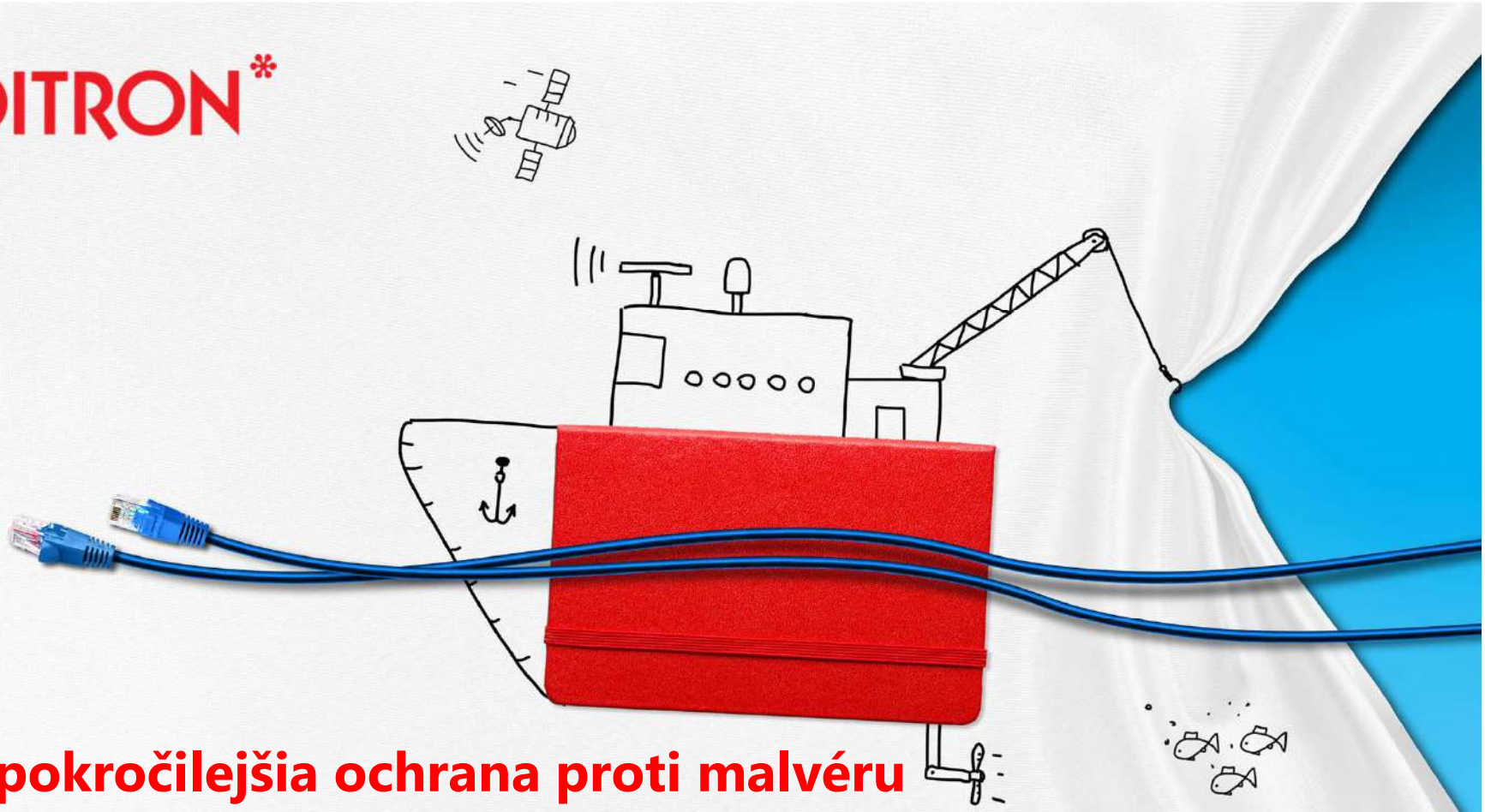
SOITRON



(Naj)pokročilejšia ochrana proti malvéru

Martin Vozár, Defense 2019

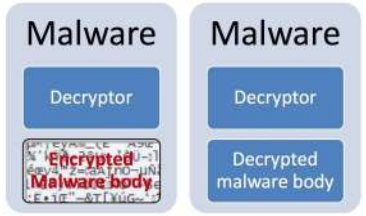
Agenda

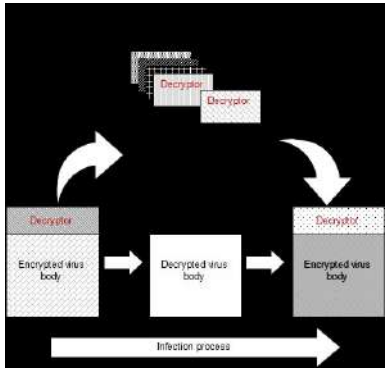
- Hrozby vs. tradičné ochrany
- Lastline Defender
- Návrh vhodného riešenia (príďte s nami konzultovať)

