Uživatelská příručka programu Exploite Guardian

v. 1.0

Úvod

Exploite Guardian je Windows aplikace určená pro ochranu stanic a serverů před malwarovými a hackerskými útoky. Aplikace obsahuje tři moduly:

- klientská část - slouží pro detekci událostí a jejich reportů uživateli počítače prostřednictvím aplikačního uživatelského rozhraní;
- Management server část – shromažďuje a zpracovává informace o událostech ze stanic v síti;
- centrální administrační konzole – zobrazuje události detekované na stanicích v síti bezpečnostnímu správci sítě pomocí webového grafického rozhraní.

Všechny komponenty se instalují pomocí společného instalačního wizardu.

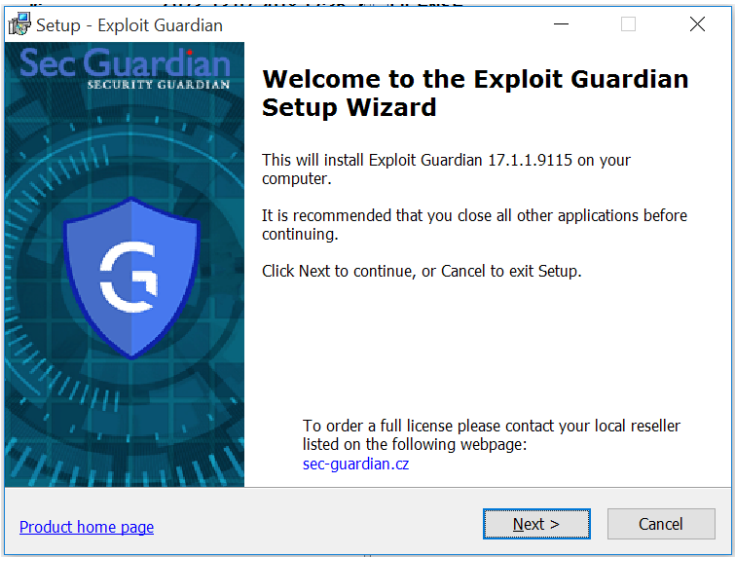
Systémové požadavky

- Windows Vista (any edition, 32 or 64 bit)/Windows 7 (32/64 bit), Windows 8, 8.1 (32/64 bit), Windows 10 (32/64 bit), Windows server 2008, Windows server 2008 R2, Windows server 2012, Windows server 2016.
- 512 MB RAM
- 300 MB diskového prostoru pro instalacina pracovní stanici a server, 500 MB pro instalaci Management serveru.

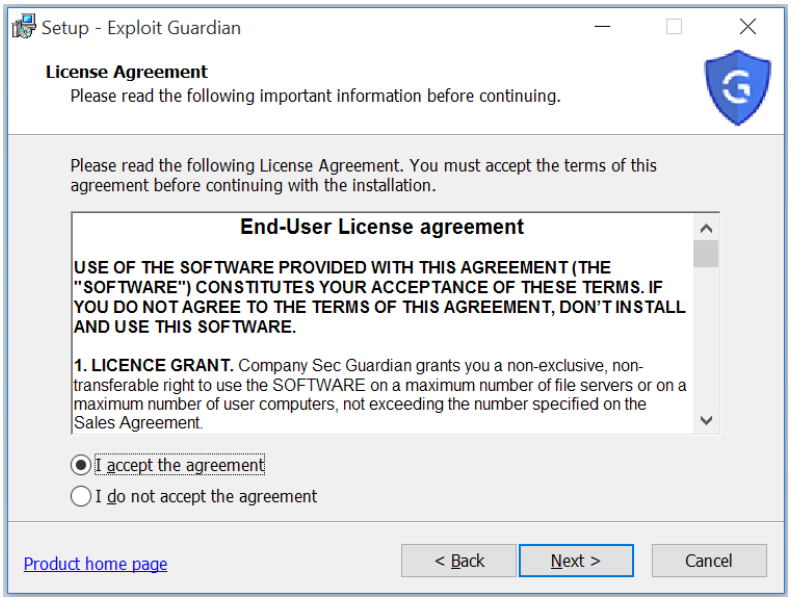
Instalace

Aplikaci nainstalujete pomocí následujících kroků:

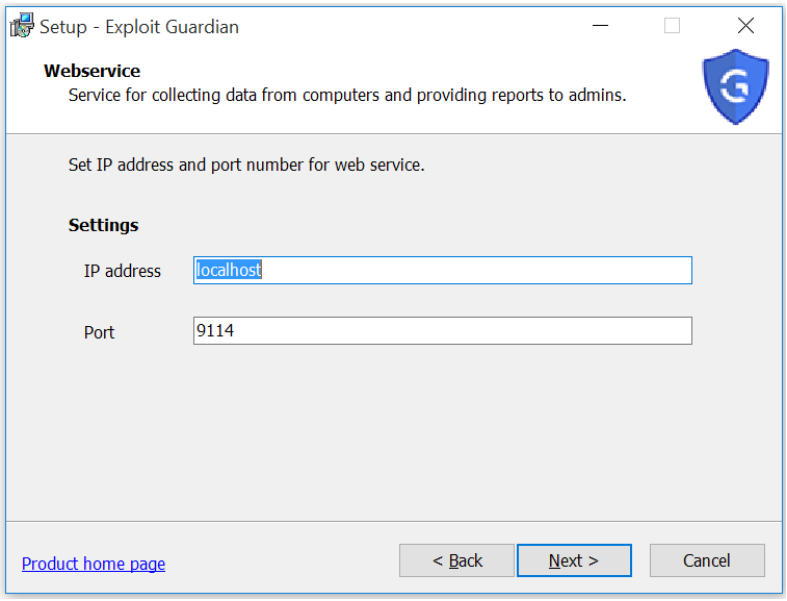
- Po spuštění instalačního wizardu aplikace můžete být vyzvání pomocí Windows funkce „User Account Control“ k povolení spuštění instalačního wizardu.
- Úvodní obrazovka instalačního wizardu vyžaduje potvrzení stisknutím tlačítka Next.



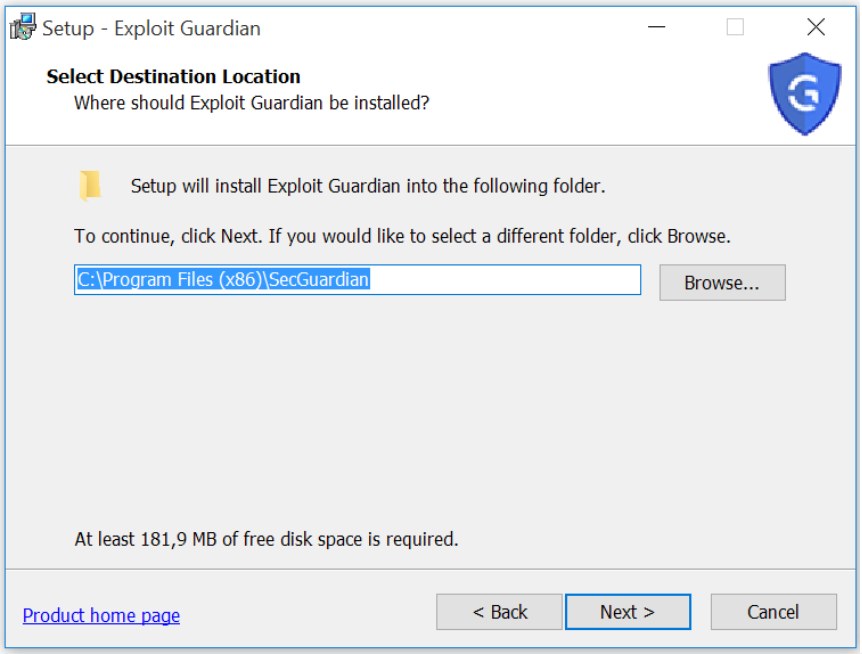
- Po odsouhlasení licenčního ujednání stiskněte tlačítko „I accept the agreement“.



