Bezpečnostní monitoring – SIEM

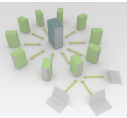
(logy pod drobnohledem)

David Vorel

Technický konzultant

Obsah prezentace

- Úvod do problematiky monitoringu bezpečnostních událostí
- Reálné hrozby
- Prvky informační bezpečnosti
- Informační audit
- Log management
- Způsoby sběru logů
- Nativní metody auditu operačních systému
- Nativní metody auditu databází
- Od log managementu k SIEM
- Hlavní funkce SIEM
- Architektura SIEM
- Základní podpůrné nástroje SIEM
- Pokročilé podpůrné nástroje SIEM
- Nejčastější chyby při nasazení LM nebo SIEM



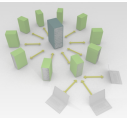
Úvod problematiky monitoringu bezpečnostních událostí

Úvod problematiky monitoringu bezpečnostních událostí

LM – Log Management
- Orientován pouze na sběr událostí

SIEM – Security Information and Event Management
- Schopnost automatických korelací a reportingu

Důvody sběru událostí
- Dodržování standardů a dobrých praktik
- Detekce a reporting útoků a anomálií
- Přehled v událostech a orientace v prostředí
- Požadavky auditorů
  - PCI DSS
- Forenzní a reverzní analýza aktivit v prostředí



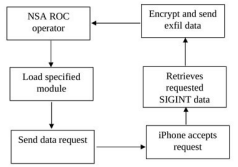
Reálné hrozby

TOP SECRET//COMINT//REL TO USA, FVEY

DROPOUTJEEP
ANT Product Data

10/01/08

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.



(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

Unit Cost: $ 0

Status: (U) In development

POC: U//FOUO [redacted], S32222, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

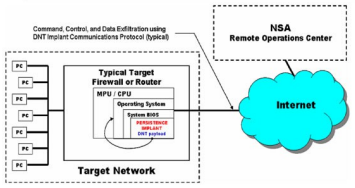
TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL USA, FVEY

FEEDTROUGH
ANT Product Data

06/24/08

(TS//SI//REL) FEEDTROUGH is a persistence technique for two software implants, DNT's BANANAGLEE and CES's ZESTYLEAK used against Juniper Netscreen firewalls.



(S//SI//REL) Persistence Operational Scenario

(TS//SI//REL) FEEDTROUGH can be used to persist two implants, ZESTYLEAK and/or BANANAGLEE across reboots and software upgrades on known and covered OS's for the following Netscreen firewalls, ns5xt, ns25, ns50, ns200, ns500 and ISG 1000. There is no direct communication to or from FEEDTROUGH, but if present, the BANANAGLEE implant can receive and transmit covert channel comms, and for certain platforms, BANANAGLEE can also update FEEDTROUGH. FEEDTROUGH however can only persist OS's included in it's databases. Therefore this is best employed with known OS's and if a new OS comes out, then the customer would need to add this OS to the FEEDTROUGH database for that particular firewall.

(TS//SI//REL) FEEDTROUGH operates every time the particular Juniper firewall boots. The first hook takes it to the code which checks to see if the OS is in the database, if it is, then a chain of events ensures the installation of either one or both implants. Otherwise the firewall boots normally. If the OS is one modified by DNT, it is not recognized, which gives the customer freedom to field new software.

Status: (S//SI//REL) FEEDTROUGH has on the shelf solutions for all of the listed platforms. It has been deployed on many target platforms

POC: [redacted], S32222, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

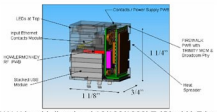
TOP SECRET//COMINT//REL USA, FVEY

TOP SECRET//COMINT//REL FVEY

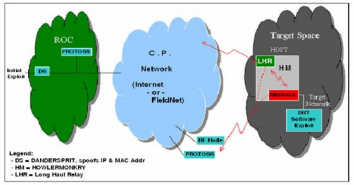
FIREWALK
ANT Product Data

08/05/08

(TS//SI//REL) FIREWALK is a bidirectional network implant, capable of passively collecting Gigabit Ethernet network traffic, and actively injecting Ethernet packets onto the same target network.



