Technický přehled

Cyber Spear Persistence je bezagentní řešení pro přesnou detekci sofistikovaných kybernetických útoků, jako např. Advanced Persistent Threats (APTs), s důrazem na minimalizaci reportování false-positive nebo nejednoznačných nálezů IT oddělení.

Cyber Spear Persistence sbírá veškeré významné indikátory o spuštěných procesech ze serverů, pracovních stanic a sítí. Nasbíraná data následně analyzuje pomocí přednastavených komplexních procesů, jejíchž cílem je detekce přítomnosti škodlivé aktivity. Tyto procesy zahrnují nejen rozsáhlé dotazování bezpečnostních databází, ale i statickou a dynamickou analýzu.

Systém následně rozdělí procesy na legitimní, škodlivé, či vyžadující hlubší úroveň analýzy. Manuální analýza je prováděna na žádost klienta vyhrazeným SOC týmem, jehož služby jsou zahrnuty v rámci licence.

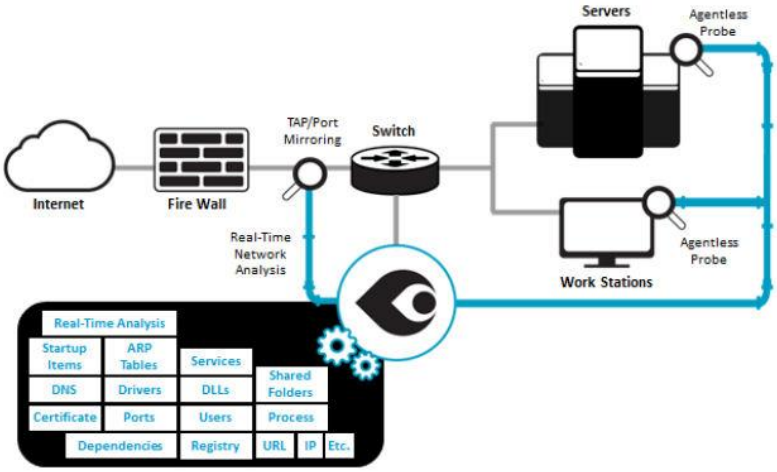
Během tohoto procesu nedochází k jakémukoliv zásahu do soukromí, dostupnosti ani výkonnosti.
CyberSpear analyzuje pouze spustitelné soubory a během analýzy jsou z koncových zařízení přenášeny pouze HASH sumy jednotlivých spustitelných souborů. Vykopírování podezřelých spustitelých souborů a jejich knihoven je prováděno na žádost zákazníka.

Cyber Spear Persistence funguje bez agentů – jediný server tak může zajistit efektivní pokrytí i rozsáhlé organizace. Toto řešení je škálovatelné a tedy schopno pokrýt jakkoliv velkou organizaci.

Cyber Spear
PRECISE THREAT DETECTION

Úroveň 1: Shromažďování indikátorů, použití Port Mirroring nebo sondy pro zachytávání síťového provozu.

Cyber Spear Persistence shromažďuje významné indikátory ze serverů, pracovních stanic a sítí společnosti. Tyto indikátory zahrnují hashe souborů a procesů, přitom však nepracují přímo s uživatelskými dokumenty, čímž je zajištěno zachování důvěrnosti.



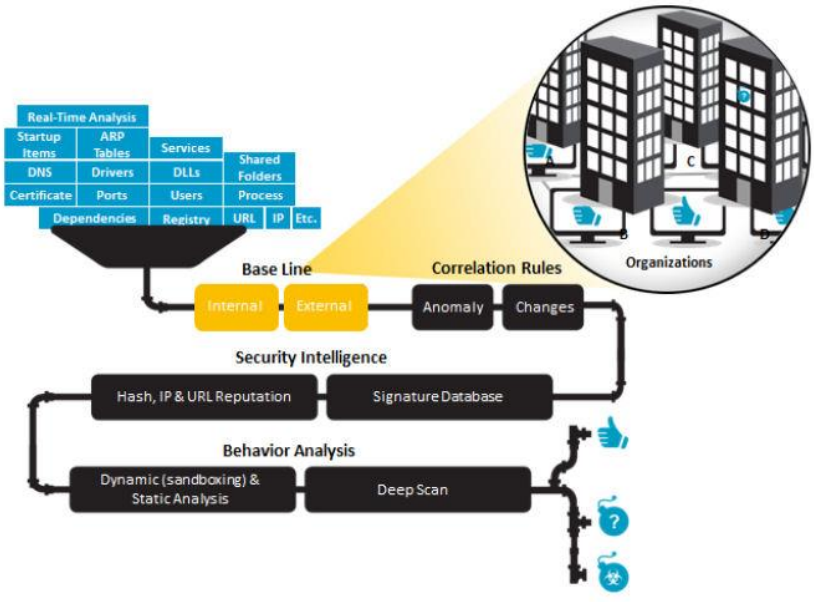
Odposlech sítě a zrcadlení portů se využívá k zjištění anomálií v síťovém provozu. Cyber Spear Persistence zkoumá veškeré servery a pracovní stanice v pravidelných hodinových intervalech (tato frekvence může být upravena). Objem přenášených dat mezi koncovým bodem a CyberSpear serverem se pohybuje v rozmezí cca. 300-500 kB a tudíž nenarušuje výkonnost sítě či koncové stanice.