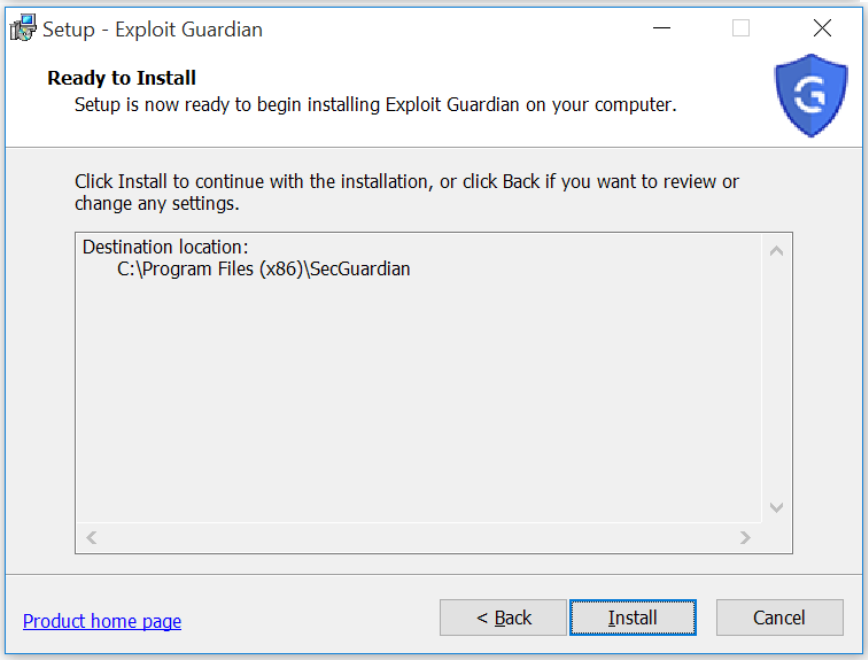
- V následujícím kroku instalačního wizardu nastavte IP adresu a port Management serveru, pokud jej chcete využívat pro správu eventů v síti. V případě individuální instalace ponechte přednastavené hodnoty.



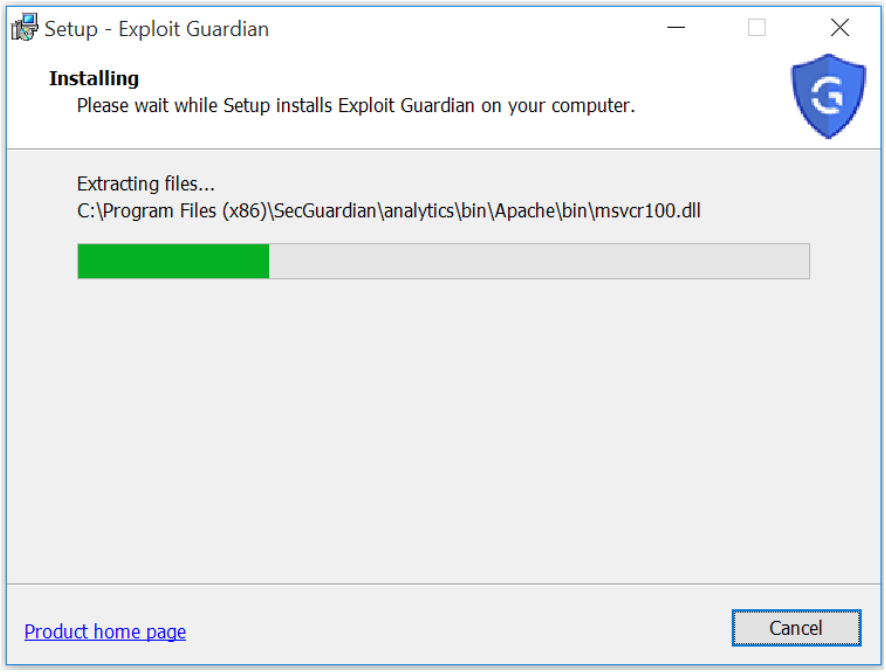
- Výběrem adresáře kam bude umístěna instalace Exploit Guardianu pomocí tlačítka „Browse…“



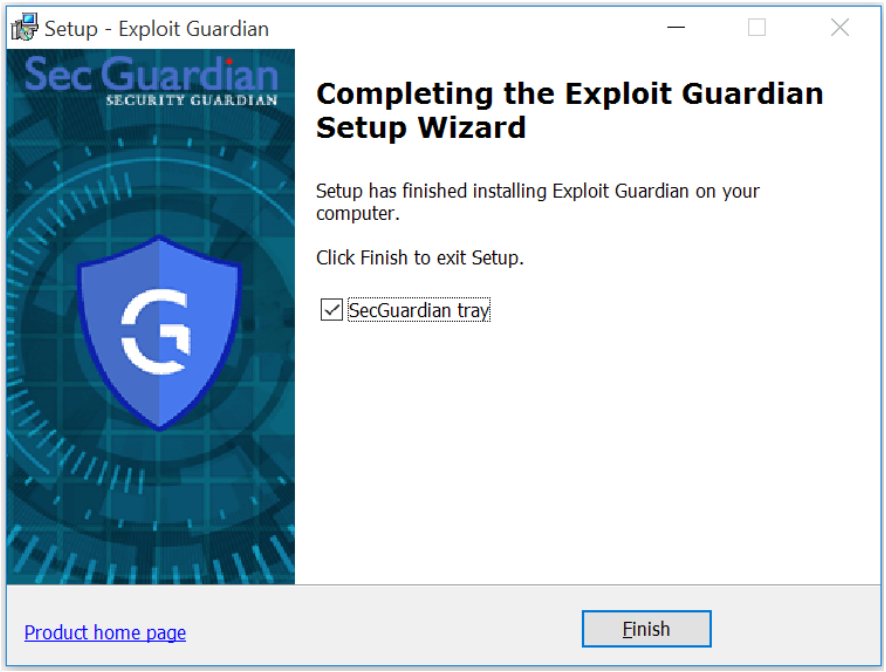
a potvrzením stisknutím tlačítka „Next“ se zobrazí potvrzení s nastavením instalace:



- Stisknutím tlačítka „Install“ se spustí vlastní instalace do Vašeho počítače.
- Ta rozbalí instalační soubory a umístí do vybraného adresáře



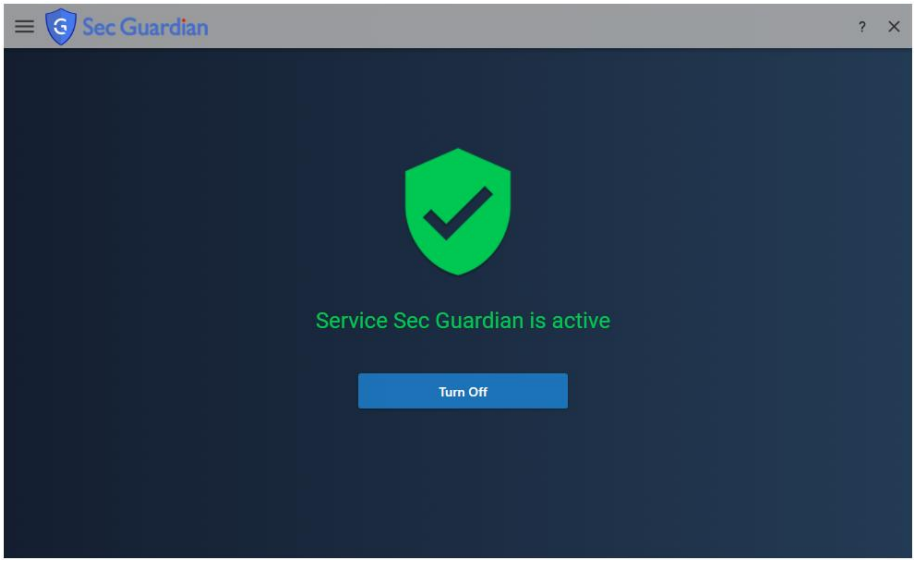
- Instalaci dokončíte stisknutím tlačítka „Finish“ a potvrzením instalace ikony produktu do Windows ovládací lišty (Systray) s restartem počítače.



- Po instalaci se zobrazí ve Windows ovládací liště modrá ikona Exploit Guardienu.
-

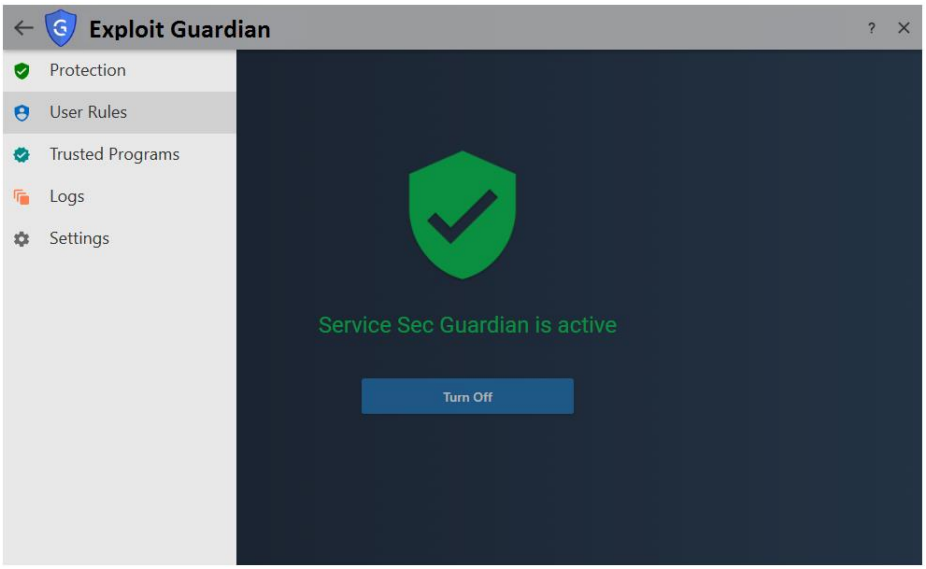
Exploit Guardian pro pracovní stanice

Po instalaci aplikace se zobrazí v ovládací liště Windows modrá ikona pomocí které může uživatel aplikaci konfigurovat. Kliknutím na ikonu se zobrazí uživatelské rozhraní:



Tlačítlo uprostřed dashboardu Turn On/Turn Off slouží k rychlému zapnutí nebo vypnutí běhu programu Exploit Guardian.

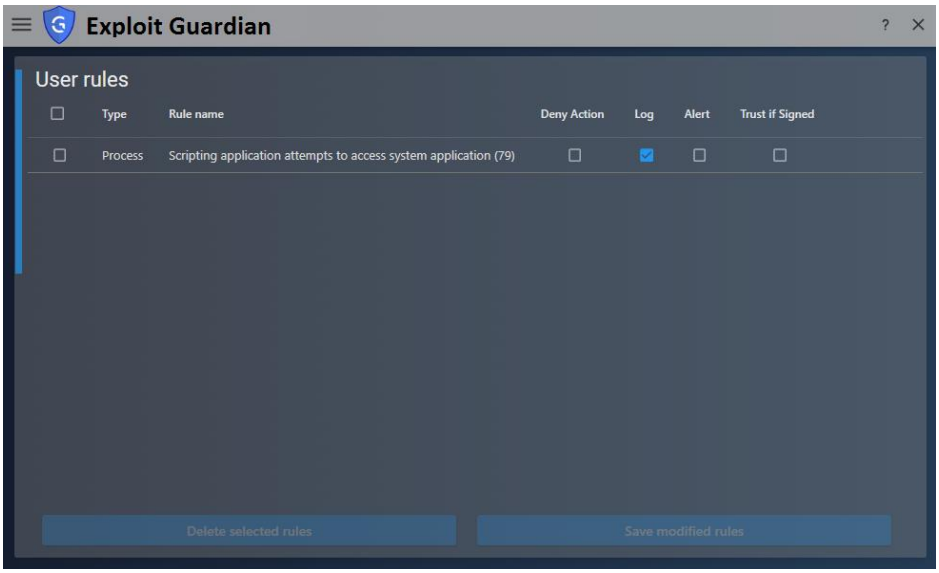
Stisknutím ikony v levém horním rohu dashboardu se otevře menu aplikace.