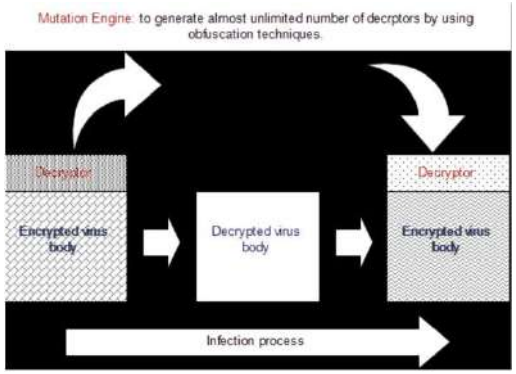
Aktuálne hrozby vs. tradičné ochrany

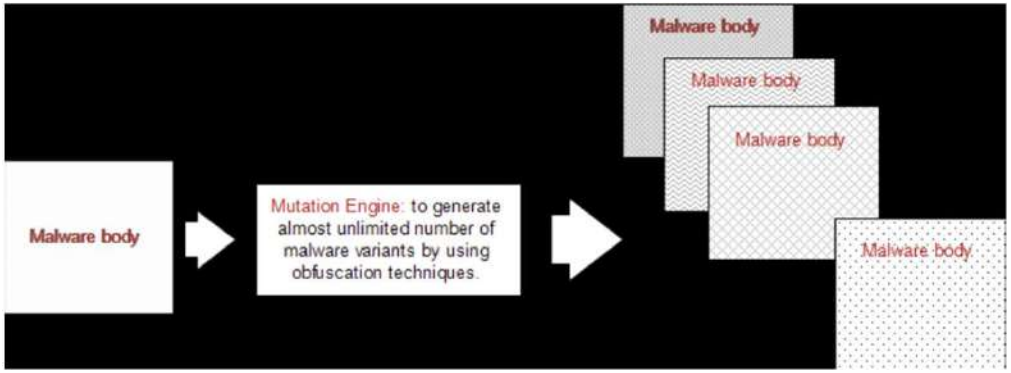
Evolúcia hrozieb

- "Bežný" (statický) kód (známa SHA256 signatúra)
  - vírusy – rootkit, spyware, crime-ware, adware, …
- Enkryptovaný malware (známym algoritmom)
- Oligomorfný/polymorfný malware (rôzne obfuskácie/dekryptory/ kombinácie – desiatky/milióny verzií, …)









- Metamorfný malware
- Zvlášť: Targeted malware

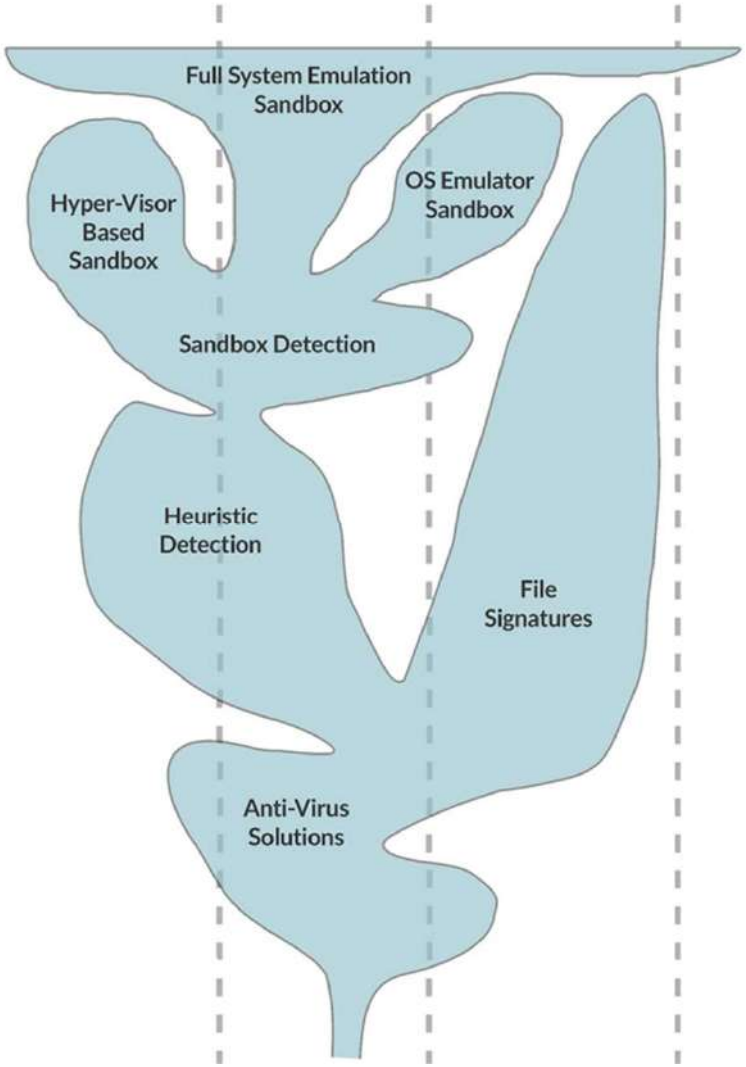
https://attack.mitre.org/

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections			Standard Cryptographic		

Evolúcia ochrán

- Evolúcia pokročilých ochrán proti hrozbám a ich zastarávanie kvôli APT (Advanced Persisent Threats)
  - Antivírus
  - Signatúry
  - Heuristika
  - Sandbox
    - Virtualizácia
    - OS emulácia
    - **Full System Emulation**



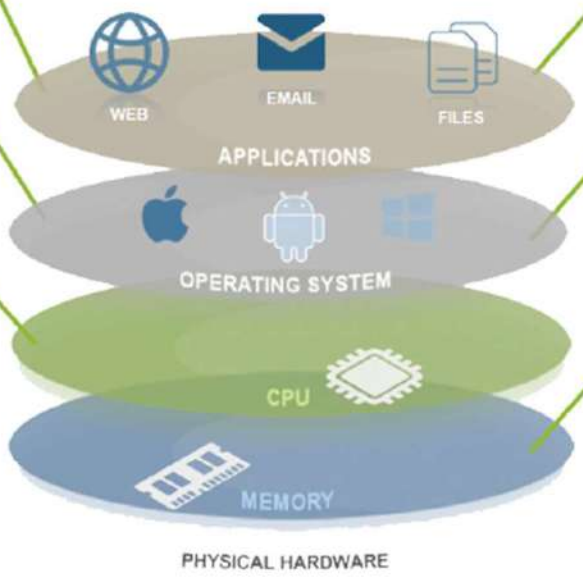
Riešenie: Full System Emulation

Čo je Full System Emulation?

