EVROPSKÁ UNIE
Evropský sociální fond
Operační program Zaměstnanost

Úřad práce ČR

příloha č.5 dohody č.:	**TAA-MN-2/2020**	POVEZ II (CZ.03.1.52/0.0/0.0/15_021/0000053)		Vzdělávací zařízení:	COMGUARD a.s., Sochorova 38, Brno, 616 00
Plán výuky				Jména lektorů:	xxxx
Zaměstnavatel:	BRISK Tábor a.s.	IČO:	47252090		
Název vzdělávací aktivity:	**Bezpečná IT infrastruktura**	**skupina**		Místo výuky:	BRISK Tábor a.s., Vožická 2068, Tábor, 390 02

PČ	Datum	Počet vyučovacích hodin	Od - do	probíraná témata
1	21.1.2020	8	8:30 - 17:00	**Školení COMGUARD - Bezpečná IT infrastruktura, kybernetické útoky (obecný úvod)** - ***Václav Štverka*** - Obecný popis bezpečné IT infrastruktury odolné proti kybernetickým útokům včetně její správy, jaké minimální a optimální vlastnosti má mít z pohledu zajištění informační bezpečnosti. / Koncept řešení infrastruktury s maximálním využitím produktů Windows Server 2016 (doména), Sophos a Eset a síťové infrastruktury (HP). / Hlavní typy kybernetických útoků (vnější i vnitřní nepřítel), preventivní obrana proti těmto útokům. / Obecný postup při jednotlivých typech kybernetických útoků (blokování útoku, okamžitá opatření), zajištění důkazů a vyšetření útoku včetně forezní analýzy.
2	22.1.2020	8	8:30 - 17:00	**Školení COMGUARD - Bezpečná IT infrastruktura, kybernetické útoky (obecný úvod)** - ***Václav Štverka*** - Obecný popis bezpečné IT infrastruktury odolné proti kybernetickým útokům včetně její správy, jaké minimální a optimální vlastnosti má mít z pohledu zajištění informační bezpečnosti. / Koncept řešení infrastruktury s maximálním využitím produktů Windows Server 2016 (doména), Sophos a Eset a síťové infrastruktury (HP). / Hlavní typy kybernetických útoků (vnější i vnitřní nepřítel), preventivní obrana proti těmto útokům. / Obecný postup při jednotlivých typech kybernetických útoků (blokování útoku, okamžitá opatření), zajištění důkazů a vyšetření útoku včetně forezní analýzy.
3	5.2.2020	8	8:30 - 17:00	**Školení COMGUARD - Bezpečná IT infrastruktura, kybernetické útoky (obecný úvod)** - ***Miloslav Urbiš*** - Obecný popis bezpečné IT infrastruktury odolné proti kybernetickým útokům včetně její správy, jaké minimální a optimální vlastnosti má mít z pohledu zajištění informační bezpečnosti. / Koncept řešení infrastruktury s maximálním využitím produktů Windows Server 2016 (doména), Sophos a Eset a síťové infrastruktury (HP). / Hlavní typy kybernetických útoků (vnější i vnitřní nepřítel), preventivní obrana proti těmto útokům. / Obecný postup při jednotlivých typech kybernetických útoků (blokování útoku, okamžitá opatření), zajištění důkazů a vyšetření útoku včetně forezní analýzy.
4	25.2.2020	8	8:30 - 17:00	**Školení COMGUARD - Doména Win Server 2016** - ***Radovan Šlechtický*** - Bezpečnostní politiky domény Win Server 2016, možnosti nastavení (zejm. s ohledem přechodu z Win Serveru 2008 na Win Server 2016), možnosti šifrování. / Praktická část, v rámci které se prověří bezpečnostní nastavení domény, na základě poznatků ze školení navrhnou účastníci školení případné změny nastavení, návrh zkonzultují s lektorem. / Důraz na monitorování systému, posouzení vhodnosti logů pro konkrétní sledování (podklad pro stanovení požadavků na systém Log management), uchování logů popř. jejich obnova, práce s logy při kontrole aktivit uživatelů i správců, notifikace a jejich nastavení.
5	26.2.2020	8	8:30 - 17:00	**Školení COMGUARD - Doména Win Server 2016** - ***Radovan Šlechtický*** - Bezpečnostní politiky domény Win Server 2016, možnosti nastavení (zejm. s ohledem přechodu z Win Serveru 2008 na Win Server 2016), možnosti šifrování. / Praktická část, v rámci které se prověří bezpečnostní nastavení domény, na základě poznatků ze školení navrhnou účastníci školení případné změny nastavení, návrh zkonzultují s lektorem. / Důraz na monitorování systému, posouzení vhodnosti logů pro konkrétní sledování (podklad pro stanovení požadavků na systém Log management), uchování logů popř. jejich obnova, práce s logy při kontrole aktivit uživatelů i správců, notifikace a jejich nastavení.
6	25.3.2020	8	8:30 - 17:00	**Školení COMGUARD - Doména Win Server 2016** - ***Radovan Šlechtický*** - Bezpečnostní politiky domény Win Server 2016, možnosti nastavení (zejm. s ohledem přechodu z Win Serveru 2008 na Win Server 2016), možnosti šifrování. / Praktická část, v rámci které se prověří bezpečnostní nastavení domény, na základě poznatků ze školení navrhnou účastníci školení případné změny nastavení, návrh zkonzultují s lektorem. / Důraz na monitorování systému, posouzení vhodnosti logů pro konkrétní sledování (podklad pro stanovení požadavků na systém Log management), uchování logů popř. jejich obnova, práce s logy při kontrole aktivit uživatelů i správců, notifikace a jejich nastavení.
7	21.4.2020	8	8:30 - 17:00	**Školení COMGUARD - SOPHOS XG (NGFW)** - ***Jan Burian*** - Správa zařízení Sophos XG, nové funkce. / Bezpečnostní nastavení zařízení (praktická část, v rámci které se projdou veškerá nastavení FW včetně seznámení s účelem nastavení, možnými variantami nastavení, jak toto nastavení ovlivní odolnost či zranitelnost infrastruktury). Zaměřit se na i na opatření snižující únik dat ze společnosti (např. blokování webových kategorií, způsoby pořizování výjimek; neblokovat celý instant messaging, ale pouze odesílání souborů, pokud je to technicky možné; povolení pouze konkrétních úložišť externích stran). / Na základě této praktické části navrhnou účastníci školení případné úpravy nastavení, proběhne konzultace s lektorem a pod jeho dohledem proběhne nastavení (v případě potřeby schválení nových politik vedením proběhne tato část až s časovým odstupem potřebným pro vyjádření vedení). / Logování zařízení popř. reporting, kontrola a prověřování bezpečnostních událostí, konkrétní postup v případě hlavních typů kybernetických útoků, možnosti monitoringu uživatelů i správců. / DLP na Sophos (doporučení k nastavení pravidel, praktické nastavení alespoň 4 pravidel). / SPX šifrování e-mailů, možnosti jeho nastavení s DLP Sophos i bez DLP, praktické nastavení a otestování.