Záložka:

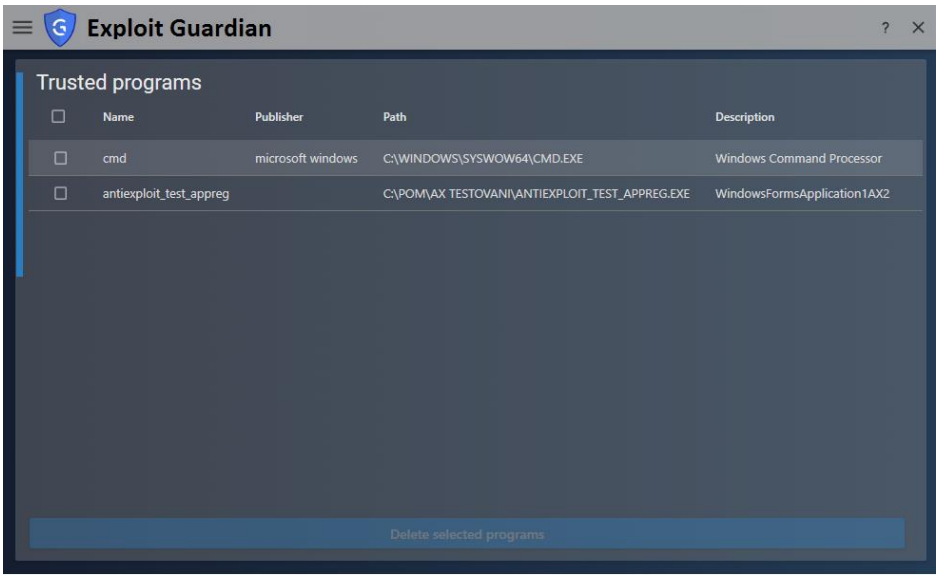
- **Protection** - zobrazuje dashboard programu.
- **User Rules** – umožňuje uživateli upravovat detekční metody, automaticky vytvořené uživatelem při definici parametrů detekované události v zobrazeném alertu. Uživatel může měnit položky:
    - **Deny Action**
    - **Log**
    - **Alert**
    - **Trust if Signed**

Po ukončení úprav jednotlivých pravidel je třeba je uložit pomocí tlačítka “Save modified rules”. Označená pravidla je možné odstranit pomocí tlačítka “Delete selected rules”.



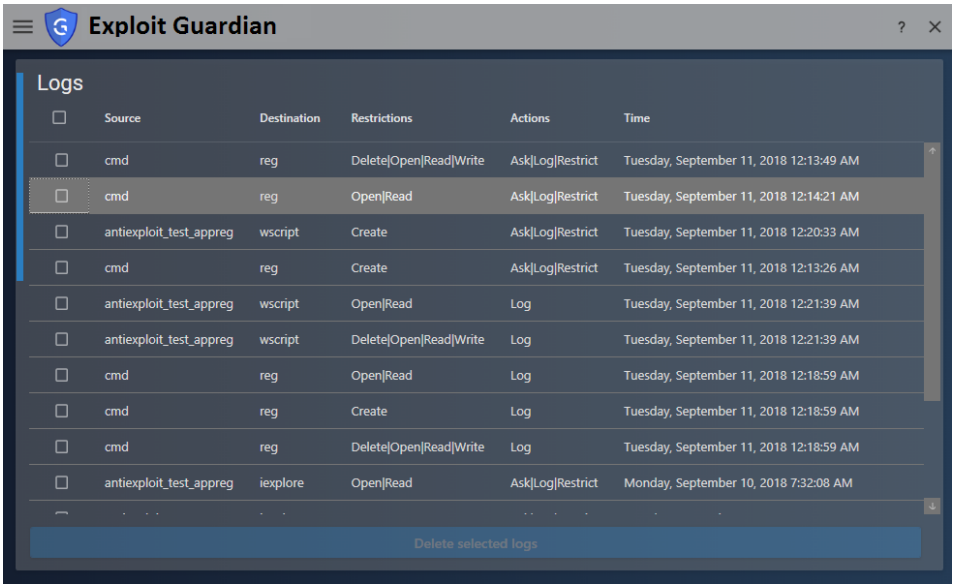
- **Trusted Programs** – vypíše seznam aplikací, které nebudou kotrolovány žádnou detekční metodou
    - **Name** – jméno aplikace
    - **Publisher** – jméno vydavatele, je-li známé
    - **Path** – cesta, kde je aplikace uložena
    - **Description** – detailnější informace o plikaci

Označené aplikace lze odstranit ze seznamu pomocí tlačítka “Delete selected program”.



- **Logs** – umožňuje uživateli zobrazit obsah log souboru detekovaných událostí. Vybrané položky log souboru lze vymazat pomocí tlačítka “Delete selected logs”. Každá ze zobrazených položek obsahuje informace o:
    - **Source** - jméno aplikace, která incident vyvolala
    - **Destination** - jméno aplikace, na kterou incidicent mířil, zápis do registru Windows je pojmenovaný “reg”
    - **Restriction** – jakou operaci se zdrojová aplikace pokusila vykonat:
        - **Create**
        - **Open**
        - **Read**
        - **Write**
        - **Open**
        - **Delete**

- **Action** - jaké opatření Exploit Guardian provedl:
  - **Ask** - uživateli se zobrazil dialog box s detaily detekované události
  - **Log** – událost byla zalogována
  - **Restrict** – aktivita zdrojové aplikace nebyla povolena
- **Time** – časová značka detekované události

