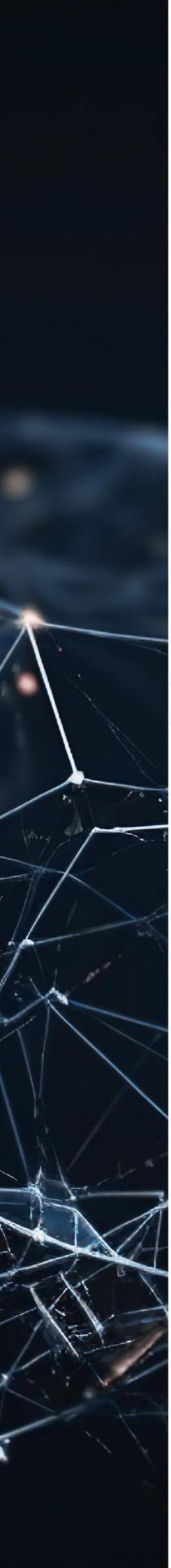

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Všeobecné informácie o službe

FORENZNÁ ANALÝZA

od **VJ CSIRT**

oAKH

Oddelenie analýzy kybernetických hrozieb

Charakteristika služby

Digitálna forenzná analýza je odborná služba zameraná na získanie, zachovanie, analýzu a vyhodnotenie digitálnych stôp súvisiacich s kybernetickým bezpečnostným incidentom. Jej cieľom je zistiť príčinu incidentu, identifikovať inicializačný vektor, zdokumentovať priebeh útoku a určiť rozsah kompromitácie. Služba poskytuje organizácii odporúčania potrebné na prijatie nápravných opatrení, obnovenie bezpečného stavu a zvýšenie odolnosti voči budúcim útokom.

Vládna jednotka CSIRT.SK poskytuje pomoc pri riešení bezpečnostných počítačových incidentov pre štátnu a verejnú správu. Forenzná analýza sa spravidla realizuje ako súčasť procesu riešenia bezpečnostného incidentu (Incident Response). Do procesu vyšetrovania sa zapája v prípadoch, keď je potrebné získať detailný pohľad na priebeh incidentu, potvrdiť alebo vyvrátiť podozrenie na kompromitáciu systémov, identifikovať aktivity útočníka alebo vyhodnotiť rozsah vzniknutých škôd. V závislosti od charakteru incidentu môže byť forenzná analýza vykonávaná paralelne s aktivitami smerujúcimi k obmedzeniu a odstráneniu incidentu alebo následne po jeho stabilizácii.

Kedy službu využiť

Služba je určená pre organizácie štátnej a verejnej správy, ktoré čelia alebo čelili bezpečnostnému incidentu, ako sú neoprávnené prístupy do systémov, ransomvérové útoky, podozrenia na únik dát, kompromitácia používateľských účtov, zneužitie privilegovaných oprávnení alebo iné formy kybernetických útokov. Digitálna forenzná analýza je poskytovaná konštituencii ako súčasť riešenia kybernetického bezpečnostného incidentu.

Priebeh forenznej analýzy a súčinnosť organizácie

Poskytovanie služby začína oznámením alebo eskaláciou bezpečnostného incidentu na CSIRT tím. Po úvodnom posúdení situácie sa stanoví rozsah vyšetrovania, identifikujú sa relevantné systémy a určí sa spôsob získania potrebných dát a dôkazov.

V závislosti od povahy incidentu môže byť vykonaná analýza živého systému (live analysis), pri ktorej sa skúmajú aktuálne procesy, pamäť, sieťové spojenia a ďalšie dostupné artefakty, alebo sa vytvorí forenzná bitová kópia dátového nosiča a obraz pamäte RAM určená na podrobnú offline analýzu. Voľba postupu závisí od typu systému, rozsahu incidentu a požiadaviek na zachovanie dôkazov.

Počas vyšetrovania prebieha priebežná komunikácia s kontaktnými osobami organizácie. V prípade potreby sú vyžiadané doplňujúce informácie, logy alebo prístupy potrebné na pokračovanie analýzy. Organizácia je priebežne informovaná o významných zisteniach, ktoré môžu mať vplyv na ďalší postup riešenia incidentu.