(TS//SI//REL) FIREWALK is a bi-directional 10/100/1000bT (Gigabit) Ethernet network implant residing within a dual stacked RJ45 / USB connector. FIREWALK is capable of filtering and egressing network traffic over a custom RF link and injecting traffic as commanded; this allows a ethernet tunnel (VPN) to be created between target network and the ROC (or an intermediate redirector node such as DNT's DANDERSPRITZ tool.) FIREWALK allows active exploitation of a target network with a firewall or air gap protection.
(TS//SI//REL) FIREWALK uses the HOWLERMONKEY transceiver for back-end communications. It can communicate with an LP or other compatible HOWLERMONKEY based ANT products to increase RF range through multiple hops.



Status: Prototype Available – August 2008 **Unit Cost:** 50 Units $537K

POC: [redacted], S3223, [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted]@nsa.ic.gov

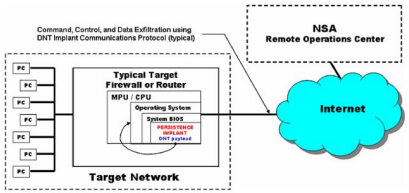
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

HALLUXWATER
ANT Product Data

06/24/08

(TS//SI//REL) The HALLUXWATER Persistence Back Door implant is installed on a target Huawei Eudemon firewall as a boot ROM upgrade. When the target reboots, the PBD installer software will find the needed patch points and install the back door in the inbound packet processing routine.



(TS//SI//REL) HALLUXWATER Persistence Implant Concept of Operations

(TS//SI//REL) Once installed, HALLUXWATER communicates with an NSA operator via the TURBOPANDA Insertion Tool (PIT), giving the operator covert access to read and write memory, execute an address, or execute a packet.

(TS//SI//REL) HALLUXWATER provides a persistence capability on the Eudemon 200, 500, and 1000 series firewalls. The HALLUXWATER back door survives OS upgrades and automatic bootROM upgrades.

Status: (U//FOUO) On the shelf, and has been deployed.

POC: [redacted], S32222, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

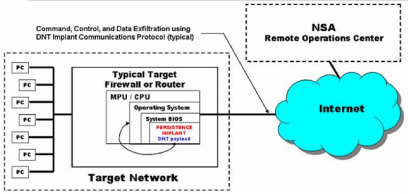
TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

JETPLOW
ANT Product Data

06/24/08

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.



(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details). **Unit Cost:** $0

POC: [redacted], S32222, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

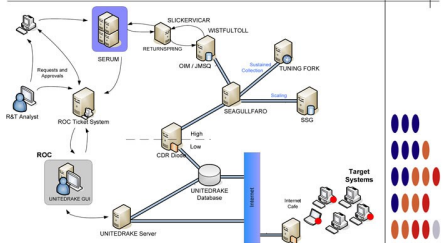
TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

IRATEMONK
ANT Product Data

06/20/08

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.



(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery **Unit Cost:** $0

POC: [redacted], S32221, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

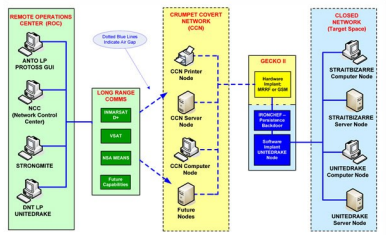
TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

IRONCHEF
ANT Product Data

07/14/08

(TS//SI//REL) IRONCHEF provides access persistence to target systems by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to communicate with a hardware implant that provides two-way RF communication.



(TS//SI//REL) IRONCHEF Extended Concept of Operations

(TS//SI//REL) This technique supports the HP Proliant 380DL G5 server, onto which a hardware implant has been installed that communicates over the I^2C Interface (WAGONBED).

(TS//SI//REL) Through interdiction, IRONCHEF, a software CNE implant and the hardware implant are installed onto the system. If the software CNE implant is removed from the target machine, IRONCHEF is used to access the machine, determine the reason for removal of the software, and then reinstall the software from a listening post to the target system.