PČ	Datum	Počet vyučovacích hodin	Od - do	probíraná témata
8	22.4.2020	8	8:30 - 17:00	**Školení COMGUARD - SOPHOS XG (NGFW)** - ***Jan Burian*** - Správa zařízení Sophos XG, nové funkce. / Bezpečnostní nastavení zařízení (praktická část, v rámci které se projdou veškerá nastavení FW včetně seznámení s účelem nastavení, možnými variantami nastavení, jak toto nastavení ovlivní odolnost či zranitelnost infrastruktury). Zaměřit se na i na opatření snižující únik dat ze společnosti (např. blokování webových kategorií, způsoby pořizování výjimek; neblokovat celý instant messaging, ale pouze odesílání souborů, pokud je to technicky možné; povolení pouze konkrétních úložišť externích stran). / Na základě této praktické části navrhnou účastníci školení případné úpravy nastavení, proběhne konzultace s lektorem a pod jeho dohledem proběhne nastavení (v případě potřeby schválení nových politik vedením proběhne tato část až s časovým odstupem potřebným pro vyjádření vedení). / Logování zařízení popř. reporting, kontrola a prověřování bezpečnostních událostí, konkrétní postup v případě hlavních typů kybernetických útoků, možnosti monitoringu uživatelů i správců. / DLP na Sophos (doporučení k nastavení pravidel, praktické nastavení alespoň 4 pravidel). / SPX šifrování e-mailů, možnosti jeho nastavení s DLP Sophos i bez DLP, praktické nastavení a otestování.
9	26.5.2020	8	8:30 - 17:00	**Školení COMGUARD - SOPHOS XG (NGFW)** - ***Jan Burian*** - Správa zařízení Sophos XG, nové funkce. / Bezpečnostní nastavení zařízení (praktická část, v rámci které se projdou veškerá nastavení FW včetně seznámení s účelem nastavení, možnými variantami nastavení, jak toto nastavení ovlivní odolnost či zranitelnost infrastruktury). Zaměřit se na i na opatření snižující únik dat ze společnosti (např. blokování webových kategorií, způsoby pořizování výjimek; neblokovat celý instant messaging, ale pouze odesílání souborů, pokud je to technicky možné; povolení pouze konkrétních úložišť externích stran). / Na základě této praktické části navrhnou účastníci školení případné úpravy nastavení, proběhne konzultace s lektorem a pod jeho dohledem proběhne nastavení (v případě potřeby schválení nových politik vedením proběhne tato část až s časovým odstupem potřebným pro vyjádření vedení). / Logování zařízení popř. reporting, kontrola a prověřování bezpečnostních událostí, konkrétní postup v případě hlavních typů kybernetických útoků, možnosti monitoringu uživatelů i správců. / DLP na Sophos (doporučení k nastavení pravidel, praktické nastavení alespoň 4 pravidel). / SPX šifrování e-mailů, možnosti jeho nastavení s DLP Sophos i bez DLP, praktické nastavení a otestování.
10	30.6.2020	8	8:30 - 17:00	**Školení COMGUARD - SOPHOS Ochrana koncových stanic** - ***Radek Kugler*** - Sophos NexGen Endpoint, synchronizovaná bezpečnost mezi koncovými zařízeními a perimetrem, seznámení s možnostmi tohoto řešení, výhody synchronizovaného řešení při jednotlivých typech kybernetických útoků popř. pro snížení rizika úniku dat ze strany zaměstnanců. / DLP a šifrování na koncových stanicích. / Otestování produktu, nastavení produktu, a seznámení se s