Úroveň 2: Porovnávací hladina – interní a externí

Jakmile je hotový prvotní sken organizace, je vytvořen referenční stav, který slouží pro porovnávání indikátorů na daném zařízení s ekvivalentními indikátory na jiném zařízení.

Dále je Cyber Spear Persistence schopen ověřit a porovnat indikátory vůči souhrnné znalostní databázi, která se skládá z dat z ostatních organizací.

Uživatelská data neopouští organizaci v žádné části procesu, čímž je udržována důvěryhodnost a soukromí.

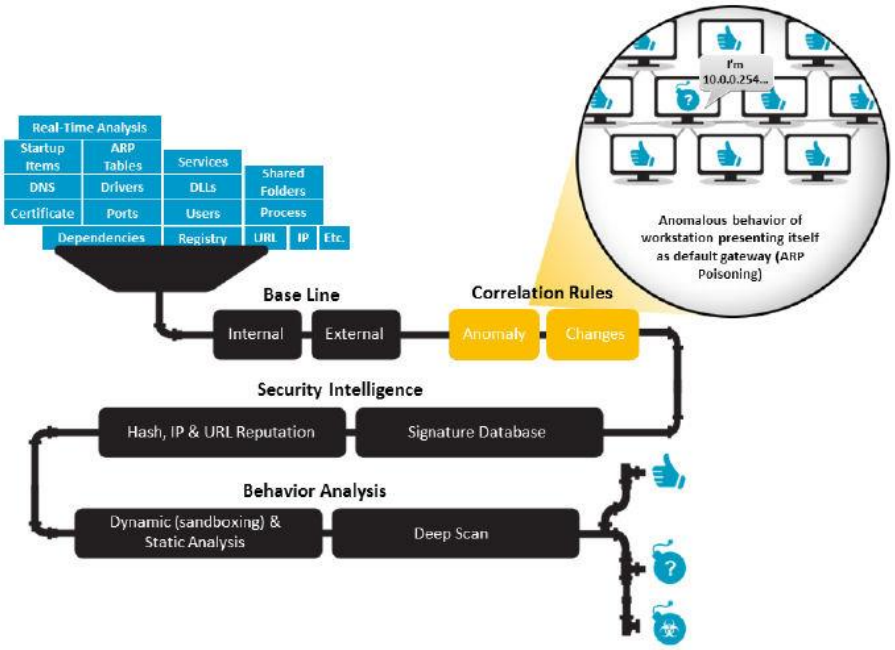


Cyber Spear
PRECISE THREAT DETECTION

Úroveň 3: Pravidla závislosti – anomálie a změny

Proprietární Cyber Spear Anomaly Engine detekuje anomálie a podezřelé chování na základě několikanásobné aplikace korelačních pravidel.

