Incident Response Retainer

Březen 2022

pwc

Obsah

Klíčové kontakty

Michal Wojnar
Senior manažer Incident Response
M: + 420 724 726 166
E: michal.wojnar@pwc.com

Marek Nejedlý
Manažer Incident Response
M: +420 735 701 525
E: marek.nejedly@pwc.com

Pohotovostní linka: +420 251 151 050


1
Incident
Response
služby

PwC Cybersecurity Incident Response služby

Služby před incidentem

Posouzení připravenosti
- Strukturované hodnocení aktuálního stavu
- Analýza existujících příruček a správy incidentů
- Posouzení minulých incidentů
- Ověření existující IT architektury

Pohotovostní služby
- Nepřetržitá koordinace při poruchách a incidentech
- Trénink týmu na místě (Cyber Arena, blue, red týmový trénink)
- Průběžné vyhodnocování bezpečnostní situace
- Průběžná optimalizace správy incidentů
- Vytváření playbooků
- Spolupráce s purple týmem

Služby po incidentu

LIVE Koordinace incidentů a krizové řízení
- Koordinování incidentů a (krizová) komunikace
- Posouzení a minimalizace následků narušení prostředí
- Analýza a podpora analýzy malwaru
- Uchovávání forenzních důkazů
- Doporučení pro další opatření – bezpečnost informací a ochrana dat
- Právní podpora

Přezkoumání situace po incidentu
- Výzkum příčin a doporučení pro preventivní opatření
- Identifikace potřeb zlepšení v řízení incidentů a krizových situací
- Zpracování znaleckých posudků pro kybernetické pojištění a posouzení rozsahu škod
- Posouzení získaných zkušeností z incidentu
- (Příprava) zpráv zainteresovaným stranám

Incident Response Retainer

Incident Response Retainer prvky

Naše služby nabízejí globální dostupnost na vyžádání v režimu 24x7x365 specializovaný tým, který funguje pro odbavení incidentů v případě kybernetického útoku.

Klíčové benefity:

- Rychlá a efektivní odezva ke snížení dopadu incidentu bez nutnosti zapojovat poskytovatele, když jste pod nátlakem, což by mohlo zpozdit vaši reakci.
- Příprava příslušných plánů, dokumentace a roadmapy vyspělosti pro posouzení vyspělost IR.
- Servisní smlouvy jsou přizpůsobené tak, aby vyhovovaly vašim specifickým obchodním požadavkům.
- Dostupnost incident reportů a údajů k prokázání spolupráce všem zúčastněným stranám a regulačním orgánům.
- Přístup k široké škále odborníků v polích kybernetické bezpečnosti, forenzního, obchodního a právního poradenství - ti všichni mají zkušenosti s úzkou spoluprací v dobách krize.

Naše Incident Response Retainer služba zahrnuje:

1. **Workshopy** za účelem pochopení vašeho podnikání, IT infrastruktury, stávajících zásad a postupů reakce na incidenty a zajištění efektivní reakce.
2. On-site i remote **doba odezvy pokryté SLA.**
3. **Více eskalačních kanálů,** včetně nepřetržité telefonické pohotovostní linky.
4. Virtuální komunikace v **reálném čase s naším IR týmem,** abychom zajistili plynulé rozšíření vašeho týmu. Nejsme **jen dalším poskytovatelem služeb.**
5. **Připravenost na krizové situace** a podpora managementu tam, kde je to potřeba, od úrovně představenstva až po týmy první linie.
6. Přístup k našim přizpůsobeným šablonám na report incidentů a řadě dalších zdrojů.
7. **Nevyužité hodiny ve službě retainer** lze použít na cvičení připravenosti a vybrat sadu poradenských služeb v oblasti kybernetické bezpečnosti**, abyste maximalizovali návratnost svých investic.**
8. **Rychlý přístup k řadě dalších služeb** v oblasti kybernetické bezpečnosti (včetně zpravodajství o hrozbách a detekce hrozeb) **pro vytvoření širší bezpečnostní strategie.**