možnostmi synchronizované bezpečnosti a správy celého řešení. / Logování popř. reporting, kontrola a prověřování bezpečnostních událostí, konkrétní postup v případě hlavních typů kybernetických útoků, možnosti monitoringu uživatelů i správců. / Základní seznámení s řešením pro zabezpečení mobilních zařízení od Sophos. / Rámcové srovnání s produkty ESET s ohledem na možný souběh obou řešení: - Seznámení s možnostmi bezpečnostního řešení ESET ve vztahu k SOPHOSu, včetně praktického doporučení nastavení (koncové stanice, mobilní zařízení), možnosti šifrování ESET. - Porovnání správy a bezpečnostních vlastností produktů ESET i Sophos s ohledem na možný souběh obou řešení.
11	1.7.2020	8	8:30 - 17:00	**Školení COMGUARD - SOPHOS Ochrana koncových stanic** - ***Radek Kugler*** - Sophos NexGen Endpoint, synchronizovaná bezpečnost mezi koncovými zařízeními a perimetrem, seznámení s možnostmi tohoto řešení, výhody synchronizovaného řešení při jednotlivých typech kybernetických útoků popř. pro snížení rizika úniku dat ze strany zaměstnanců. / DLP a šifrování na koncových stanicích. / Otestování produktu, nastavení produktu, a seznámení se s možnostmi synchronizované bezpečnosti a správy celého řešení. / Logování popř. reporting, kontrola a prověřování bezpečnostních událostí, konkrétní postup v případě hlavních typů kybernetických útoků, možnosti monitoringu uživatelů i správců. / Základní seznámení s řešením pro zabezpečení mobilních zařízení od Sophos. / Rámcové srovnání s produkty ESET s ohledem na možný souběh obou řešení: - Seznámení s možnostmi bezpečnostního řešení ESET ve vztahu k SOPHOSu, včetně praktického doporučení nastavení (koncové stanice, mobilní zařízení), možnosti šifrování ESET. - Porovnání správy a bezpečnostních vlastností produktů ESET i Sophos s ohledem na možný souběh obou řešení.
12	12.8.2020	8	8:30 - 17:00	**Školení COMGUARD - SOPHOS Ochrana koncových stanic** - ***Radek Kugler*** - Sophos NexGen Endpoint, synchronizovaná bezpečnost mezi koncovými zařízeními a perimetrem, seznámení s možnostmi tohoto řešení, výhody synchronizovaného řešení při jednotlivých typech kybernetických útoků popř. pro snížení rizika úniku dat ze strany zaměstnanců. / DLP a šifrování na koncových stanicích. / Otestování produktu, nastavení produktu, a seznámení se s možnostmi synchronizované bezpečnosti a správy celého řešení. / Logování popř. reporting, kontrola a prověřování bezpečnostních událostí, konkrétní postup v případě hlavních typů kybernetických útoků, možnosti monitoringu uživatelů i správců. / Základní seznámení s řešením pro zabezpečení mobilních zařízení od Sophos. / Rámcové srovnání s produkty ESET s ohledem na možný souběh obou řešení: - Seznámení s možnostmi bezpečnostního řešení ESET ve vztahu k SOPHOSu, včetně praktického doporučení nastavení (koncové stanice, mobilní zařízení), možnosti šifrování ESET. - Porovnání správy a bezpečnostních vlastností produktů ESET i Sophos s ohledem na možný souběh obou řešení, závěrečný pohovor

Vyplňte pouze bílá pole

Datum:	20.1.2020	jméno, příjmení, funkce a podpis oprávněné osoby	
Vyřizuje:	xxx		(razítko)
Číslo telefonu:	xxx		
Email:	xxx	xxx	