Version-less inspection and analysis does not require gold images

Dormant code analysis identifies code blocks even if they do not execute

Dynamic code analysis elicits malicious behaviors



Identification of malicious document macros

True Kernel visibility

Inspection of malware memory including encrypted strings

Čo vidí tradičný sandbox?

- Stalling Loops
- Last User Login
- Presence Of Typical Programs
- Last Time System Booted
- Delaying Tactics
- Race Conditions
- CPU Core Checks

```
callq   0x100070478     ; symbol stub for: _open
callq   0x1000704b4     ; symbol stub for: _read
callq   0x1000702b6     ; symbol stub for: _close
```

Čo vidí Full System Emulation?

- ✓ **See every instruction**
- ✓ Manipulate conditions and identify highly evasive techniques
- ✓ “Fake Out” detection without need for numerous virtual instances

```
1   cmpl    $0x0c,%ebx
2   je      0x10000f21e
3   xorl    %esi,%esi
4   movq    %r15,%rdi
5   xorl    %eax,%eax
6   callq   0x100070478     ; symbol stub for: _open
7   movl    %eax,%r12d
8   testl   %eax,%eax
9   js      0x10000f21e
10  leaq    0xffffff70(%rbp),%rcx
11  movq    %rcx,0xffffffec0(%rbp)
12  movl    $0x00000050,%edx
13  movq    %rcx,%rsi
14  movl    %eax,%edi
15  callq   0x1000704b4     ; symbol stub for: _read
16  movq    %rax,%r13
17  movl    %eax,%r14d
18  movl    %r12d,%edi
19  callq   0x1000702b6     ; symbol stub for: _close
20  cmpl    $0x02,%r13d
21  jle     0x10000f21e
```


Konkrétne riešenie:
Lastline Defender

Kto je Lastline

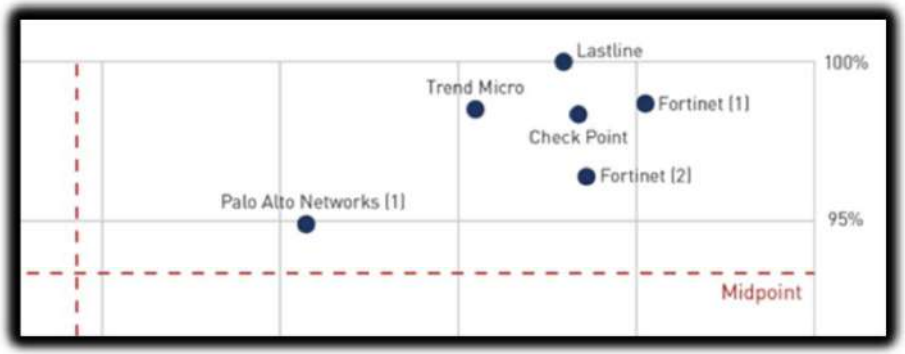
- Spoločnosť založená v 2011 troma z 10 top bezpečnostných akademikov na svete
- Podporená dostatočným kapitálom
- Vysoký nárast predaja year-to-year
- Viac ako 5 miliónov chránených používateľov*
- Viac ako 100 zamestnancov celosvetovo
- Technologický líder (NSS Labs, Forrester, Frost&Sullivan), patentované riešenia
- 250+ enterprise zákazníkov, 25+ technologických/OEM/servisných partnerov
- Víťaz prestížnych priemyselných ocenení

*licencovanie

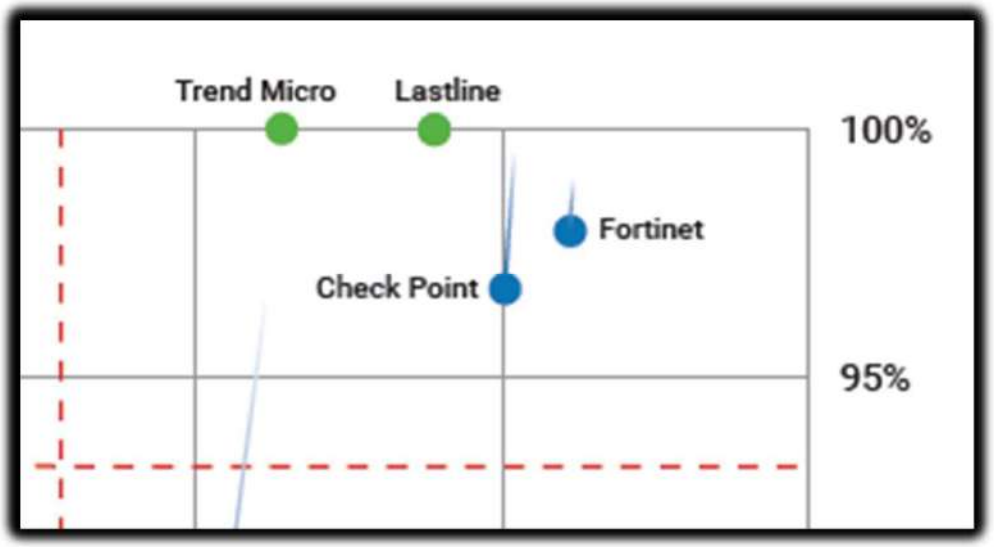
NSS Labs – Breach Detection Systems

- Nezávislé testovanie: 100% úspešnosť identifikácie škodlivého kódu a hrozieb (100/100/0)