Úspešné vykonanie forenznej analýzy vyžaduje primeranú súčinnosť zo strany organizácie. Organizácia by mala zabezpečiť kontaktné osoby oprávnené poskytovať informácie o incidente, infraštruktúre a dotknutých systémoch. Dôležité je poskytnutie informácií o čase zistenia incidentu, pozorovaných prejavoch kompromitácie a už vykonaných opatreniach.

V závislosti od rozsahu vyšetrovania môže byť potrebné poskytnúť prístup k systémom, logovacím nástrojom, bezpečnostným riešeniam, cloudovým službám alebo ďalším zdrojom údajov relevantným pre analýzu. Organizácia by zároveň mala zabezpečiť, aby nedošlo k zbytočnému odstráneniu alebo zmene potenciálnych dôkazov pred začiatkom vyšetrovania. Kvalita a dostupnosť poskytnutých údajov, logov a technických informácií má významný vplyv na rozsah a presnosť výsledkov forenznej analýzy.

Rozsah analyzovaných prostredí

Počas forenznej analýzy sú zhromažďované, zabezpečované a vyhodnocované relevantné digitálne stopy a dôkazy z dostupných systémov a zariadení. Skúmajú sa logy, systémové artefakty, sieťová komunikácia, používateľské aktivity, zmeny v konfiguráciách, škodlivý kód a ďalšie dostupné zdroje informácií. Výsledkom je rekonštrukcia časovej osi incidentu, identifikácia vektora útoku, použitých techník a nástrojov útočníka, ako aj vyhodnotenie rozsahu kompromitácie vrátane prípadného prístupu k citlivým údajom alebo kritickým systémom.

Analýza môže byť realizovaná na širokom spektre prvkov informačnej infraštruktúry. Medzi nich patria pracovné stanice a servery s operačnými systémami Microsoft Windows (napr. IIS, Exchange, DC), Linux (napr. Apache, nginx), virtualizačné platformy a sieťové prvky, ako sú firewally, VPN brány, routery alebo prepínače. Analýza ďalej pokrýva záznamy zo SIEM, IDS/IPS a NDR/EDR/XDR platforiem, ktoré umožňujú korelovať bezpečnostné udalosti naprieč celým prostredím a spresniť rekonštrukciu priebehu útoku. V prípade potreby je možné analyzovať aj mobilné zariadenia so systémami Android a iOS, pokiaľ rozsah incidentu a dostupnosť dát umožňujú vykonanie relevantnej analýzy.

Výstupy

Výstupom služby je komplexná forenzná správa, ktorá dokumentuje všetky relevantné zistenia získané počas vyšetrovania. Správa obsahuje popis identifikovaného vektora útoku, časovú os incidentu, zoznam dotknutých systémov a aktív, vyhodnotenie rozsahu kompromitácie, identifikované indikátory kompromitácie (IoC) a technické detaily potrebné na pochopenie priebehu útoku. Súčasťou výstupu sú aj odporúčania na odstránenie zistených nedostatkov, návrhy bezpečnostných opatrení a kroky vedúce k zvýšeniu odolnosti organizácie voči budúcim bezpečnostným incidentom. V prípade potreby môžu byť výsledky prezentované aj formou konzultácie alebo pracovného stretnutia.

Obmedzenia

Úspešnosť a rozsah forenznej analýzy sú závislé najmä od dostupnosti a kvality podkladových dát, najmä systémových, aplikačných a sieťových logov, ako aj ďalších relevantných artefaktov. Ak tieto údaje nie sú dostupné, sú neúplné, boli prepísané, vymazané alebo neboli vôbec generované, môže byť analýza výrazne obmedzená.

Ďalšie obmedzenia vyplývajú z retenčných politík, časového odstupu od incidentu, použitia šifrovania bez dostupných kľúčov, ako aj z právnych a organizačných limitov alebo závislosti od tretích strán. Všetky tieto faktory môžu zásadne ovplyvniť schopnosť CSIRT tímu plne rekonštruovať priebeh incidentu a určiť jeho rozsah.

Prínosy služby

Realizácia forenznej analýzy umožňuje organizácii nielen získať presné informácie o incidente, ale aj minimalizovať jeho následky, urýchliť obnovu prevádzky a prijímať kvalifikované rozhodnutia založené na overených faktoch. Výsledky vyšetrovania zároveň poskytujú dôležitý základ pre ďalšie bezpečnostné opatrenia, zlepšovanie procesov riadenia incidentov a budovanie celkovej kybernetickej odolnosti organizácie.