SandBlast Zero-Day Protection – Workshop (jednodňový kurz)

BUĎTE O KROK NAPRED PRED NEZNÁMYMI HROZBAMI

Zero-day a APT používajú moment prekvapenia aby obišli tradičné bezpečnostné riešenia, čo spôsobuje ťažkosti pri ochrane proti nim a zvýšenú obľúbenosť u útočníkov. Tradičný sandboxing bol navrhnutý pre ochranu proti týmto typom hrozieb, ale útočníci vylepšili svoje postupy vytvorením malvéru, ktorý sa dokáže vyhnúť detekcii na mnohých sandboxoch. Výsledkom je, že veľa firiem musí odstraňovať následky napadnutia malvérom, namiesto ich zabráneniu už v zárodku.

Byť o krok vpred znamená, že firmy potrebujú mnohostrannú prevenčnú stratégiu, ktorá kombinuje proaktívnu ochranu eliminujúcu hrozby predtým ako sa dostanú k používateľom a súčasnú pokročilú CPU-level detekciu exploitov odhaľujúcu aj tie najskrytejšie hrozby.

CIEĽ KURZU:

Poskytnúť pochopenie základných konceptov a schopností potrebných na konfiguráciu a implementáciu Check Point SandBlast technológie.

HLAVNÉ TÉMY KURZU

- Anatómia hrozby
- SandBlast Threat Emulation
- SandBlast Threat Extraction
- ThreatCloud Emulation Service
- Scenáre nasadenia
- SandBlast Troubleshooting

PRAKTICKÉ CVIČENIA

Pochopenie zraniteľností

- Zoznámenie sa so softvérovými zraniteľnosťami.
- Ako porozumieť CVSS skóre pre zraniteľnosti.
- Pozrite sa na to ako malvér môže obísť sandbox.

Práca s Threat Emulation

- Aktivujte lokálnu emuláciu a pripravte systém pre emuláciu súborov.
- Použite príkazový riadok na emuláciu súborov z lokálneho súborového systému.
- Pozrite si logy Threat Emulation pomocou SmartView Trackera.
- Pozrite si a vytvorte hlásenie pomocou SmartEvent.
- Overte, že security gateway funguje ako MTA.

Práca s Threat Extraction

- Aktivujte Threat Extraction na security gateway s nastavenou MTA funkciou.
- Overte ako Threat Extraction dokáže doručiť bezpečný obsah.

Práca s ThreatCloud

- Zistite ako nakonfigurovať security gateway, aby emulácia prebiehala v ThreatCloud.
- Prezrite forenzné hlásenie.

CIELE KURZU

Anatómia hrozby

- Prediskutovať súčasné hrozby a bezpečnostné výzvy.
- Pochopiť komponenty útoku.
- Poučiť sa o tom ako útočníci obchádzajú tradičné bezpečnostné metódy.
- Pochopiť CPU a OS-level sandbox technológie.

SandBlast Threat Emulation

- Identifikovať rôzne komponenty SandBlast Zero-Day.
- Prediskutovať rôzne emulačné procesy a mechanizmy.
- Pochopiť tri spôsoby nasadenia emulácie súborov.

SandBlast Threat Extraction

- Pochopiť ako SandBlast Zero-Day Protection chráni firmy pred hrozbami vďaka Threat Extraction.
- Poučiť sa o základných nastaveniach a konfiguráciach pre Threat Extraction.

ThreatCloud Emulation Service

- Poučiť sa o tom ako funguje emulácia súborov v ThreatCloud.
- Prediskutovať rôzne komponenty ThreatCloud.

Scenáre nasadenia

- Poučiť sa o rôznych scenároch nasadenia SandBlast Zero-Day Protection.
- Pochopiť ako systémoví administrátori môžu využiť lokálnu emuláciu alebo ThreatCloud v rôznych situáciach.

SandBlast Troubleshooting

- Identifikovať základné nástroje príkazovej konzoly pre monitorovanie Threat Emulation a Threat Extraction.
- Poučiť sa o tom ako riešiť problémy s výkonom Threat Emulation a Threat Extraction.