Status: Ready for Immediate Delivery **Unit Cost:** $0

POC: [redacted], S32221, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

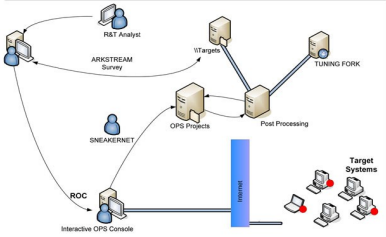
TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

SWAP
ANT Product Data

06/20/08

(TS//SI//REL) SWAP provides software application persistence by exploiting the motherboard BIOS and the hard drive's Host Protected Area to gain periodic execution before the Operating System loads.



(TS//SI//REL) SWAP Extended Concept of Operations

(TS//SI//REL) This technique supports single or multi-processor systems running Windows, Linux, FreeBSD, or Solaris with the following file systems: FAT32, NTFS, EXT2, EXT3, or UFS 1.0.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS and TWISTEDKILT to write the Host Protected Area on the hard drive on a target machine in order to implant SWAP and its payload (the implant installer). Once implanted, SWAP's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery **Unit Cost:** $0

POC: [redacted] S32221, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

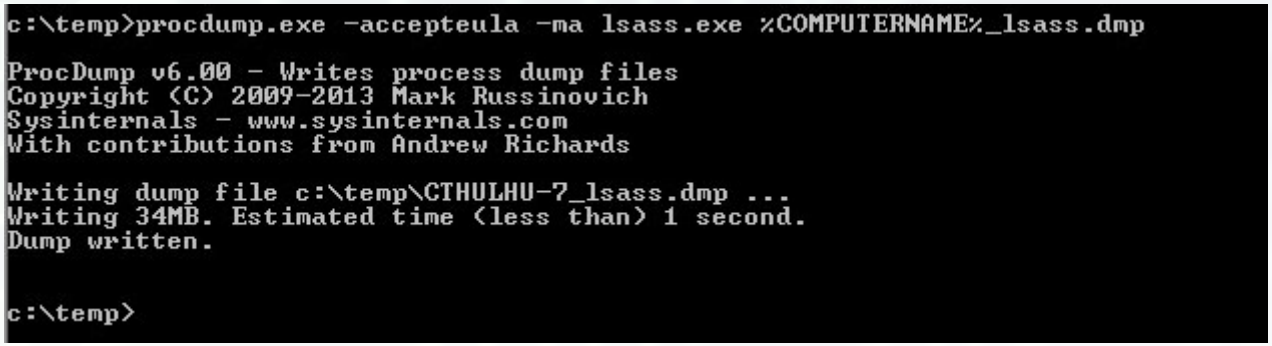
Reálné hrozby

Útoky zvenčí

- Viry
- Cílená špionáž
- Penetrace klientské strany
- Penetrace pomocí sociálních medií

Útoky zevnitř

- Sociální inženýrství
- Sdílení hesel
- Extrakce hesel v čitelné formě pomocí Mimikatz

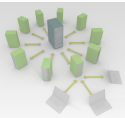


Mimikatz – extrakce hesel v čitelné podobě

Extrakce z paměti

- LM
- NTLM
- WDigest
- SSP
- Kerberos
- PIN
- Certifikáty

```
C:\forensics>mimikatz.exe

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jan 23 2014 00:5
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with  14 modules * * */


mimikatz # sekurlsa::minidump c:\temp\CTHULHU-7_lsass.dmp
Switch to MINIDUMP

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 558720 (00000000:00088680)
Session           : Interactive from 0
User Name         : operator
Domain            : cthulhu-7
SID               : S-1-5-21-3628218508-2835621438-3746398616-1003
        msv :
         [00000003] Primary
         * Username : operator
         * Domain   : cthulhu-7
         * LM       : 8880f85ff03eaf3b944e2df489a880e4
         * NTLM     : e337e31aa4c614b2895ad684a51156df
         * SHA1     : c203279fc91536021e64cc54092300bde54d3feb
        tspkg :
         * Username : operator
         * Domain   : cthulhu-7
         * Password : operator
        wdigest :
         * Username : operator
         * Domain   : cthulhu-7
         * Password : operator
        kerberos :
         * Username : operator
         * Domain   : cthulhu-7
         * Password : operator
        ssp :

Authentication Id : 0 ; 547499 (00000000:00085aab)
Session           : Interactive from 0
User Name         : operator
Domain            : cthulhu-7
SID               : S-1-5-21-3628218508-2835621438-3746398616-1003
        msv :
         [00000003] Primary
         * Username : operator
         * Domain   : cthulhu-7
         * LM       : 8880f85ff03eaf3b944e2df489a880e4
         * NTLM     : e337e31aa4c614b2895ad684a51156df
         * SHA1     : c203279fc91536021e64cc54092300bde54d3feb
        tspkg :
         * Username : operator
         * Domain   : cthulhu-7
         * Password : operator
        wdigest :
         * Username : operator
         * Domain   : cthulhu-7
         * Password : operator
        kerberos :
```