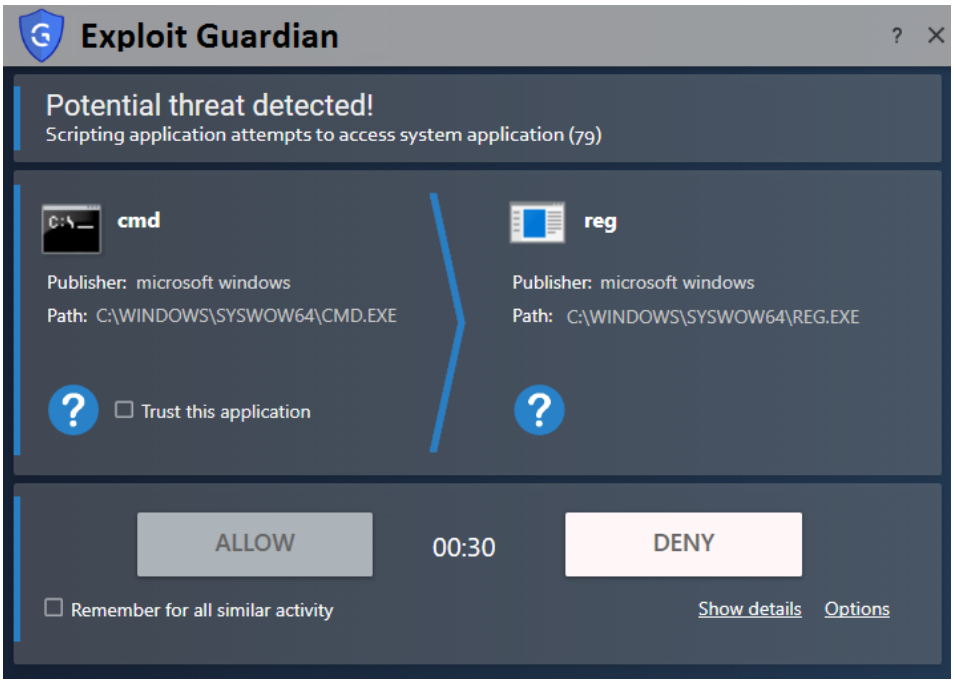


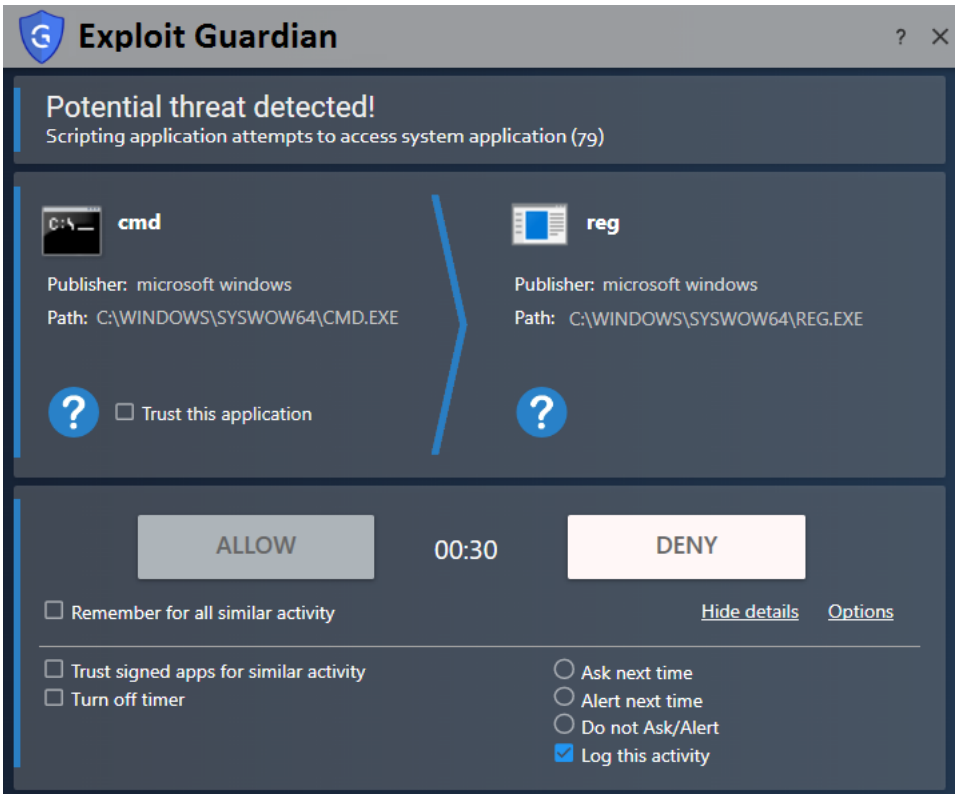
- **Settings** – slouží pro nastavení program Exploit Guardian s individuálními nastaveními:
  - **Exploit Guardian service** – umožňuje zapnutí/vypnutí ochrany
  - **Silent mode** – zapíná/vypíná zobrazení alertů, uživatelských hlášení detekovaných incidentů s možností volby reakce na detekovanou událost. Pokud je „Silent mod“ zapnutý, jsou všechny detekce pouze logovány do log souborů
  - **Display alert messages** – při zapnutém Silent módu zobrazuje v uživatelském rozhraní alerty. Uživatel ale nemá v tomto případě možnost reagovat na zobrazenou událost
  - **Exploit Guardian Updates** – zapíná/vypíná automatické aktualizování detekčních pravidel se serveru výrobce
  - **Exploit Guardian is up to date** – stavová ikona zobrazující zda je aplikace s aktuálními aktualizacemi
  - **Version** – verze aplikace.

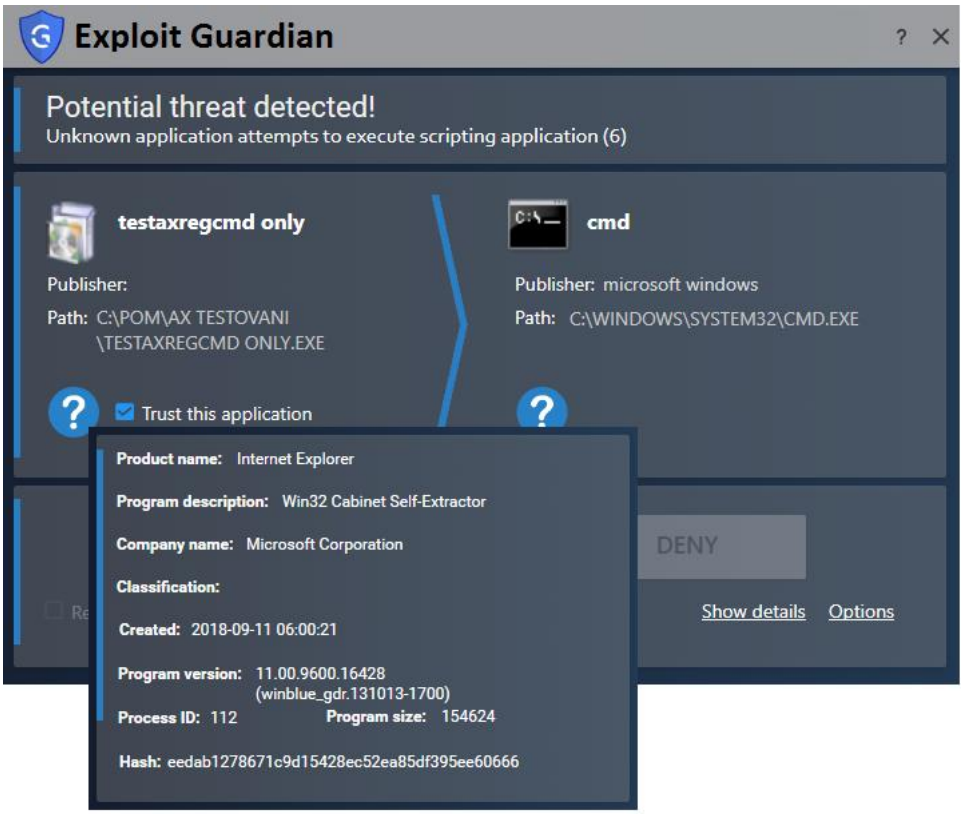
Menu “Get help” a “Report an issue” nabízí uživateli zobrazení nápovědy a možnost zaslat výrobci informace o chybě program, případně dotaz na product pomocí emailu.

Alerty

Klientská část aplikace Exploit Guardian při detekci události může volitelně zaznamenat informace o události do log souboru, odeslat do Management konzole k analýze bezpečnostnímu správci sítě nebo uživateli počítače zobrazit informační okno s informacemi o události - alert okno.