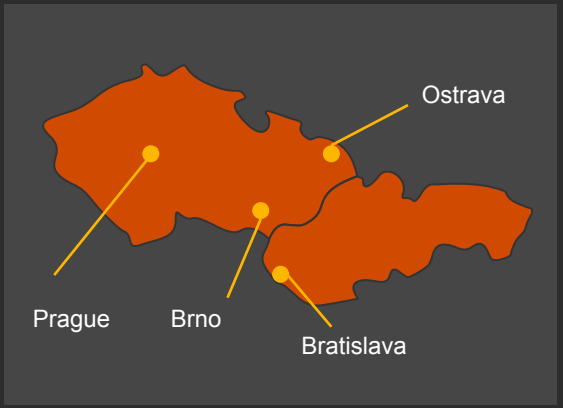
Globální PwC dosah řízený lokálním teamem

Jsme strukturování tak, abychom přinášeli naše globální odborné znalosti, hluboké technické zkušenosti, oborové specializace a technologická partnerství do každého případu reakce na incident. Tuto službu nabízíme prostřednictvím našeho lokálního a snadno dostupného týmu v Praze, Brně, Ostravě a Bratislavě, který lze kontaktovat jediným telefonátem, emailem nebo chatovou zprávou přes definovanou komunikační platformu.

Místní kontakty PwC budou spolupracovat s vašimi místními týmy, aby pochopili konkrétní výzvy. Tímto způsobem zajišťujeme, že bezpečnostní incidenty mohou být adekvátně řešeny na každém jednotlivém místě. V rámci přípravy jsou koordinovány metody spolupráce a testovány procesy reakce na incidenty.

Naši kolegové reagují na každý požadavek na bezpečnostní incident okamžitě. Naše IR call centrum přijímá vaše dotazy 24x7. Naši odborníci na reakce na incidenty budou na vašem místě co nejrychleji. Konkrétní smlouvy SLA lze přizpůsobit na základě vašich požadavků.

Naši profesionálové, vybraní z armády a bezpečnostních služeb mají dlouholeté zkušenosti s identifikací a reakcí na řadu incidentů na některých z nejcitlivějších světových sítí. Naši bezpečnostní experti byli součástí cvičení NATO Locked Shield, kde obsadili 3. místo napříč zeměmi NATO.



Síť PwC je přítomna téměř po celém světě: Našich 721 poboček je rozmístěno ve 158 zemích s více než 250 000 lidmi.

PwC má více než 650 odborníků na forenzní IT, reakci na incidenty a zpravodajství o hrozbách a více než 60 forenzních IT laboratoří po celém světě.

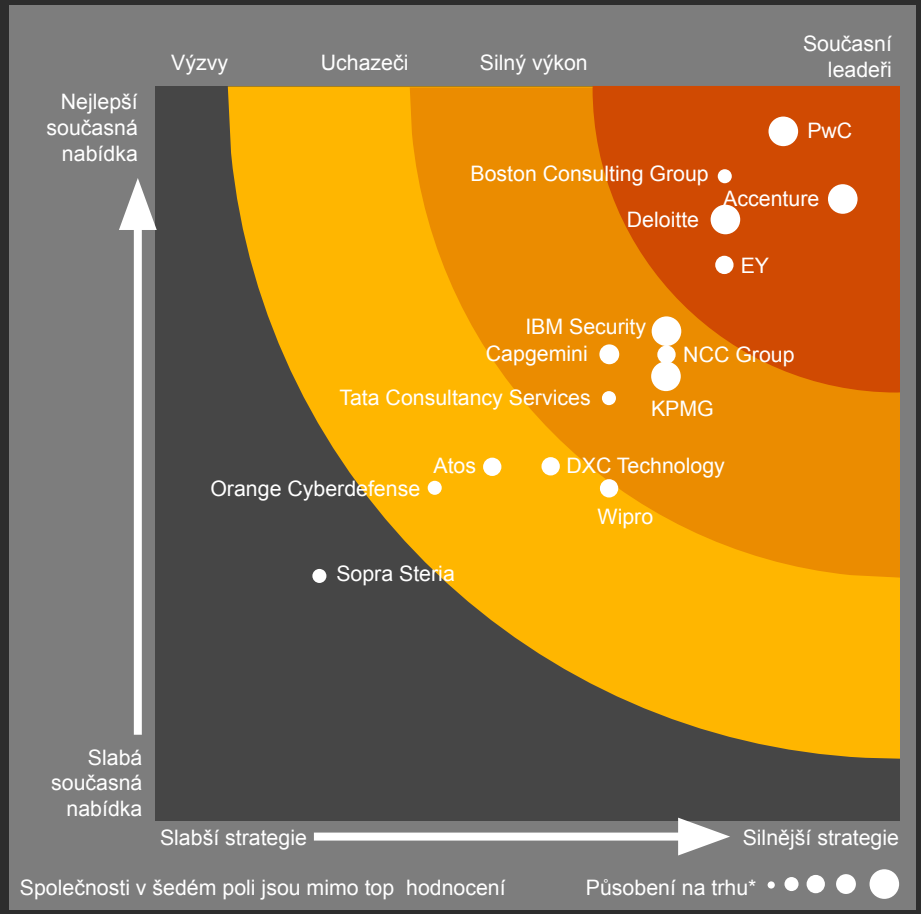
PwC IR team má certifikace ISO 9001, TISAX a ISO 27001.