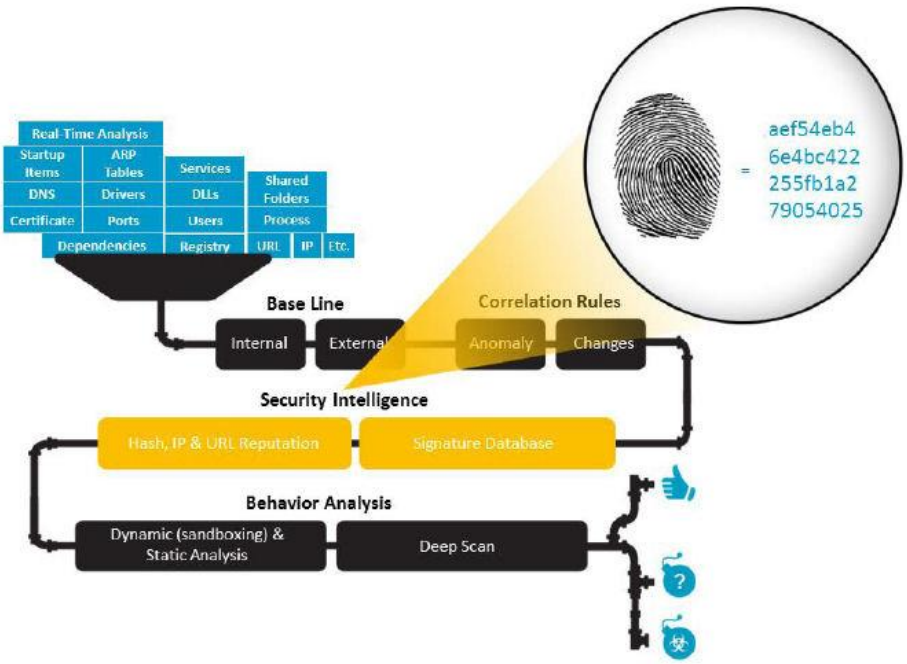
Tato pravidla zkoumají křížové reference mezi metadaty koncových stanic. Tato úroveň zajišťuje relevantní průběžně informace.



Úroveň 4: Bezpečnostní informace – databáze signatur a hashí, IP & URL reputace

Databáze hashí a IP & URL reputace jsou využívány k ověření integrity a „čistoty“ IT prostředí („whitelisting“ souborů a procesů).

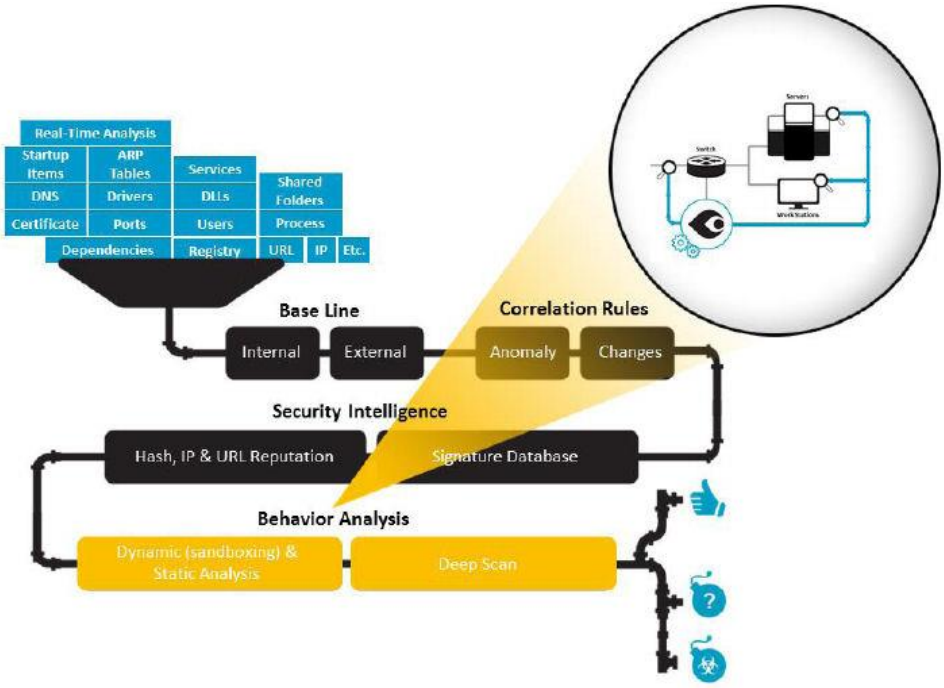
Další skupina databází signatur škodlivého softwaru se využívá k tvorbě „blacklistu“.



Úroveň 5: Behaviorální analýza – statická a dynamická analýza, podrobná kontrola

Statická analýza, tj. analýza bez spuštění vlastního programu, je prováděna dekompilací různých částí binárního souboru a studováním každé komponenty.

Dynamická analýza se provádí za pomoci Cyber Spear Smart Simulated Execution (SSE) sandbox enginu.