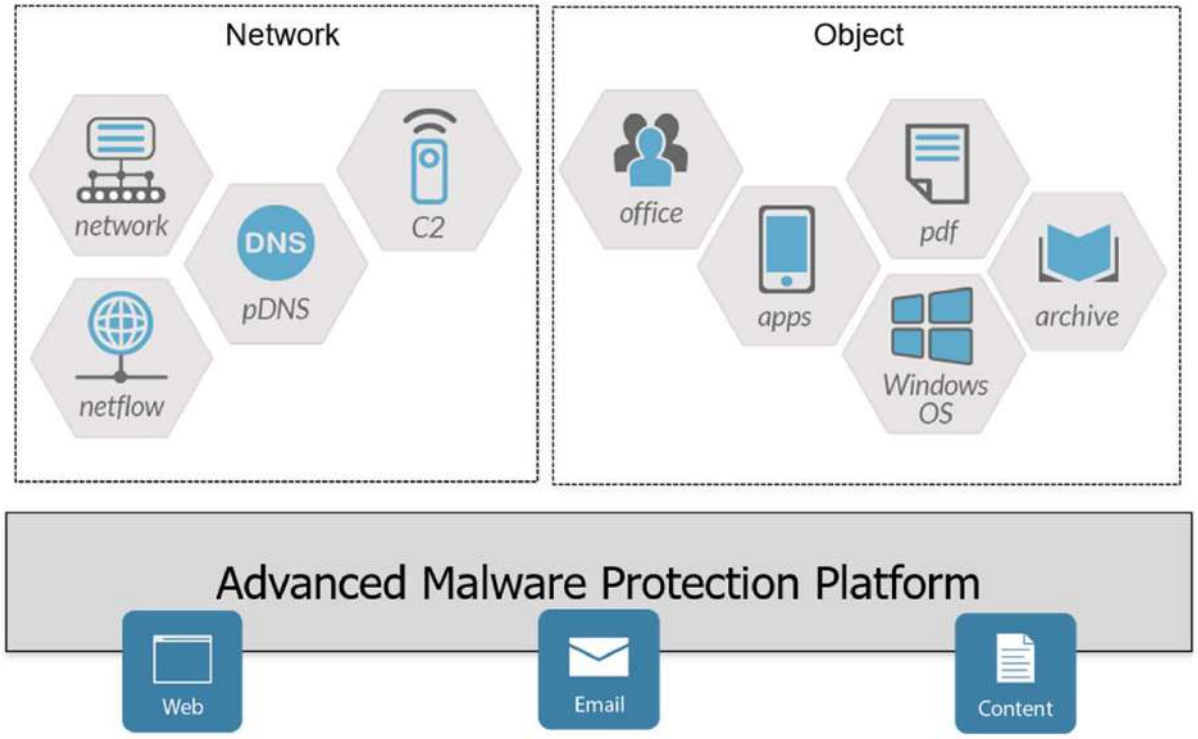
2016



2017



Produkt – Lastline Defender – Ochrana na viacerých frontoch



ICAP/proxy

MTA/SMTP/O365/POP3/IMAP

DNS/inline/**SPAN**/GUI/API

Lastline Defender – základné stavebné prvky / nasadenie

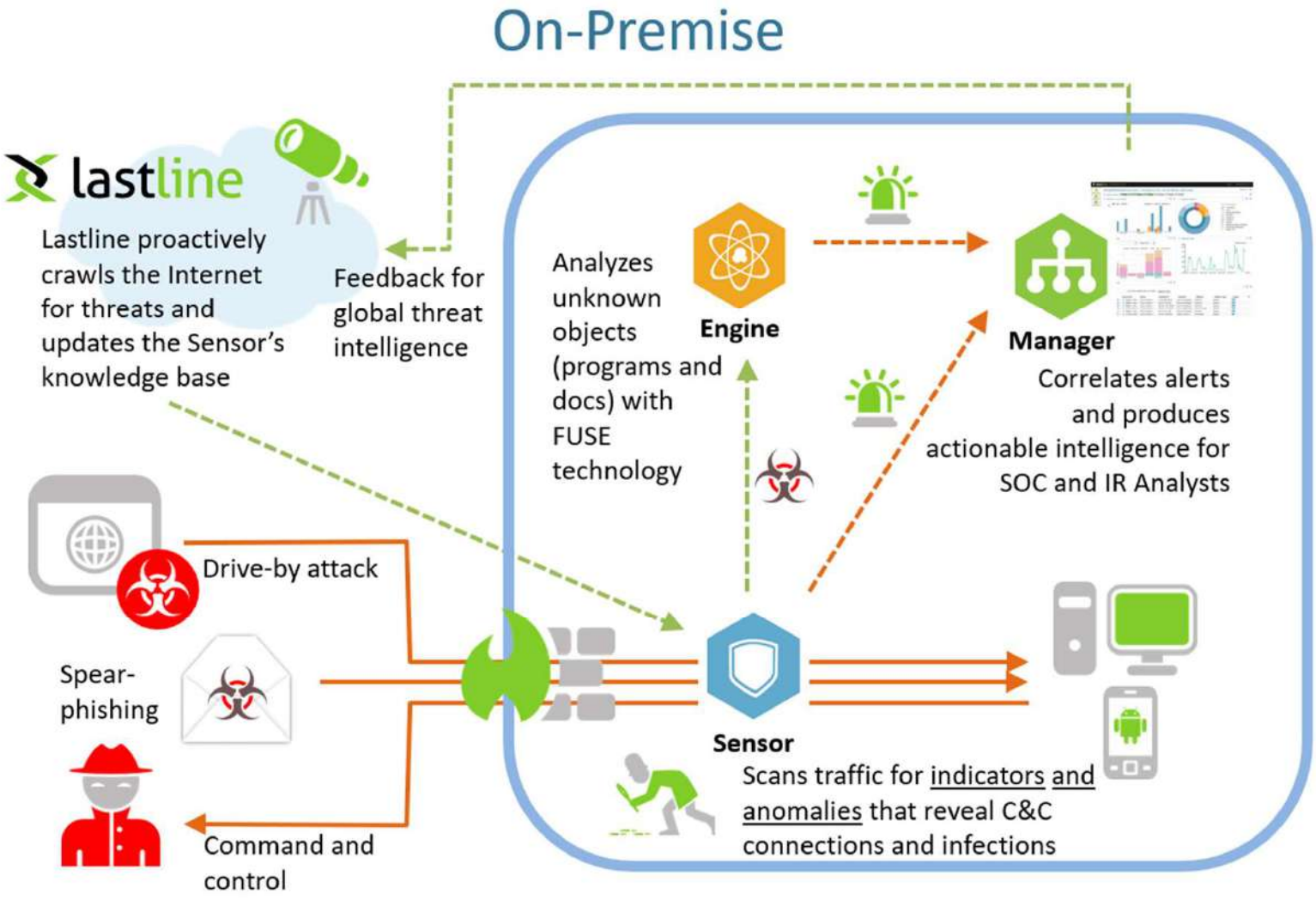
Sensor	Sonda v sieti analyzujúca **sieťovú premávku, email, web, súbory**. Extrahuje z premávky objekty a informácie a analyzuje ich.
Manager	**Koreluje threat events z rôznych zdrojov do incidentov,** obsahuje databázu incidentov a nastavení, spravuje pripojené senzory a engines.
Engine	Analyzuje vzorky pomocou **FULL SYSTEM EMULATION** technológie (**FUSE**)

Vlastný HW/vHW (flexibilita)