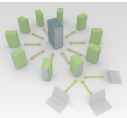
Prvky informační bezpečnosti

Fyzická bezpečnost

- Přístupové body
  - Vstupní karty
  - Turnikety
- Přistup do sítě
  - 802.1x
  - NAC
  - DHCP Enforcing

Bezpečnost síťové komunikace

- ACL
- IPS/IDS
- DLP
- DNS
- Antiviry pro obsah
  - WWW
  - SMTP
  - Souborové systémy
- Vzdálený přístup
  - VPN
  - Vzdálená plocha
  - Terminály virtualizace
  - Vytáčený přístup

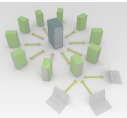


Prvky informační bezpečnosti

Bezpečnost serverů
- Segmentace služeb
- Řízení přístupů
  - RBAC
  - MAC
- Antiviry
- HIPS/HIDS
- DLP
- Kontrola integrity

Bezpečnost stanic
- Řízení přístupů
- Antiviry
- HIDS
- DLP

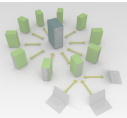
Bezpečnost mobilních zařízení
- Centrální management
- Vynucení firemních politik



Prvky informační bezpečnosti

Centrální evidence

- Detailní popis adresního prostoru
- Konfigurační databáze počítačových systémů
  - O serveru
  - Aplikace
  - Klasifikace
- Schémata sítí na úrovních L2 a L3
- Aplikační schémata
- Evidence změnových řízení



Informační audit

- C2 audit obecně
- Pouze neúspěšné pokusy
- Úspěšné či neúspěšné pokusy
- V reálném čase
- Dávkově

- Detekce zranitelností
- Síťový audit pomocí NetFlow
- Audit operačních systémů
- Audit aplikací
- Audit změnových řízení

Log management

- Kde jsou logy, má být i log management
- Vychází z potřeb informačního auditu
- Centrální log managementu je výhodou
  Životní cykly
  - Identifikace IS a jeho možností logování
  - Konfigurace vhodné úrovně logování
  - Efektivní sběr logů do centrálního uložiště
  - Prvotní ověření úrovně logování
  - Nastavení vhodné retenční doby
    - V uložišti informačního systému
    - Na centrálním uložišti
  - Automatická archivace po uplynutí doby retence

Způsoby sběru událostí

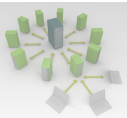
- Syslog – UDP, TCP, TLS
- Prosté soubory
- Síťové svazky
- Databázové konektory – ODBC/JDBC
- WMI
- SNMP
- Cisco – SDEE, NSEL
- Check Point OPSEC
- SOAP

Nativní metody auditu operačních systémů

Windows
- Audit procesů operačního systému
- Audit přístupů na souborový systém
- Audit řízení změn v GPO

Linux
- Audit procesů operačního systému - SELinux
- Audit přístupu na souborový systém – démon Auditd

Solaris
- BSM audit pomocí Auditd

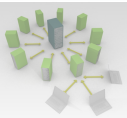


Nativní metody auditu databází

MS SQL – trace file pomocí store procedury
Oracle – Audit trail
MySQL – pouze v MySQL Enterprise edici
IBM DB2 – pomocí db2audit
SAP
- SM20 - přístupy
- SM19 - transakce