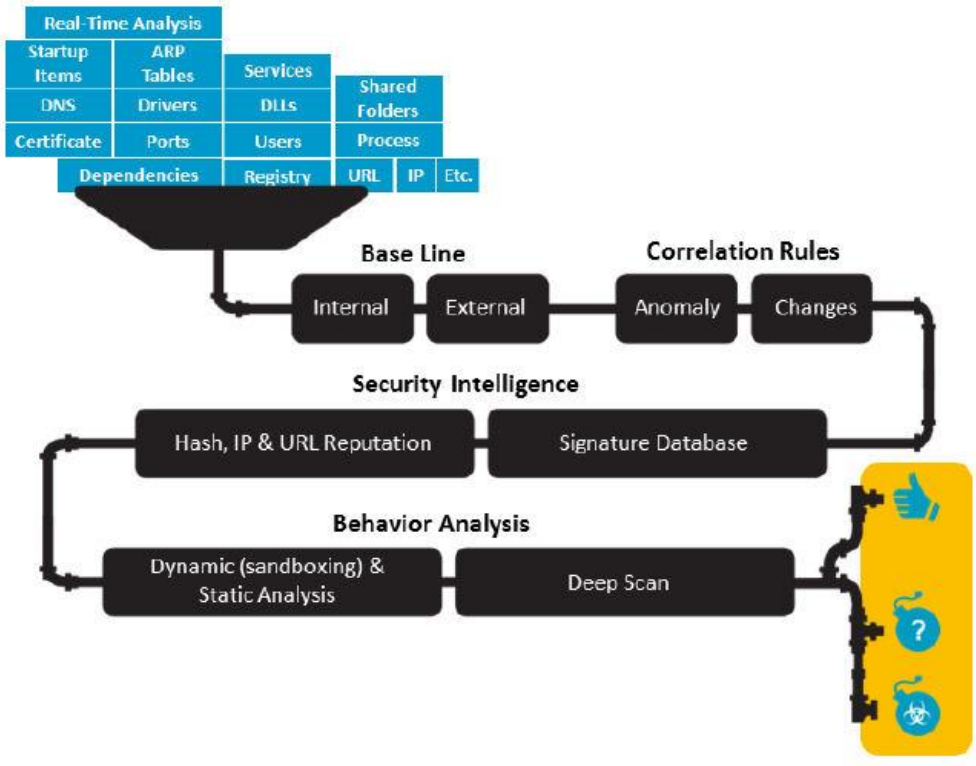
SSE sandbox engine vytvoří cluster izolovaných prostředí, v rámci kterých se provádí spouštění procesů a aplikací za současného monitoringu jakéhokoliv podezřelého chování.

To se děje opakovaně za různých podmínek, aby byly odhaleny i důkladně skryté hrozby vytvořené sofistikovanými útočníky.

Úroveň 6: Uživatelské rozhraní

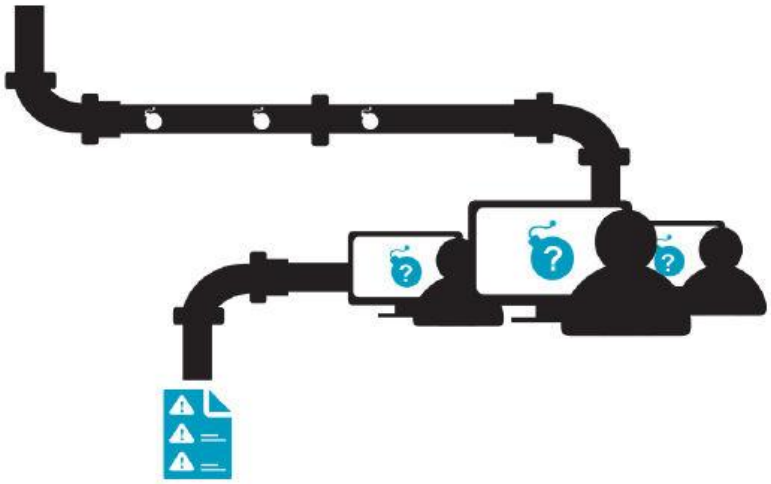
Grafické uživatelské rozhraní Cyber Spear Persistence se skládá z následujícího:

Sekce	Popis
Hlavní panel / Dashboard	Celkový pohled na systém
Scanner	Ovládací panel a náhled stavu scanneru
Aktiva	Náhled všech koncových bodů v organizaci; Umožňuje zajištění specifických informací o koncových bodech
Soubory	Náhled všch souborů v organizaci; Umožňuje zajištění specifických informací o souborech
Síť	Náhled síťového provozu organizace protékajícího přes odposlouchávaný interface
Uživatelé	Náhled všech uživatelů v organizaci; Umožňuje zajištění specifických informací o uživatelích
Upozornění	Detailní pohled na alerty
Mapy	Geografický a / nebo organizační náhled alertů
Nastavení	Podrobný panel systémového managementu; Zahrnuje oskenované podsítě a detailní nastavení; NAC a SIEM nastavení
Výstupy	Tvorba výstupů v různých formátech



Úroveň 7: SIEM (Security Information and Event Management) integrace

Cyber Spear Persistence zahrnuje jednoduchou integraci se SIEM systémy.