Exploit Guardian
Potential threat detected!
Scripting application attempts to access system application (79)
cmd
Publisher: microsoft windows
Path: C:\WINDOWS\SYSWOW64\CMD.EXE
Trust this application
reg
Publisher: microsoft windows
Path: C:\WINDOWS\SYSWOW64\REG.EXE
ALLOW
00:30
DENY
Remember for all similar activity
Hide details
Options
Trust signed apps for similar activity
Turn off timer
Ask next time
Alert next time
Do not Ask/Alert
Log this activity


Exploit Guardian
Potential threat detected!
Unknown application attempts to execute scripting application (6)
testaxregcmd only
Publisher:
Path: C:\POM\AX TESTOVANI
\TESTAXREGCMD ONLY.EXE
Trust this application
cmd
Publisher: microsoft windows
Path: C:\WINDOWS\SYSTEM32\CMD.EXE
Product name: Internet Explorer
Program description: Win32 Cabinet Self-Extractor
Company name: Microsoft Corporation
Classification:
Created: 2018-09-11 06:00:21
Program version: 11.00.9600.16428
(winblue_gdr.131013-1700)
Process ID: 112
Program size: 154624
Hash: eedab1278671c9d15428ec52ea85df395ee60666
DENY
Show details
Options

Ovládací konzole TrustPort Management

Aplikace TrustPort Management se ovládá pomocí tenkého klienta - konzole. Tímto tenkým klientem může být téměř jakýkoliv webový prohlížeč např. Microsoft Internet Explorer nebo Firefox. Tímto tenkým klientem se správce připojí na počítač, kde je nainstalován server TrustPort Management s webovým serverem pro ovládání centrální správy. Výhodou tenkého klienta je dostupnost služby z kteréhokoli počítače nebo tabletu, nezávisle na operačním systému a to že není třeba instalovat na stanici správce centrální správy žádné další programové vybavení. Stačí mu obyčejný webový prohlížeč, který je předinstalovaný na všech počítačích.

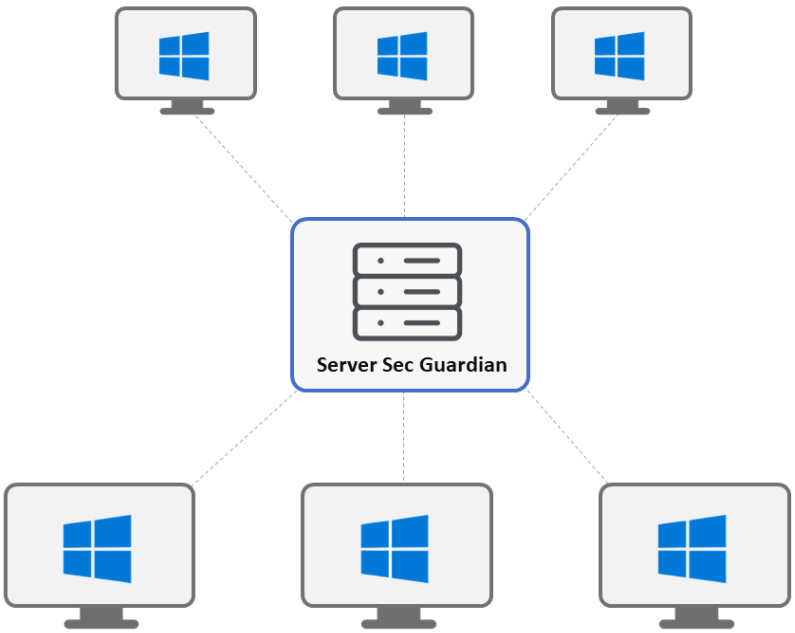
Optimální rozlišení obrazovky pro správu pomocí Ovládací konzole TrustPort Management je 1024x768 pixelů.

Řešení Exploit Guardian monitoruje chování spouštěných programů na počítači s cílem detekovat neobvyklé chování, které může indikovat útok malware nebo hackera. V podstatě se jedná o vytvoření obsluhy základních systémových operací, např. otevírání souborů, spouštění procesů, zápis do registrů a přístup do sítě. Podle nastaveného režimu je toto podezření na útok buď reportováno nebo je podezřelý proces zablokován před tím, než stačí vykonat svoji aktivitu.

Zaznamenání událostí se provádí takovým způsobem, aby bylo možné jednoduše dohledat směr útoku a s ním související informace, které byly během provedení útoku zaznamenány a slouží pro jeho analýzu administrátorem systému.

Management server

Incidenty nalezené na koncových stanicích jsou zasílány do Management serveru, který slouží k jejich remediaci a vyhodnocení rizikovosti sítě administrátorovi nebo SOC operátorovi.

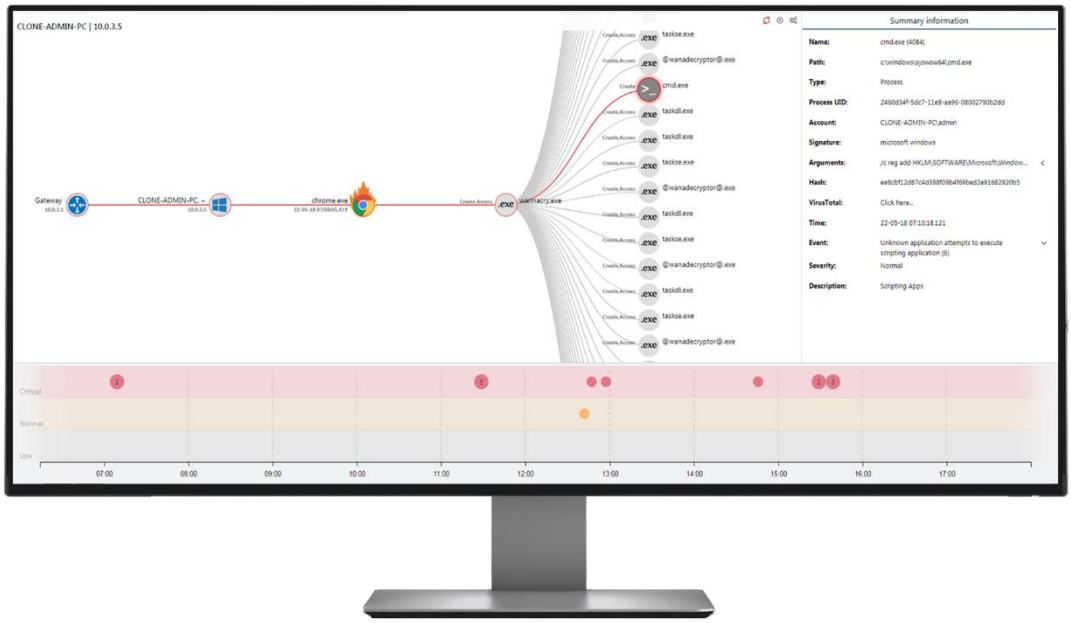


Pro správu incidentů detekovaných aplikací Exploit Guardian ve firemních prostředích je využíván Management server, který přijímá informace o incidentech a návazných informacích

ze stanic, koreluje informace podle nadefinovaných vektorů útoků a poskytuje předzpracované informace bezpečnostním správcům s cílem zpřehlednit stav bezpečnosti na síti a ušetřit čas při analýze bezpečnostních událostí. Příkladem může být automatické vyhledání stanic se stejným bezpečnostním incidentem v síti. Poskytuje přehledně informaci o rozšíření malware v síti a bezpečnostním kontextu pro rychlou reakci. Návazné uložené informace pak pomohou administrátorovi zjistit detaily o incidentech a jejich příčinách bez nutnosti fyzické přítomnosti u problematických koncových zařízení v síti.

