kontron

The day after: Od kaosa do nadzora

Alex Crgol, Analitik za kibernetsko varnost
Luka Grah, Skrbnik upravljanja storitev

kontron

PORAST KIBERNETSKIH NAPADOV ZA PRIBLIŽNO 30 % V PRIMERJAVI Z LETOM 2023

Slovenija kljub majhnosti ni nepomembna tarča

kontron

Hekerski napad na upravo za zaščito: klice na 112 si zapisujejo na papir

SLOVENIJA | Avtor: STA | 19. Avg 2022 18:38 > 18:56 | 1 komentar

Delite :

ZNANOST IN TEHNOLOGIJA

Naša medijska hiša je bila žrtev hekerskega napada

Ljubljana, 08. 02. 2022 18.50 |

PREDVIDEN ČAS BRANJA: **1 min**

Tarča kibernetske grožnje tudi vrhovno sodišče

DIGITALNO | Avtor: N1 | 02. Feb 2024 17:57 | 2 komentarja

Skupina HSE tarča obsežnega kibernetskega napada #video

Policija potrdila hekerski napad: Kibernetski incident smo uspešno zamejili

SLOVENIJA | Avtor: M. V. | 03. Sep 2022 16:27 | 2 komentarja

Delite :

SLOVENIJA

Vladne spletne strani znova tarča kibernetskega napada

Ljubljana, 11. 04. 2024 10.23 |

PREDVIDEN ČAS BRANJA: **3 min**

AGENDA

1 SOC vs. ITOps

2 Primer odziva na kibernetski incident

3 Obnova po incidentu

4 Preprečevanje bodočih napadov

5 Zaključek

SOC vs. ITOPS

- **SOC (Security Operations Center)** je specializirana enota, ki nadzoruje, zaznava in se odziva na varnostne incidente v IT okolju organizacije. **Njegova glavna naloga je zagotavljanje kibernetske varnosti s stalnim spremljanjem in analizo groženj v realnem času**.

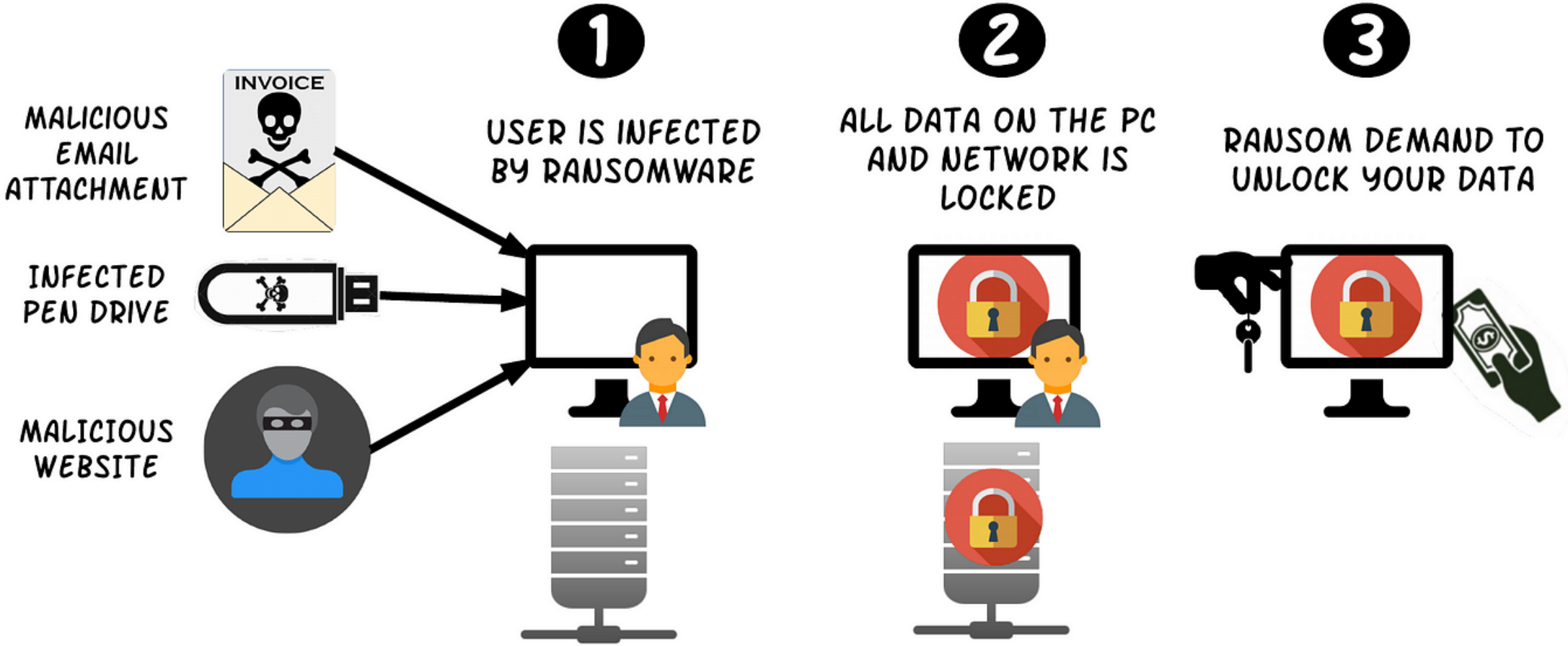
- **IT Ops (Information Technology Operations)** je oddelek, odgovoren za upravljanje, vzdrževanje in podporo IT infrastrukture in storitev v organizaciji. **Njegova glavna naloga je zagotavljanje nemotenega delovanja sistemov, omrežij in aplikacij ter zagotavljanje, da so IT storitve zanesljive, dostopne in učinkovite**.