Členové našeho týmu jsou držiteli různých certifikací kybernetické bezpečnosti (SANS, CISSP, OSCP, CEH) a členy GIAC Advisory Board.

Nejlepší Evropské konzultační společnosti v poli kybernetické bezpečnosti Q3 2021

Forrester: Co odlišuje PwC od konkurence?

- PwC přesvědčuje vysoce kvalifikovanou a cílenou podporou pro vedoucí pracovníky v oblasti kybernetické bezpečnosti: S exkluzivním programem CISO Masterclass podporuje PwC vašeho CISO v růstu do jeho nové vedoucí role.
- PwC investuje do vývoje nástrojů a aplikací v oblastech DevSecOps, Cyber Threat Intelligence a Incident Response, které jsou dostupné prostřednictvím SaaS platformy.
- PwC podporuje technický rozvoj svých konzultantů s důrazem na efektivní a praktické řešení incidentů, čímž zajišťuje skupinu zkušených poradců.
- Klientům, kteří se spoléhají na strategickou podporu na úrovni vedení a vysoce kvalifikované technické dovednosti, PwC dobře slouží.



PwC CZ & SK– Digital Forensics & Incident Response

Náš team

Náš tým pro reakci na incidenty zahrnuje experty na kybernetické bezpečnostní incidenty a počítačové forenzní experty. V rámci naši Incident Response služby PwC nabízí podporu při přípravě na bezpečnostní incident, řešení vznikajícího bezpečnostního incidentu a provádění uchovávání a analýzy forenzních důkazů IT. Níže je uvedena reprezentace našeho základního týmu IR Response Retainer. V případě potřeby tuto službu podporují další odborníci z oblasti IT bezpečnosti, informační bezpečnosti, ochrany dat a forenzní vědy, stejně tak i naši právníci.

Základní tým **Incident Response Retainer** má dovednosti v oblasti služeb reakce na incidenty, **krizového řízení** a **IT forenzní analýzy**.

Cyber & Privacy Team

Michal Wojnar
Vedoucí Threat Management

Incident Response Services

Marek Nejedlý
Vedoucí IR
Praha

Ondřej Šrámek
IR Expert
Brno

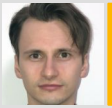
Antonin Novokhatko
L3
Praha

William Reich
L3
Bratislava

Michal Pohludka
L2
Ostrava

Joshua Zrzavy
L2
Brno

Josef Pinďák
L2
Praha

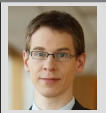


Marcel Sisler
L2
Brno

Forensic Services Team

Pavel Jankech
Vedoucí Forensics

Forensic Technology Services



Jakub Javorský
DF Expert
Praha

Oliver Waczulík
L3
Praha

2

Incident Response Retainer služba

Rychlý přístup k odborným znalostem, když je nejvíce potřebujete

Incident Response Retainer | Readiness a Rapid Modely

CZK 2 400,- / 3 400,- hovor

Za basic*

CZK 23 900,- / měsíc

Za Readiness

CZK 63 800,- / měsíc

Za Rapid

Incident Readiness

- Každoroční workshop řízení incidentů
- Každoroční workshop architektury
- 5 (readiness) -15 (rapid) dní specializovaných zdrojů ve formátu zálohy
- Výroční zpráva vedení s doporučeními na základě incidentů

