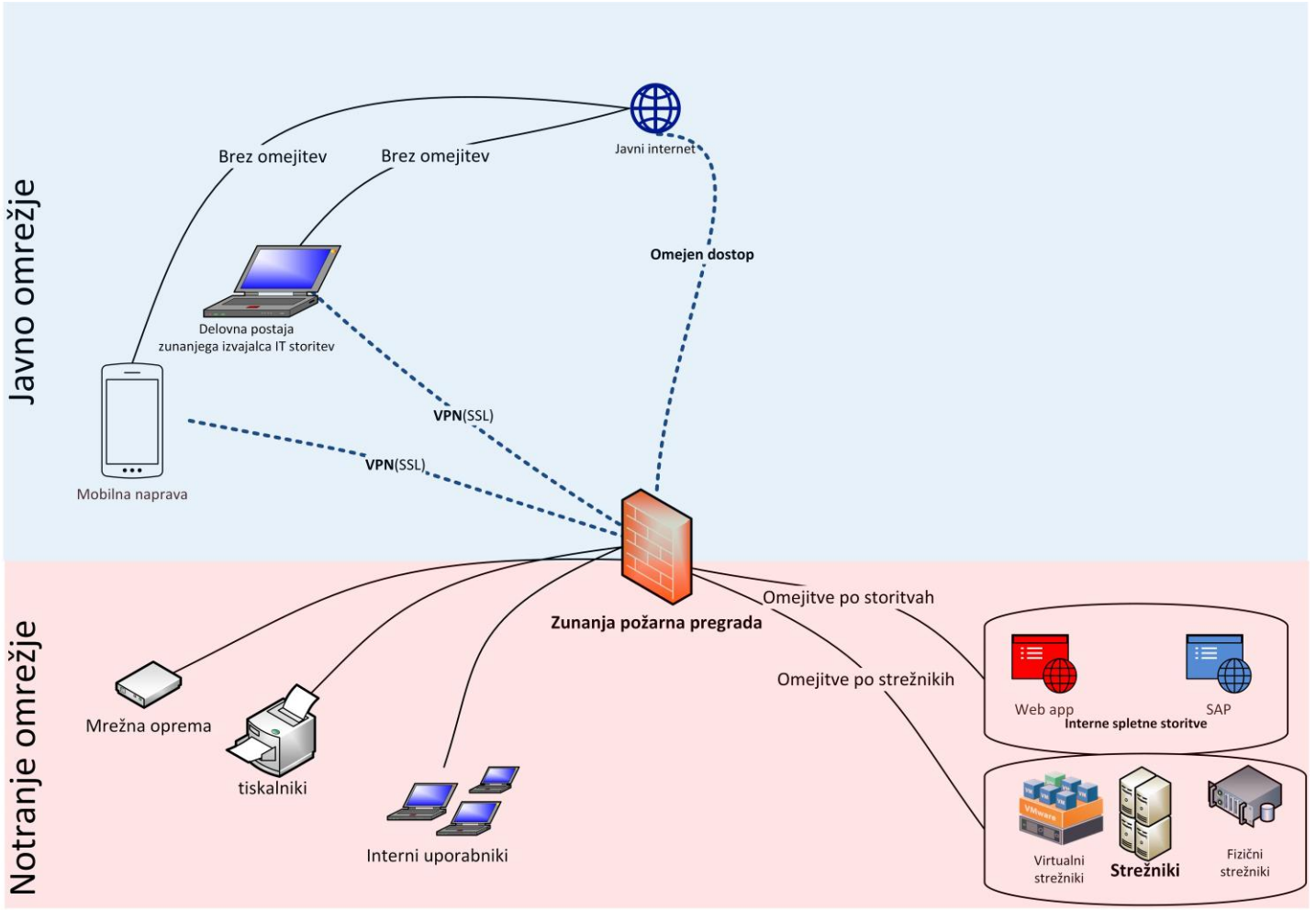
OUR OVERALL VENDOR RISK SCORE	OUR VENDOR BREACHES LTM	OPEN VENDOR CRITICAL ISSUES
C 73	1	600