SOC vs. ITOPS

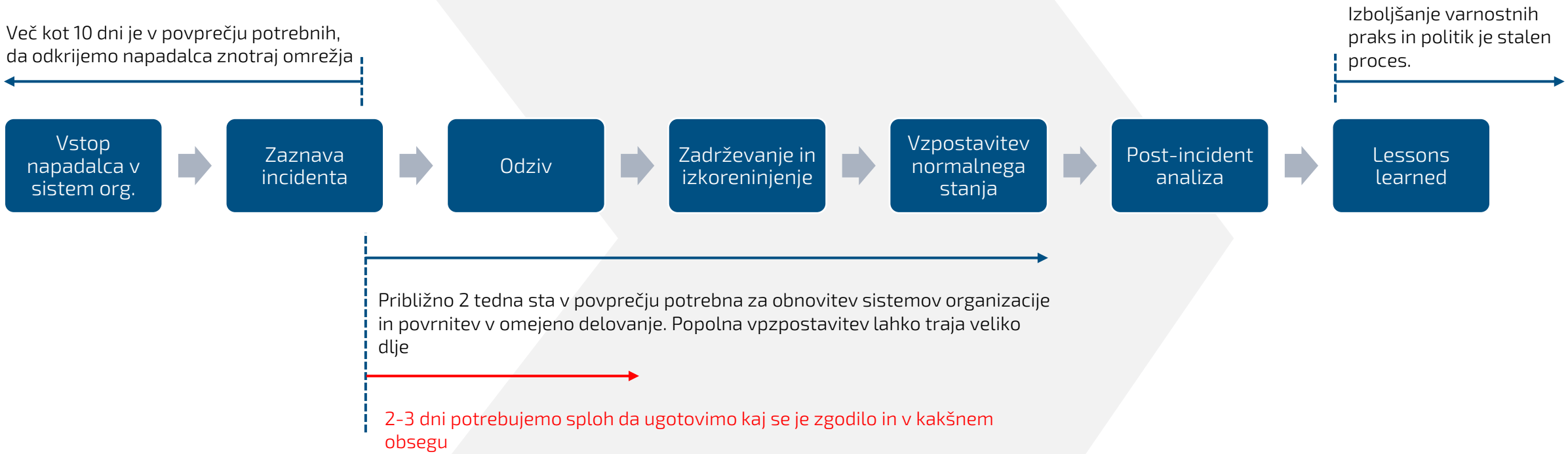
- Nadzor in spremljanje
- Odziv na incidente
- Analiza groženj
- Upravljanje ranljivosti
- Upravljanje groženj
- Izobraževanje

- Upravljanje infrastrukture
  - Upravljanje sistemov in omrežji
  - Nadzor in spremljanje delovanja
  - Podpora uporabnikom in reševanje incidentov
  - Pomoč in izobraževanje uporabnikov
- Upravljanje ITSM procesov
  - Razvoj in vpeljava
  - Vodenje procesov
- Razovj infrastrukture

Scenarij


1
2
3
MALICIOUS EMAIL ATTACHMENT
INVOICE
INFECTED PEN DRIVE
MALICIOUS WEBSITE
USER IS INFECTED BY RANSOMWARE
ALL DATA ON THE PC AND NETWORK IS LOCKED
RANSOM DEMAND TO UNLOCK YOUR DATA

Časovnica zaznave in odziva na incident



Zaznava in odziv na kibernetski incident

Uporabniki javijo “čudno” delovanje aplikacij.