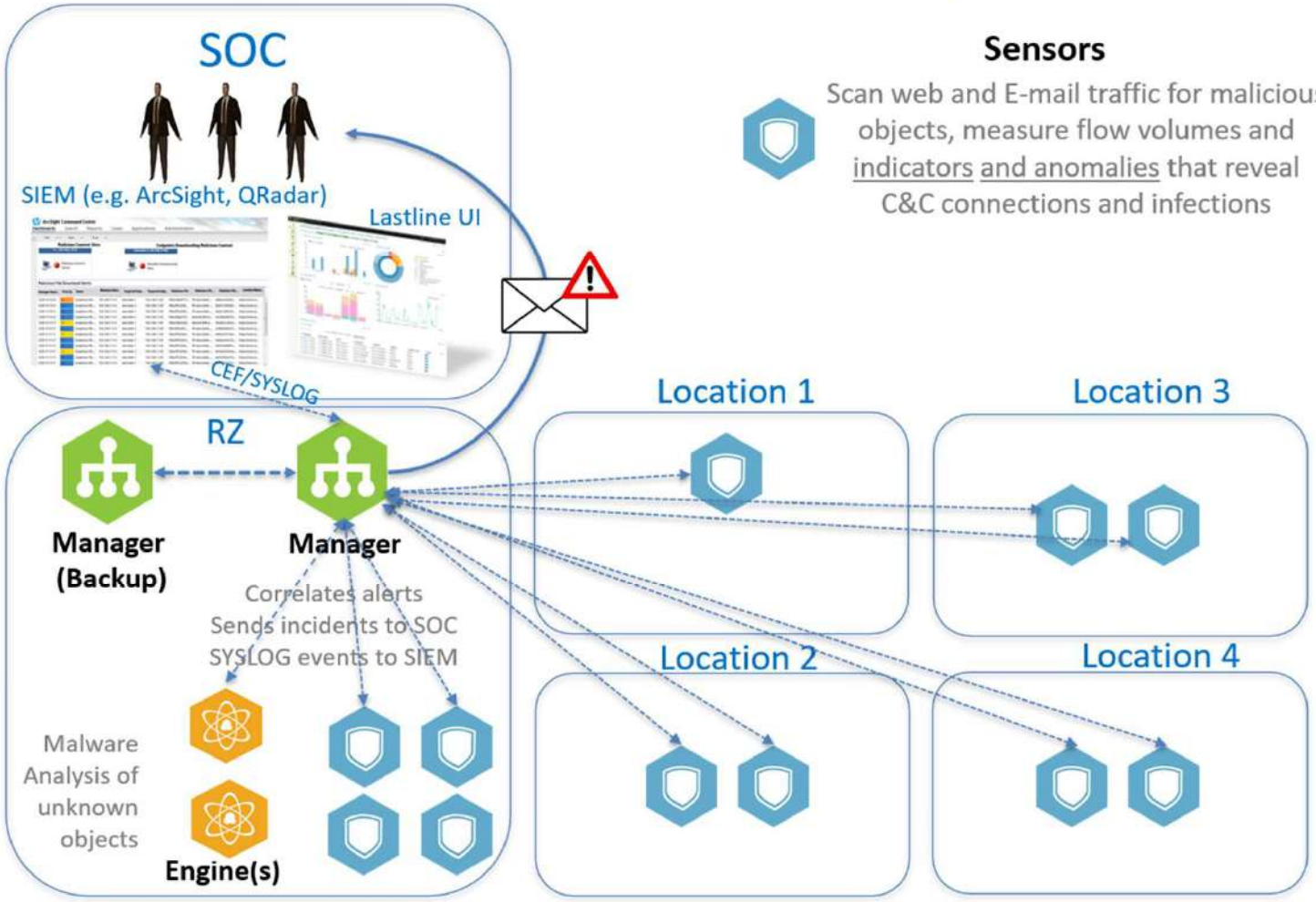
/

Threat Intel

API


On-Premise
lastline
Lastline proactively crawls the Internet for threats and updates the Sensor's knowledge base
Feedback for global threat intelligence
Analyzes unknown objects (programs and docs) with FUSE technology
Engine
Manager
Correlates alerts and produces actionable intelligence for SOC and IR Analysts
Drive-by attack
Spear-phishing
Command and control
Sensor
Scans traffic for indicators and anomalies that reveal C&C connections and infections

Distributed Detection – Central Analysis



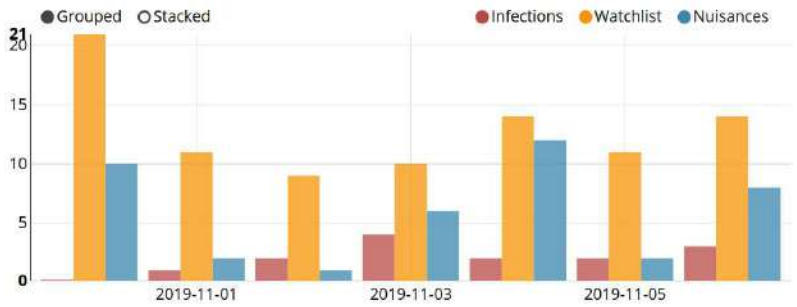