PERFORMANCE TREND OVER 30 DAYS



Ukrep: kontrola zunanjih dostopov

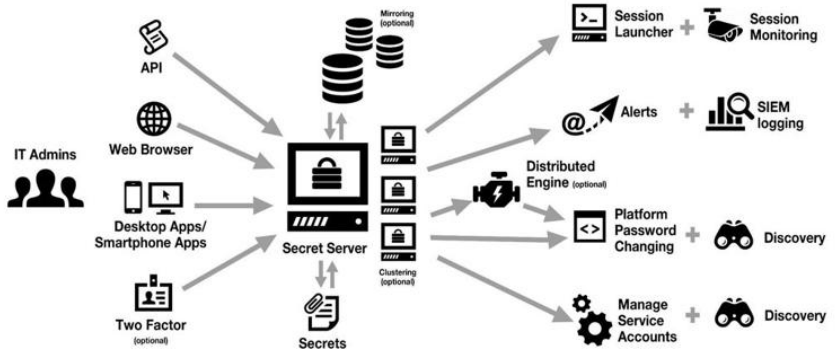
- Direkten dostop do omrežja
- Ni kontrole nad dostopi
- izmenjava poverilnic
- kompleksnost mrežne arhitekture in administracije

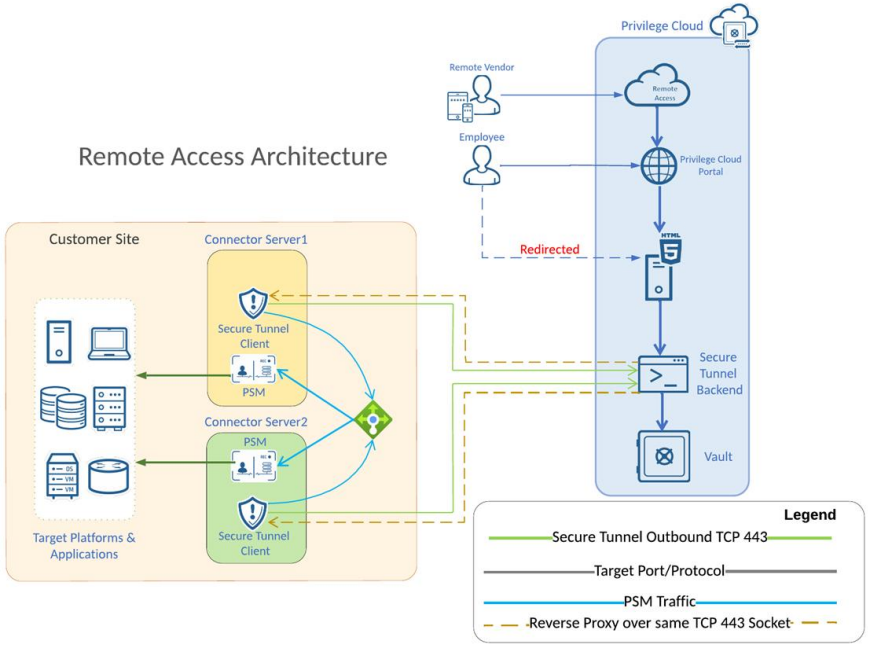


Večplastni nadzor dostopov

Ključni cilji:

- Poenostavitev omrežja, enotna varna točka dostopa brez direktne povezave do IS podjetja (smart proxy + cloudPC + PAM)
- Varen dostop za notranje in zunanje administratorje (password-less) - PAM
- Shramba poverilnic Upravljanje sprememb (Sef) - PAM
- Natančno določena pravila za dostope (role, časovna omejitev) - PAM
- Avtomatizirana menjava poverilnic - PAM
- Enotno beleženje, alarmiranje in poročanje - PAM
- Snemanje sej za nedvoumne revizijske sledi - PAM