ITOPS začne s testiranjem ter iskanjem napake

Sum na napad z zlonamerno programsko opremo

+

SOC začne z analizo izsledkov ITOPS ekipe

Kdo je vse lahko udeležen?

SOC z ekipo za odziv na kibernetske incidente, ki:
- vodi obravnavo incidenta
- Zavaruje dokaze (če je potrebno)
- Sodeluje z ostalimi udeleženci

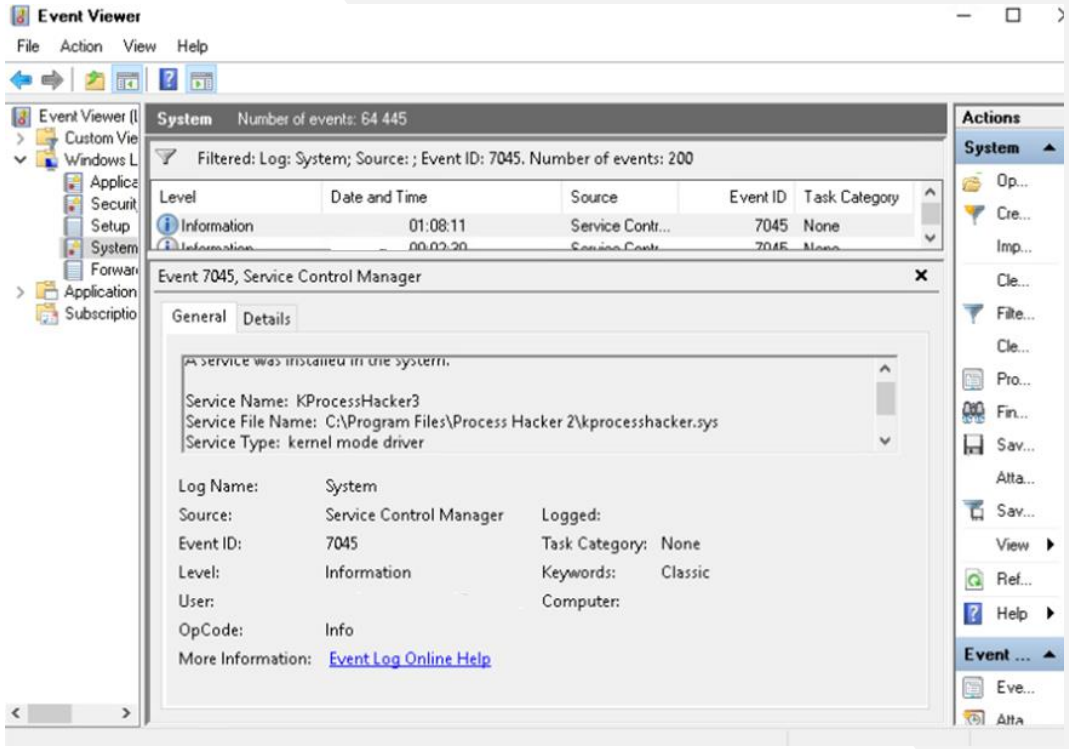
IT OPS ekipa nudi:
- informacij o sistemu (razlago, dokumentacijo)
- Dostop do sistema (uporabiška imena, gesla, fizični dostop do opreme)
- Izvaja spremembe na sistemu