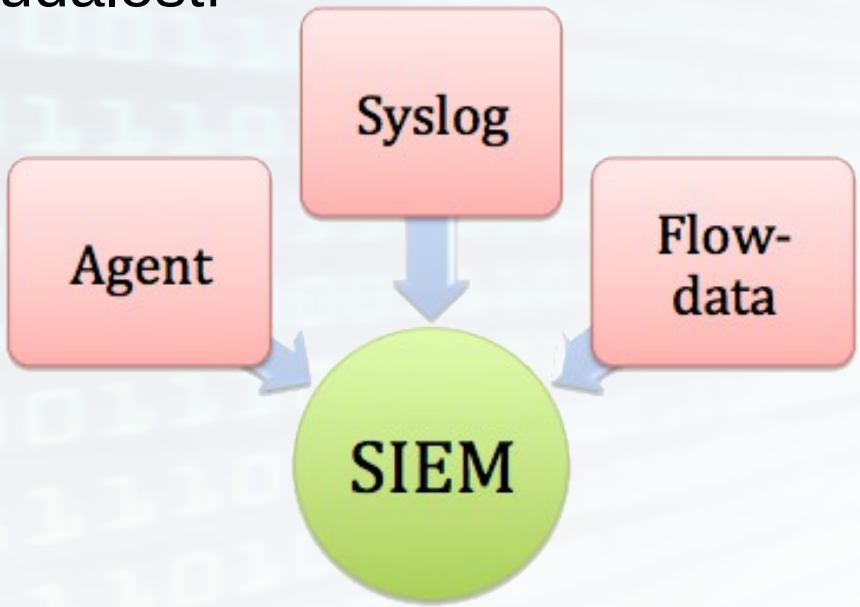
SyBase – nástroj Auditinit

Omezení DB auditu
- Nativní formáty logování
- Možné výpadky služeb
- Zvýšené nároky zdrojů OS