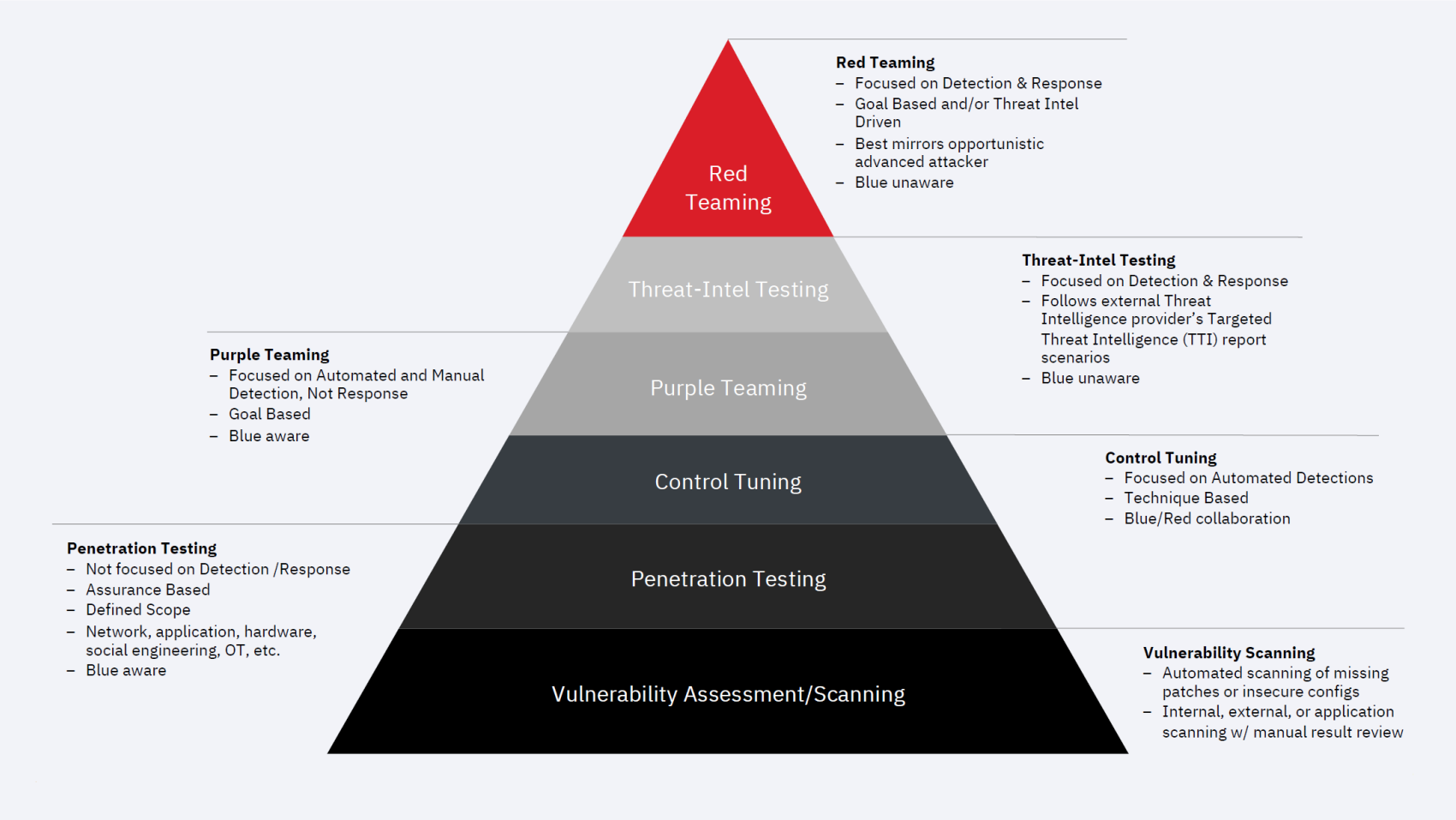
Ukrep: Vpeljava varnostnih kontrol

Ukrep: Odziv na incidente

Varnostno operativni center (SOC)

- Število in raznovrstnost napadov se iz leta v leto povečujeta
- Izredno pomembna je hitra reakcija na napade
- Za hitro in učinkovito zaznavo varnostnih incidentov je potrebna utečena ekipa visoko usposobljenih analitikov

Preverjanje učinkovitosti ukrepov



Vir: IBM

Ukrep: „Red teaming“ kibernetska vaja

Preverjanje učinkovitosti obrambe, zaznavanja in odzivanja na incidente s t.i. kibernetskimi vajami:

Pridobimo realno:

- oceno izpostavljenosti kibernetskim grožnjam;
- oceno zrelosti organizacije pri obvladovanju kibernetskih groženj;
- identificiramo področja, ki jih je potrebno izboljšati.

Vprašanja