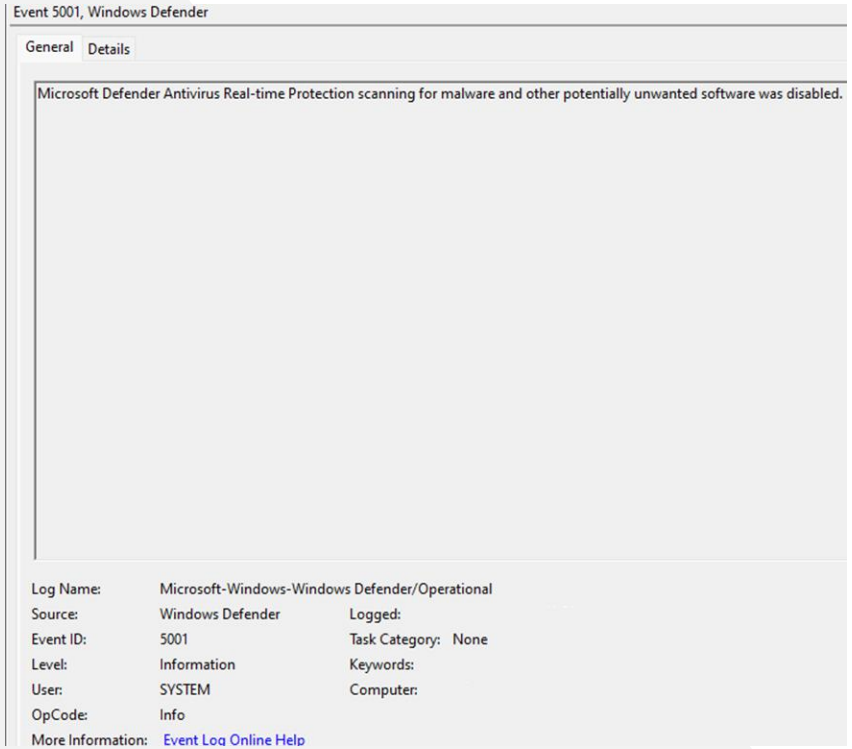
Vodstvo podjetja
Pravna služba
PR služba
Zunanji partnerji

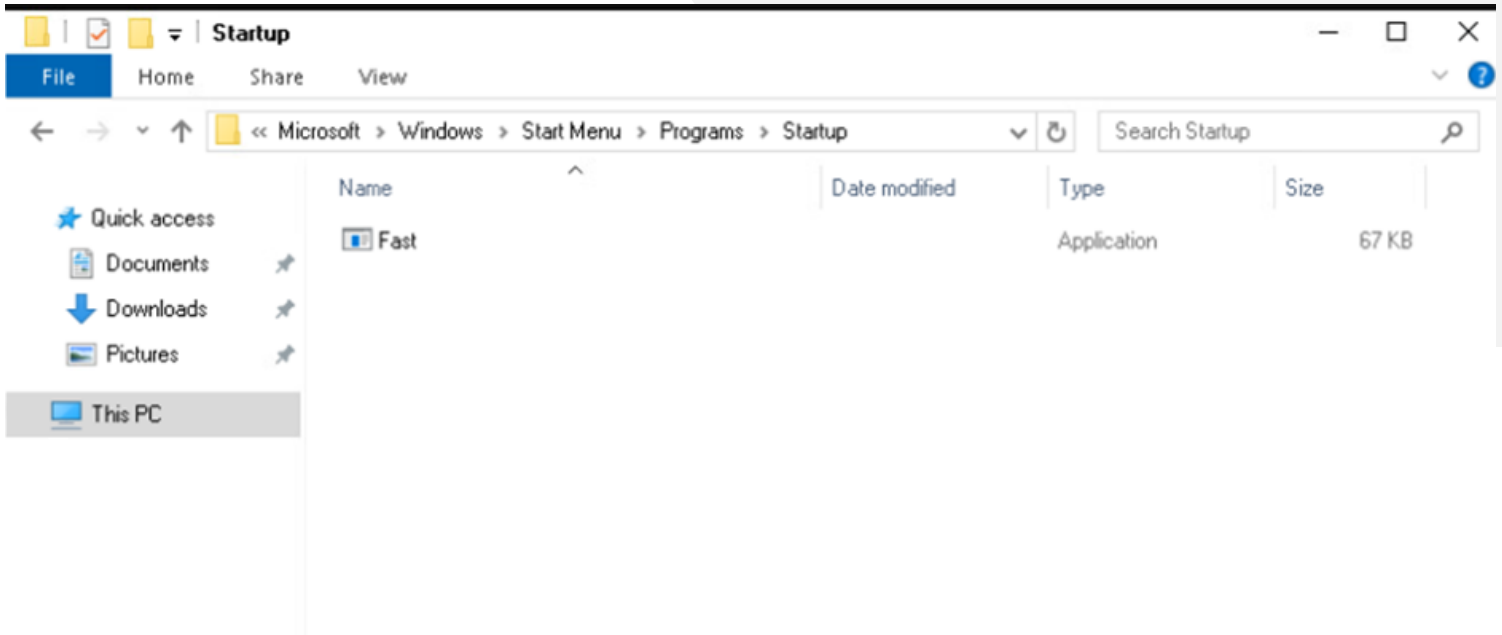
Nadzorni organi
Stranke in partnerji
Zaposleni