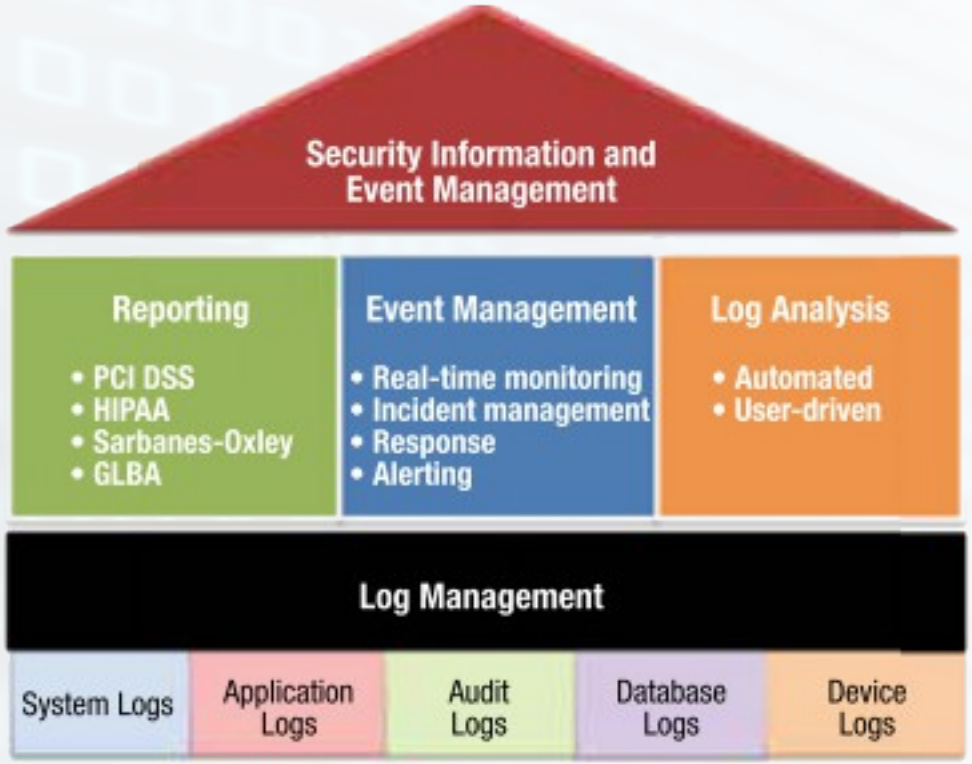
Od log managementu k SIEM

- Když surové logy nestačí
- Rozsáhlé prostředí
- Korelace v reálném čase
- Eliminace nutnosti náhledu do více konzolí
- Dodatečná indexace
- Efektivní směrování potřebných událostí
- Efektivní reporting