Analýza útoků

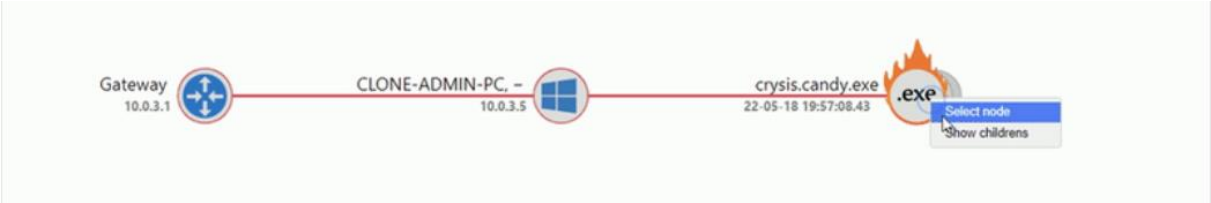
Vytvoření komplexního přehledu o nebezpečných aktivitách procesů a jimi ovlivněných aktivitách



Webová aplikace nabízí inteligentní rozhraní, které se jednoduše ovládá, je dynamické a skládá se ze třech hlavních komponent, kde každá se stará o konkrétní funkci. První komponenta zastupuje časovou osu, na které jsou vzniklé incidenty tříděny podle jejích závažnosti a času. Druhá komponenta představuje graf reprezentující vývoj útoku na koncové stanice. Třetí komponenta tvoří informační panel poskytující informace o zvoleném incidentu a zprostředkovává přístup k službám jako jsou VirusTotal a IP Geolocation.

Vizualizace síťové hierarchie

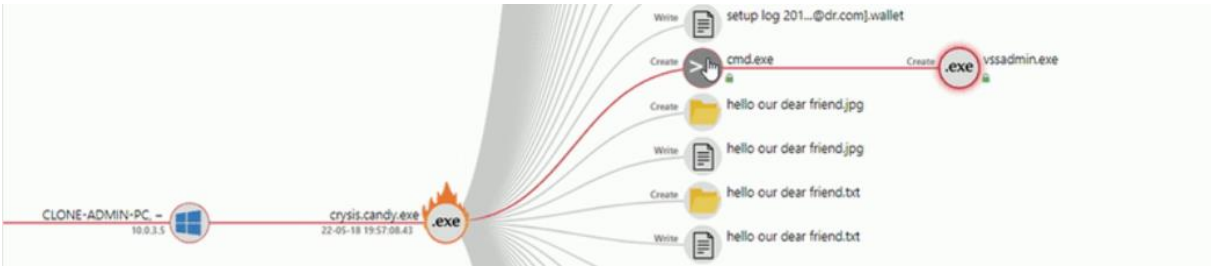
Řešení Sec Guardian poskytuje uživateli zobrazení koncové stanice v síťové struktuře



Z důvodu lepší orientace v topologii chráněné infrastruktury byla informace o vzniklém útoku navíc rozšířena o informace o koncové stanici a výchozí bráně. Každý strom útoku ve svém kořeni obsahuje element zastupující výchozí bránu a všechny s ní spojené informace, které je také možné zjistit z informačního panelu vpravo. Za výchozí branou se umísťuje koncová stanice s uvedenou IP adresou a doménovým jménem. Další úroveň hierarchie představuje proces vývoje konkrétního detekovaného útoku. První ikona v tomto uspořádání zastupuje proces, který byl v rámci útoku zdrojovým bodem.

Detailní charakteristika incidentů

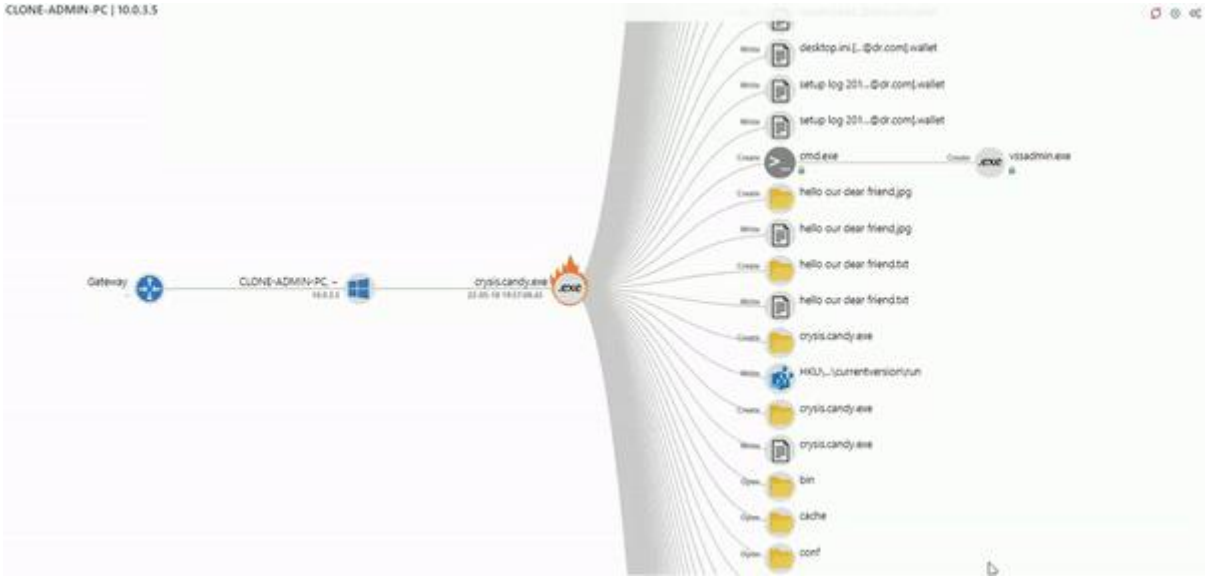
Grafická komponenta odpovídá za vizualizaci útoku
a jeho zobrazení uživateli v přehledné podobě



Plně dynamická grafická komponenta se stará o vytvoření vyšší úrovně abstrakce nad vzniklými incidenty a uspořádá vá je do souvislého vývojového diagramu. Navíc provádí klasifikaci jednotlivých uzlů podle jejich kategorií, přidává odpovídající ikony a zobrazuje informace relevantní pro uživatele. Další silnou stránkou této komponenty je jednoduché a intuitivní ovládání na různých zařízeních (tablety, mobily, počítače).