Glavna vprašanja pri odzivu na incident

- Kje se je incident začel?
- Kdo je zaznal dogodek in kako?
- Kateri sistemi, uporabniki in storitve so prizadeti?
- Ali so bili že uvedene protiukrepi? Če da, kakšni so bili? Kdaj in kje?
- Ali lahko sisteme omejimo, da se zadeva ne širi?
- Ali so IT in OT sistemi ločeni? Če ne, ali lahko postanejo?
- Ali oddaljen dostop še deluje?
- Ali so bile opažene sumljive dejavnosti, kot so aktivnosti računov, povezanih s privilegiranimi identitetami, ali ponastavitve gesel?
- **So na voljo dnevniki iz sumljivih sistemov?**
- **Obveščanje deležnikov (prijava SI-CERT, Policija, URSIV)**


Event Viewer
File Action View Help
System Number of events: 64 445
Filtered: Log: System; Source: ; Event ID: 7045. Number of events: 200
Level Date and Time Source Event ID Task Category
Information 01:08:11 Service Contr... 7045 None
Event 7045, Service Control Manager
General Details
Service Name: KProcessHacker3
Service File Name: C:\Program Files\Process Hacker 2\kprocesshacker.sys
Service Type: kernel mode driver
Log Name: System
Source: Service Control Manager Logged:
Event ID: 7045 Task Category: None
Level: Information Keywords: Classic
User: Computer:
OpCode: Info
More Information: Event Log Online Help
Actions
System


Event 5001, Windows Defender
General Details
Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender Logged:
Event ID: 5001 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer:
OpCode: Info
More Information: Event Log Online Help


Startup
File Home Share View
Microsoft › Windows › Start Menu › Programs › Startup
Search Startup
Name Date modified Type Size
Fast Application 67 KB
Quick access
Documents
Downloads
Pictures
This PC

Zadrževanje in izkoreninjanje

SOC

- Priprava načrta za obnovo varno sistemov
- Začetna analiza zlonamerne kode
- Nadaljevanje iskanja indikatorjev kompromisa

ITOPS

- Nudi podporo SOC ekipi
- Pripravi postopke za varno obnovo sistema
- Pripravi postopke za zavarovaje nekomprimiranih podatkov

Vzpostavitev normalnega stanja

kontron

SOC

- Analiza zlonamerne kode
- Priprava hardening priporočil za nove sisteme
- Nadzor nad obnovitvijo sistema
- Nadzor prometa (SIEM, FW itd.)

ITOPS

- Izvajanje postopkov za povrnitev sistema v delujoče stanje
- Izvedba hardening priporočil SOC ekipe
- Vzpostavitev dodatnih metod nadzora po priporočilih SOC ekipe

Priporočila za zmanjšanje verjetnosti napada z zlonamerno kodo

Kratkoročne

- Upoštevanje splošnih priporočil varnosti
- Politika varnih gesel
- Odprava ranljivosti
- Izvedbe penetracijskih testiranj
- Nameščanje varnostnih popravkov
- Večfaktorska avtentikacija

Dolgoročne

- Politike in procesi (ITSM)
  - Vpeljava procesa za spremljanje sprememb (Change management)
  - Vpeljava procesa za odziv na incidente
  - Vpeljava postopkov neprekinjenega poslovanja ter varovanja podatkov (Testiranje!!!!)
- Izobraževanja uporabnikov
- Ocena varnostnih tveganj
- Upravljanje dobaviteljev

Kontakt

Alex Crgol
Analitik za kibernetsko varnost
Alex.Crgol@kontron.si
+386 51 343 857

Luka Grah
Skrbnik upravljanja storitev
Luka.Grah@kontron.si
+386 41 386 943

Kontron, d. o. o.
Ljubljanska cesta 24a
4000 Kranj, Slovenia
www.kontron-slovenia.com