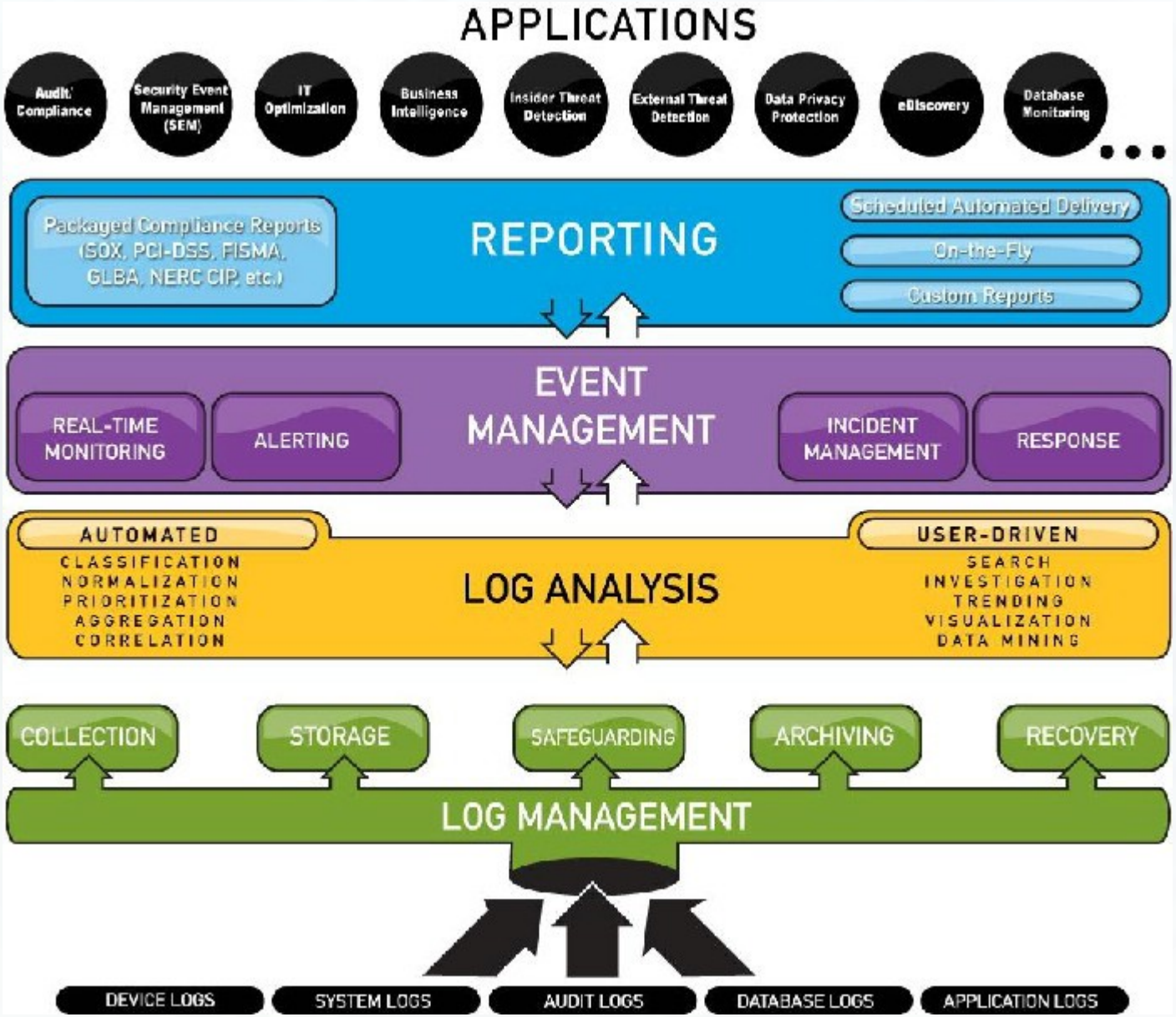


Hlavní funkce SIEM

- Kolekce
- Agregace
- Normalizace
- Filtrace
- Korelace
- Notifikace
- Archivace
- Retence
- Reporting



Architektura SIEM



Architektura SIEM

Vše v jednom
- Nižší cena HW i SW
- Menší propustnost
- Menší škálovatelnost

Modulární
- Možnost škálování
- Větší propustnost
- Vyšší nároky na HW

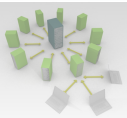
Vysoká dostupnost
- Efektivnější provozní odezva
- Kombinace s modulární
- Větší propustnost
- Vyšší cena HW i SW

Gartner - Magický kvadrant pro SIEM

Source: Gartner (May 2013)

Základní podpůrné nástroje SIEM

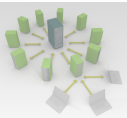
- **Testování na zranitelnosti**
  - Pravidelné automatizované kontroly pomocí VA nástrojů
  - Penetrační testy při nasazení, nebo při zásadních změnách
- **Evidence adresního prostoru**
  - Rychlá identifikace zdroje na síti
  - Aktualizace z centrální evidence
  - Klasifikace segmentu
- **Evidence systémů**
  - Vkládání dodatečných informací o systému do incidentů
    - Fyzické umístění
    - Organizační jednotka
    - Správce systému
  - Klasifikace systémů



Pokročilé podpůrné nástroje SIEM

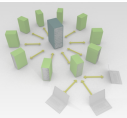
- **IAM** - identity a access management
  - Efektivní řízení přístupů dle nastavených pravidel
  - Sledování anomálií a odchylek v přístupech
  - Aktuální zobrazení informací:
    - Systém – kdo je přihlášen do systému a z jakého zdroje
    - Účet – kde všude je účet přihlášen a z jakého zdroje

- **NBAD** - detekce anomálií v síťovém provozu L3<
  - Umístění sondy na na úrovni L2, nebo mirror portu
  - Sledování odchylek v chování pro:
    - zdroje a cíle spojení
    - počty spojení
    - četnost vytváření spojení
    - přenesený objem dat pro protokoly
    - časy aktivit



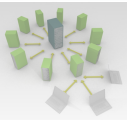
Pokročilé podpůrné nástroje SIEM

- **Sandboxing** – runtime analýza
  - Příchozí soubory z internetu - MTA, WWW, FTP
  - Analýza potencionálně infikovaných souborů
  - Zpětná analýza událostí v případě detekce anomálie
    - DNS, IP, ASN, URL
- **Darknet**
  - Alokovaný síťový prostor
  - Dříve neadresovaný prostor
  - Jakýkoliv paket je anomálie
- **Implementace principů honeypotů**
  - Honeytoken
  - Nativní honeypoty
  - Emulované honeypoty
  - V kombinaci s Darknet



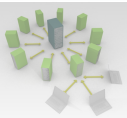
Nejčastější chyby v nasazení LM nebo SIEM

- Neexistuje implementace log managementu
- Log management se řeší až v případě incidentu
- Průběžně se neověřuje obsah shromažďovaných událostí
- Malé retenční doby
- Malá propustnost řešení
- Neexistují krizové scénáře



Shrnutí na závěr

- Motivace nasazení LM a SIEM
- Požadavky na lidské zdroje
- Komunikace s administrátory
- Řízení přístupů v sítích
- Řízení změn na sítí
- Zpětná kontrola
- Pravidelná profylaxe



Děkuji za pozornost

?

david.vorel@mosec.cz