První kontakt - Vzdálená podpora

- Nepřetržitá pohotovostní služba 24/7 z České republiky jako SPOC (jednotné kontaktní místo)*
- Záznam incidentu
- Přidělení specialistům (druhá úroveň)
- Prvotní analýza incidentu společně se zákazníkem a prezentace dalších kroků
- Readiness: reakční doba do 4 hodin (pondělí-pátek 9-17 hodin)
- Rapid: reakční doba do 1,5 hodiny (pondělí-neděle 0-24)

Zvládání a koordinace incidentů

- Posouzení dopadu
- Rozdělení úkolů a koordinace se specialisty zákazníka a našimi odborníky
- Podávání zpráv zainteresovaným stranám
- Podpora zapojených oddělení
- Na místě následující pracovní den (pondělí-pátek) v rámci ČR

Forenzní a bezpečnostní expertiza

- Provádění forenzního zálohování a analýzy dat
- Možnost vyhledávání hrozeb na bázi EDR
- Výzkum příčiny a rekonstrukce incidentu
- Bezpečnostní testování
- Specialisté na konkrétní systémy
- Přístup k PwC Threat Intelligence a OT Security Competence Center
- Analýza logů
- Analýza malwaru

*Pouze pokud je hovor mimo pondělí – pátek 9:00–17:00. Jinak je zdarma.

Snížené sazby poplatků v modu Readiness v případech odezvy na incidenty, platformy externí komunikace a výměny dat, detekční techniky a technologie sandbox na vyžádání.

Uvedené ceny a služby jsou pouze strukturovanou reprezentací typických služeb Reakce na bezpečnostní incidenty a nejsou závaznou nabídkou. I přes měsíční paušály se jedná o roční službu (12 měsíců). Mezi modely Readiness a Rapid můžete přecházet jednou ročně.

Incident Response Retainer možnosti

Nabízíme tři základní charakteristiky reakce na incidenty – rychlost, efektivitu a odbornost v různých formách.

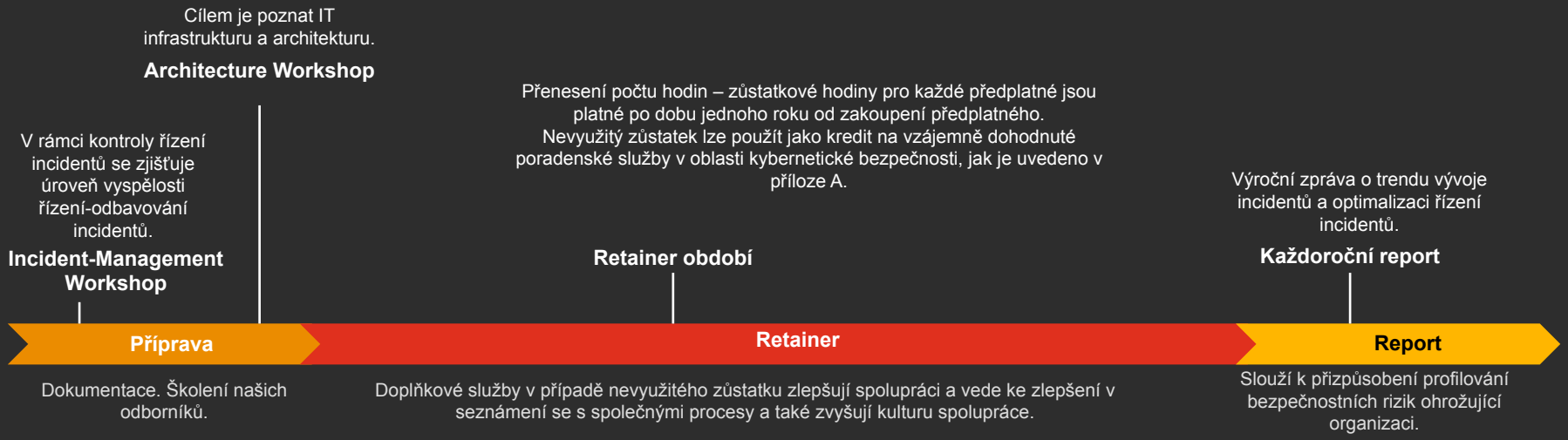
	1 Rychlost			2 Efektivita			3 Odbornost
	24/7 Incident Response Pohotovostní linka*			Incident Readiness & roční report	Spolupráce	Retainer	Škálovatelný počet odborníků na digitální forenzní a incidenty s certifikací SANS (Analýza malwaru, Inteligence hrozeb, OT atd.)
	Vzdálená podpora	Podpora na místě	Cena				
Basic Zdarma s rámcovou smlouvou.*	Vzdálená podpora s ohledem na naší vytíženost	Podpora na místě s ohledem na naší vytíženost Základní sazba za den	Standard	Nezahrnuto	Nezahrnuto	Nezahrnuto	
Readiness CZK 23 900,- měsíčně	Vzdálená podpora do 4 hodin (pondělí–pátek 9–17 hodin)	Podpora na místě následující pracovní den (CZ+SK)	Snížená (retainer ceník)	Dva workshopy k přezkoumání Incident Mgmt & Architecture	Platforma pro komunikaci a výměnu dat	Kredit 5 dnů použitý na incident response nebo konzultace	Standardy kvality a zabezpečení (ISO 9001, 27001, TISAX)
Rapid CZK 63 800,- měsíčně	Vzdálená podpora do 1,5 hodiny (operace 24x7)	Pohotovostní podpora na místě do 12 hodin (CZ+SK)	Snížená (retainer ceník)	Stejné jako modul Readiness	Stejné jako modul Readiness	Kredit 15 dnů použitý na incident response nebo konzultace	Holistické znalosti z jednoho zdroje (právo, soukromí, krizové řízení, obchodní rizika)