Dashboards

lastline

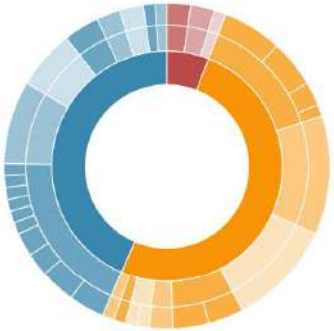
Martin Vozar
martin.vozar@soitron.com

Sensors Status: UP: 1 / 1 | MONITORING: 1 / 1 | ICAP: 0 / 1 | MAIL: 1 / 1 | INTEGRATIONS: 1 / 1

Infections in your network



Detected threats



Top 10 threats

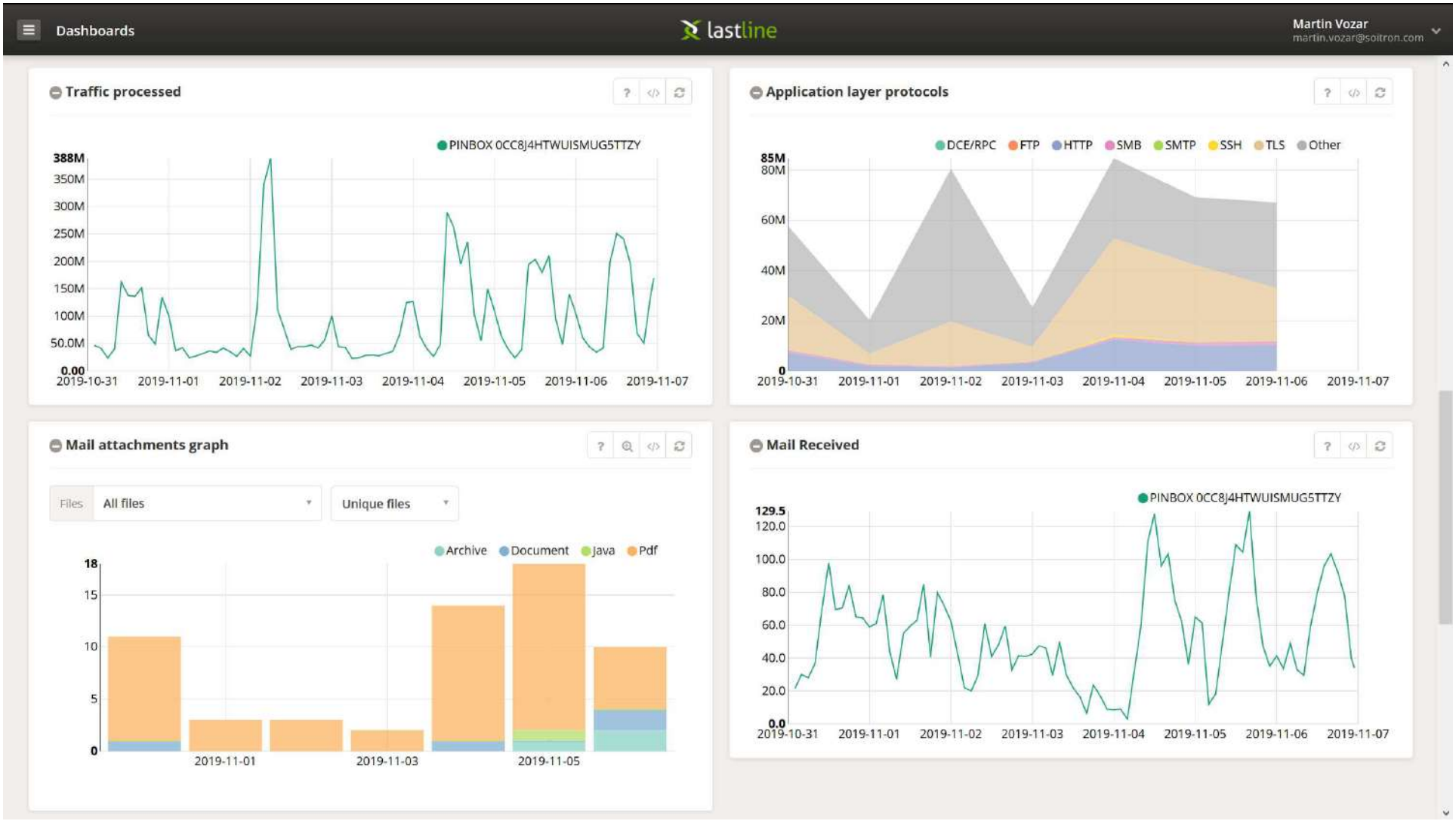
- 10 - Phishing
- 9 - Unknown Crypto Miner
- 7 - Phishing
- 5 - ETERNALBLUE
- 5 - URLhaus blacklisted host
- 4 - Potential ThinkPHP RCE Exploitation Attempt
- 3 - SQL Injection
- 3 - Web Application Attack
- 3 - Suspicious DNS-over-HTTPS resolution
- 3 - Suspicious Trusted Domain Enumeration