Analýza chování škodlivého procesu

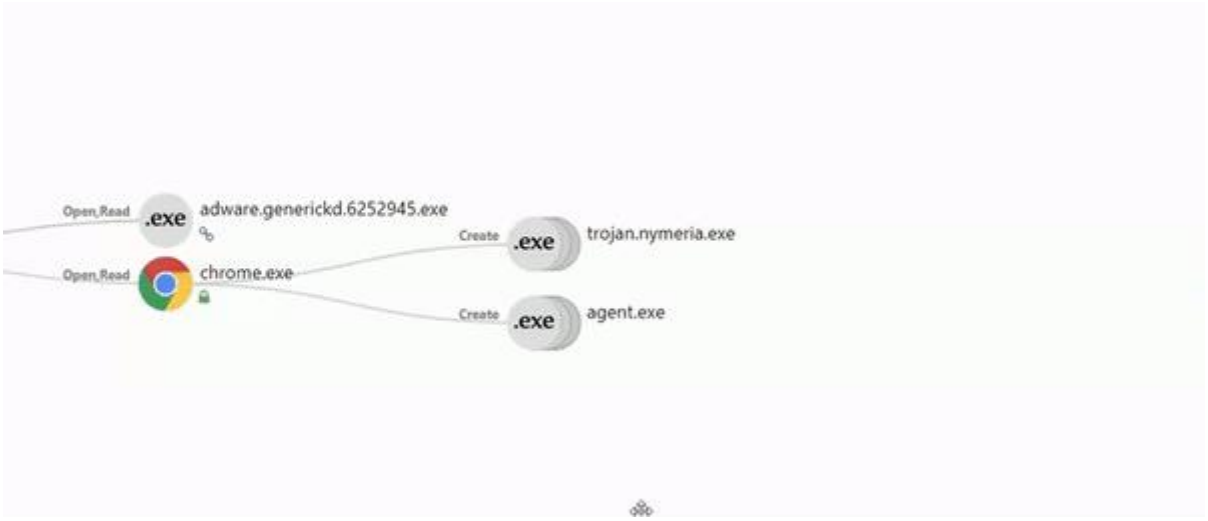
Uživatel webové aplikace je schopen pomocí různých režimů
zobrazení zkoumat vzniklý útok efektivněji a jednodušeji



Z důvodu provedení jednodušší analýzy, obsahuje webová aplikace různé režimy zobrazení, jejichž primárním cílem je zprostředkovávat různé úhly pohledu na incident, který se vyskytl v chráněném systému. Uživatel je v aktuální verzi aplikace schopen volit mezi třemi různými režimy, tj. *Full view, Access view* a *Grouped view*. Režim zobrazení *Full view* poskytuje klasický režim zobrazení reprezentující vývojový diagram útoků bez následující analýzy. Režim zobrazení *Group view* se zaměřuje na uspořádání nebezpečných událostí na základě pravidel. V důsledku čeho je administrátor schopen ihned stanovit zaměření škodlivého procesu nezávisle na tom, kolik pokusů uskutečnil na provedení dané akce. Režim zobrazení *Access view* spočívá v zařazení dílčích událostí útoku do skupin v závislosti na cílovém objektu. Vytvořené skupiny v sobě skrývají přístupové události roztříděné do kategorií, tzn. přístupy k registrům, procesům a souborům.

Zobrazení síťové aktivity

Pomocí řešení Sec Guardian je možné provádět analýzu síťové aktivity procesů

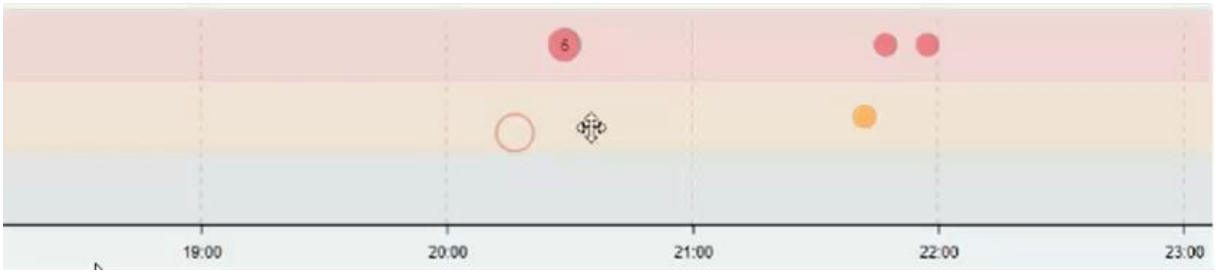


Grafická komponenta webové aplikace umožňuje zkoumat síťovou aktivitu procesů. Systém Sec Guardian spoluprací s externími službami provádí lokalizaci IP adres, vyhodnocuje za nimi skrytá nebezpečí a zaznamenává účel připojení. V případě potřeby je uživatel schopen pomocí speciálního režimu zobrazení se zaměřit pouze na tu kategorii incidentů, kterou

zrovna potřebuje. Skupiny jsou tvořeny událostmi v závislosti na cílovém objektu přístupu, tj. procesy, registry anebo soubory.

Dynamická časová osa

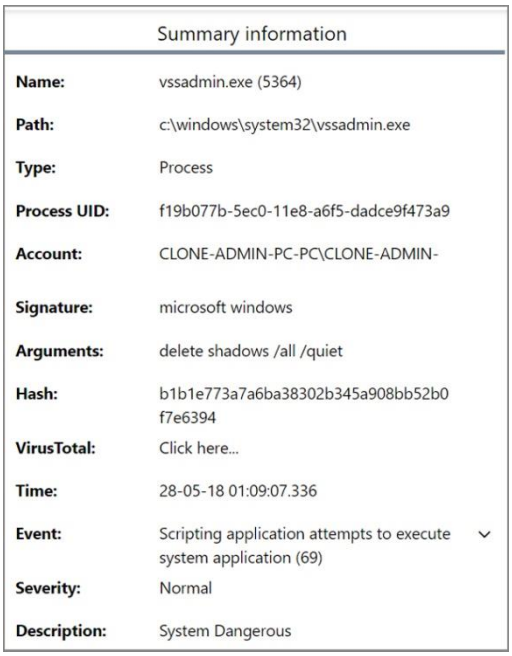
Časová osa se přizpůsobuje vstupním datům a je ji možné jednoduše ovládat pomocí myši



Po načtení zaznamenaných útoků ze serveru, proběhne jejich zpracování a zobrazení na časové ose, která představuje bodový graf, ve kterém jsou události setříděné podle severit a času. Z důvodu lepší přehlednosti je každá severita zastoupena jinou barvou a časové úseky jsou mezi sebou rozdělené přerušovanými čarami. Tečky vzniklé po načtení dat zastupují útoky, které v počítačové síti nastaly. Po najetí ukazatelem myši na incident se objeví krátký popis s informacemi. Je důležité zmínit, že na časové ose můžou vznikat skupiny teček a to z důvodu lepší přehlednosti pro administrátora. Po najetí myši na takovou skupinu se objeví seznam jejích vnitřních prvků. Časová osa je plně dynamická, to znamená, že se zobrazovaný časový úsek automaticky přizpůsobuje vstupním datům a uživatel jej může pomocí myši přibližovat, oddalovat anebo přemísťovat.

Podrobné informace

Webová aplikace poskytuje informační panel
umožňující se zaměřit na detaily konkrétního incidentu



Informační panel zobrazuje podrobné informace o incidentech zvolených v grafické komponentě a zprostředkovává např. přístup k externím webovým službám. VirusTotal a IP

Geolocation. Z dané komponenty je možné zjistit název cílového objektu, cestu k jeho umístění, jeho typ, podpis, argumenty se kterými byl spuštěn, předchozí stav apod. Navíc informační panel poskytuje charakteristiku detekované události, konkrétně její závažnost, čas vzniku a krátký popis události.

Je důležité zdůraznit, že komponenta je plně dynamická. Znamená to, že se dokáže přizpůsobit jak různým velikostem obrazovky, tak i odlišným vstupním datům.

Kontakt

Sec Guardian, s.r.o.
Veveří 2845/102,
616 00 Brno, ČR,

Web: www.sec-guardian.cz
Email: info@sec-guardian.cz