*2 400 Kč za hovor v pracovní dny (pondělí – pátek 9-17 hodin) /3 400 Kč za hovor mimo pracovní dny.

Incident Response Retainer Model

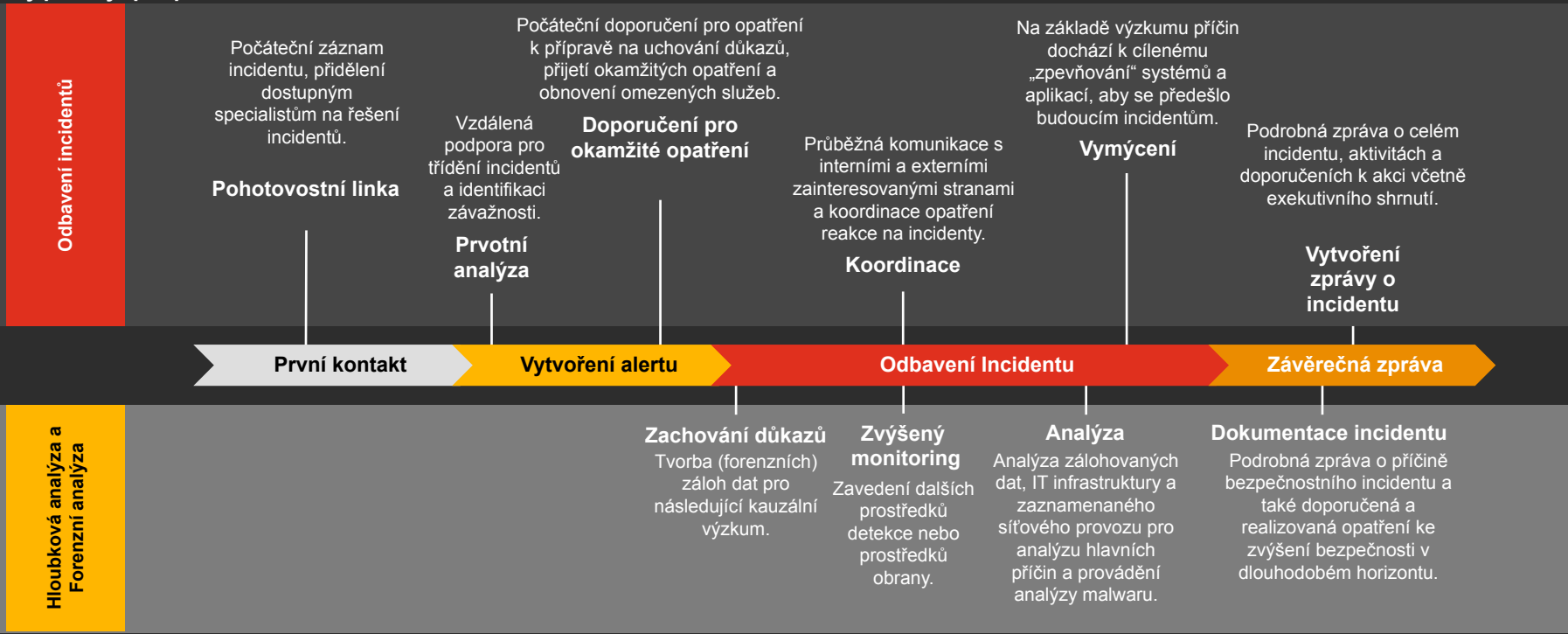
Rok bez významných incidentů

Podporujeme vás v udržitelném a neustálém zlepšování řízení vašich incidentů, abyste byli schopni optimálně reagovat na aktuální hrozby.



Cybersecurity Incident Response a Crisis Management naživo

Typický případ:

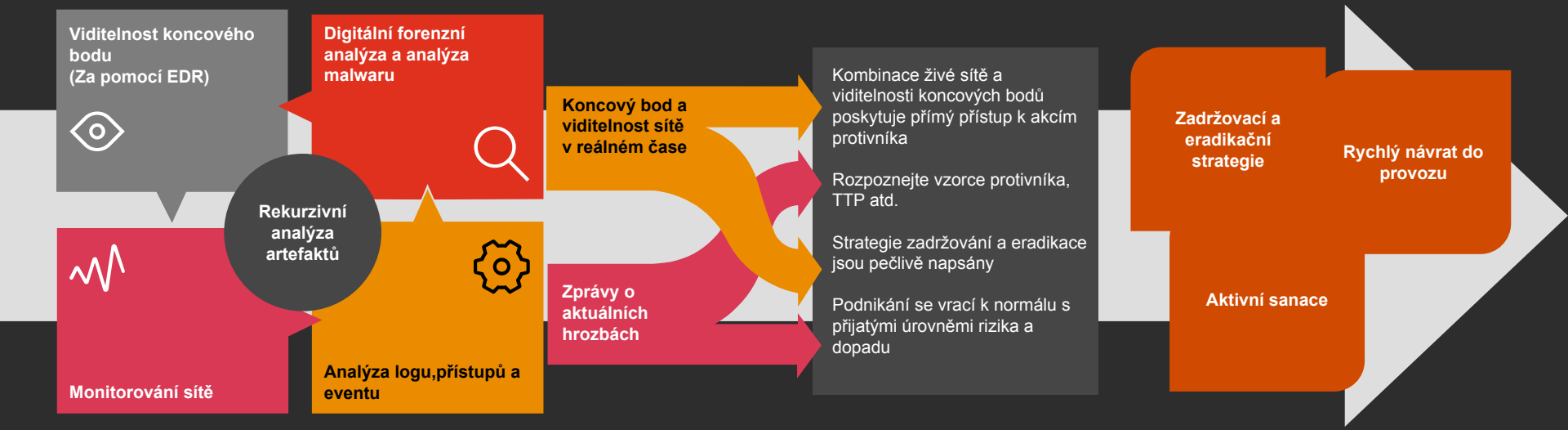


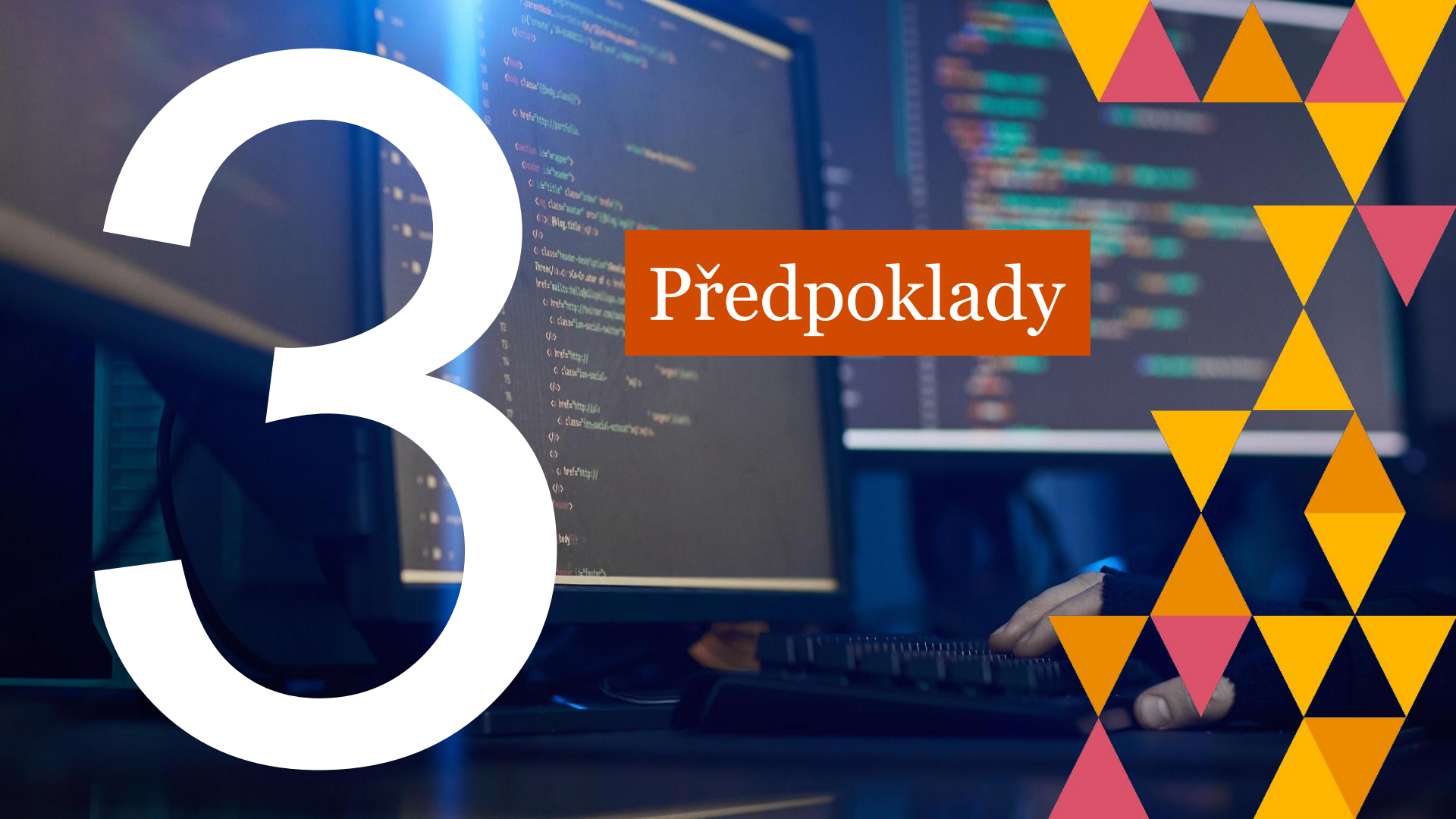
Incident Response technologie

Technická analýza, odezva a náprava

V případě incidentu vás plně podpoříme během reakce a obnovy, abychom minimalizovali a zmírnili poškození systémů a dat a minimalizovali obchodní riziko. Naše postupy jsou založeny na osvědčených průmyslových postupech a dlouholetých praktických zkušenostech. U „živého“ vyšetřování reakce na incidenty (např. narušení sítě) je naší obecnou praxí důsledně dodržovat standard NIST Computer Security Incident Handling a odchylovat se pouze tehdy, když víme, že je to nutné.

Naše technická analýza, reakce a nápravné činnosti jsou v souladu s vašimi procesy a postupy (tj. s plány řízení reakcí na kybernetické incidenty a krizového řízení kybernetické bezpečnosti).




3
Předpoklady

Předpoklady

Zaručujete, že máte všechna potřebná práva nebo souhlasy k tomu, abychom mohli pracovat a používat všechny takové systémy a informace v souvislosti s poskytováním služeb.