Úroveň 8: Integrace NAC (Network Access Control) a firewallu

Integrace NAC:

Průběžně:

1. Testování koncových bodů a serverů podle dat získaných z NAC
2. Testování koncových bodů a serverů podle nastavení Cyber Spear management konzole

Prevence útoků / blokování útoků v reálném čase (podle možností NAC):

1. Blokování portu kompromitovaného nodu:
    a. zabránění komunikace z kompromitovaného nodu do jiných nodů organizace
    b. zabránění úniku dat izolováním nodu
2. Přenesení kompromitovaného nodu do izolovaného forenzního vyšetřovacího prostředí
3. Přenesení kompromitovaného nodu do bezpečného prostředí s cílem odstranění hrozby

Integrace firewallu:

1. Blokování odchozí komunikace z kompromitovaného nodu (egress filtering na firewallu)
2. Blokování útočníka používajícího Command & Control (C&C) server či Botnet od jakýchkoliv nodů v organizaci (egress filtering na firewallu)

Cyber Spear
PRECISE THREAT DETECTION

Expertní zázemí

Cyber Spear SOC (Security Operations Center) se skládá z profesionálů na kybernetickou bezpečnost v oblastech:

- analýza malware
- reverzní inženýrství
- síťová analýza

Tým je připraven poskytnout konzultace (reakce na incident) a pomoci s řešením incidentu.

Multidoménová administrace

Díky jedné serverové instalaci je možno spravovat více domén současně.

Škálovatelnost

Cyber Spear Persistence nevyžaduje instalaci agentů – jedna serverová instalace dokáže zajistit efektivní analýzu i značně rozsáhlých organizací. Jedna instalace dokáže zvládnout 10 000 – 20 000 koncových bodů (závisí na topologii sítě). Toto řešení je škálovatelné a při instalaci na více serverech pak pokryje jakoukoliv velikost organizace.

Cyber Spear
PRECISE THREAT DETECTION

Cyber Spear hardwarové požadavky

Typ serveru:	Fyzický či virtuální
Operační systém:	Microsoft Windows Server 2008/2012
CPU:	Dual či Quad core (využití snifferu v síti vyžaduje další CPU)
Paměť:	16GB RAM a vyšší (závisí na velikosti sítě)
Místo na disku:	300 GB
Síťové karty:	2x1 Ethernet NICs

SSE Sandboxing engine hardwarové požadavky

Typ Serveru:	Virtuální – Vmware Workstation / Player
Hostitelský operační systém:	Microsoft Windows platforma
CPU:	Quad core
Paměť:	6 GB RAM
Místo na disku:	100 GB

Možnost instalace SSE z image na Hypervisor / ESX OS

Nastavení sítě

Síťové karty rozhraní

První síťová karta se používá k přístupu ke koncovým zařízením. Druhá síťová karta se používá pro připojení na mirror port / sondě k zachytávání síťového provozu na interním rozhraní Firewallu / Proxy serveru.

Konfigurace portů

Následující nastavení firewallu musí být povoleny:

- Otevření portů (Active Directory porty) ze Cyber Spear serveru do koncových bodů
- Otevření portu (náhodný port – defaultně je port 71) z koncových bodů k Cyber Spear serveru

Administrativní požadavky

Následující administrativní nastavení je požadováno pro funkčnost operace:

- IP adresa a port interního Firewallu / Proxy serveru (pokud přítomen)
- rozsahu IP adres ke skenování
- práva lokálního administrátora pro všechny analyzované nody

Cyber Spear
PRECISE THREAT DETECTION

Cyber Spear kontaktní informace pro Českou republiku:

Risk Analysis Consultants, s.r.o.
Španělská 2
120 00 Praha 2

RISK ANALYSIS CONSULTANTS

T: +420 221 628 400
F: +420 221 628 401
E: zu@rac.cz
W: www.rac.cz/CyberSpear