Souhlasíte s tím, že pokud neplníte své závazky a to ovlivní naši schopnost plnit naše závazky, jsme těchto závazků zproštěni.

Vaše povinnosti

Naše role je pouze poradní. Jste odpovědní za všechny řídící funkce a rozhodnutí související s touto zakázkou, včetně vyhodnocení rozsahu služeb a určení, zda splňují vaše potřeby. Jste také odpovědní za výsledky používání služeb nebo dodávek a za vytvoření a udržování vašich vnitřních kontrol. Vy určíte kompetentního člena vašeho vedení, který bude dohlížet na poskytované služby.

Pokud v souvislosti se službami používáte třetí strany, odpovídáte za uzavření smlouvy s nimi. Pokud se nedohodneme jinak, budete odpovědní za řízení těchto třetích stran a kvalitu jejich vstupů a práce.

Poskytnete nám:

- Přístup k vašim systémům a dalším nezbytným zdrojům, které přiměřeně potřebujeme k poskytování služeb;
- Přístup k, a podporu kvalifikovaných zaměstnanců; a
- Přesné, spolehlivé a včasné informace, které můžeme přiměřeně požadovat o vašich systémech, které potřebujeme k tomu, abychom mohli poskytovat služby;
- Budete zodpovědní za poskytování informací týkajících se stávajících zásad, plánů nebo postupů, IT a bezpečnostní infrastruktury a jakýchkoliv dalších informací, které potřebujeme k plnění našich úkolů. To bude zahrnovat také přístup k vašim pracovníkům, kteří jsou schopni poradit s architekturou sítě a systémů. Budete také zodpovědní za zajištění jakéhokoli přístupu požadovaného k systémům nebo IT prostředím třetích stran, abychom mohli plnit naše úkoly;
- Uvědomujete si, že dodání a provedení této služby je na vyžádání, na vyžádání bude určeno specifiky bezpečnostní události; a
- Přijmete, že provedení na dálku nebo na místě bude po dohodě odrážející aktuální případ potvrzené telefonickým hovorem a e-mailem.

Předpoklady

Počáteční přihlášení

Po dobu trvání smlouvy budeme každoročně provádět onboarding a koordinační schůzky.

Vstupní relace budou zahrnovat následující aktivity:

- Soupis technologií, procesů a řešení dostupných pro použití v krizovém managementu
- Diskuse s vámi na základě poskytnutého inventáře za účelem definování a poskytování přístupu k požadovaným řešením, která umožní našemu týmu reakce na incidenty
- Definice cílů úrovně služeb pro náš IR tým na základě
- Sladění našich plánů odezvy a stávajících procesů tak, aby byly v souladu s následujícími procesy:
  - Řízení reakce na incidenty v oblasti kybernetické bezpečnosti
  - Řízení krizových situací kybernetické bezpečnosti


4
Příklady
z praxe

Příklady Incident Response projektů

Typ zapojení	Anonymizovaný popis klienta	Klientská výzva	Co jsme udělali	Rok
Kompromitované jednotky (Compromised Breach)	**Global Fortune 500**	Klient měl velký bezpečnostní incident a chtěl ověřit, zda se nový útočník TTP během doby nezměnil.	Poskytli jsme službu zjišťování kompromitací, shromáždili a analyzovali shromážděná data z klientského prostředí a poskytli doporučení na nové detekce, které pomohly k odhalení velkého incidentu v létě 2020.	2020
Incident Response Retainer	**International Retail Chain**	Klient měl bezpečnostní incident související s ransomwarem od aktéra z DarkSide.	Podpořili jsme globální IR aktivity PwC a společně s forenzním týmem určili potenciálního pacienta nula. Provedli jsme bezpečnostní analýzu, která odhalila hlavní příčinu incidentu a pomohla s omezováním a nápravnými činnostmi.	2021
Globální SOC	**Global Fortune 500**	Průběžné monitorování klientského prostředí a pravidelná reakce na incidenty	Pro tohoto klienta poskytujeme služby bezpečnostního operačního centra již více než 3 roky a byli jsme součástí dvou velkých incidentů, do kterých byli zapojeni lidé ovládání útočníci. Podařilo se nám zastavit útočníky v dosažení jejich cílů, najít základní příčiny a pomoci s nápravnými činnostmi.	On-going