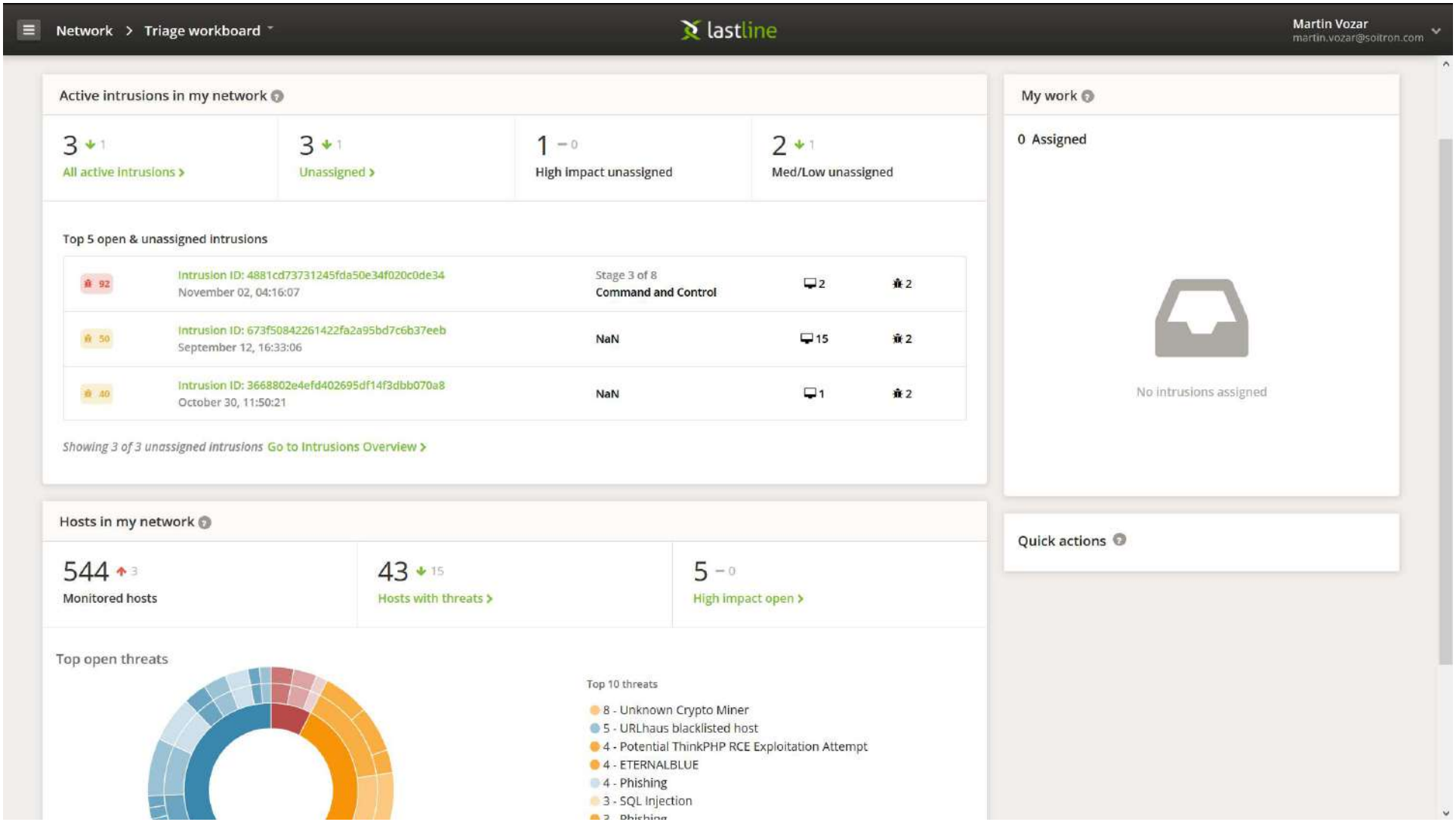
New unique detections

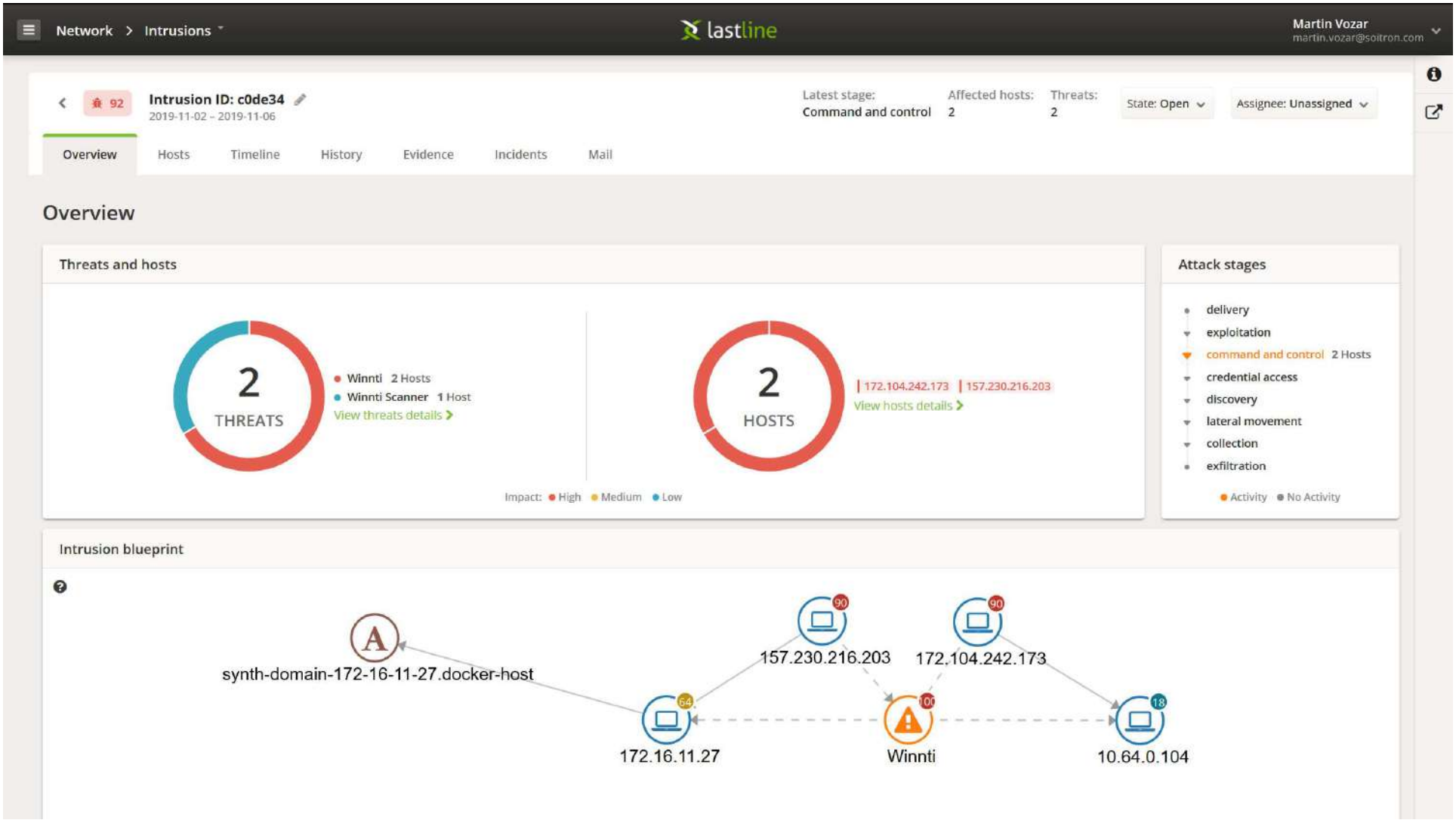
TIME	SCORE	DETECTION	THREAT	TYPE	REFERENCE
2019-10-31	65	llrules:1547129337431	NMAP	Lastline network signature	Event
5 days ago	25	llrules:10896391770652	SUSPICIOUS PASSWO...	Lastline network signature	Event
Today	25	jumpercursos.com.br	PHISHING	Blacklist	Event
5 days ago	25	llrules:10896309813532	SUSPICIOUS PASSWO...	Lastline network signature	Event
Today	22	momo2.test.zinimedia.com	URLHAUS BLACKLIST...	Blacklist	Event
Today	22	test.devel8.com	URLHAUS BLACKLIST...	Blacklist	Event
Today	22	youronlinempire.com	URLHAUS BLACKLIST...	Blacklist	Event

Downloaded files graph

Files | Files uploaded for analysis | Unique files


Dashboards
lastline
Martin Vozar
martin.vozar@soitron.com
Traffic processed
PINBOX 0CC8J4HTWUISMUG5TTZY
388M
350M
300M
250M
200M
150M
100M
50.0M
0.00
2019-10-31
2019-11-01
2019-11-02
2019-11-03
2019-11-04
2019-11-05
2019-11-06
2019-11-07
Application layer protocols
DCE/RPC
FTP
HTTP
SMB
SMTP
SSH
TLS
Other
85M
80M
60M
40M
20M
0
2019-10-31
2019-11-01
2019-11-02
2019-11-03
2019-11-04
2019-11-05
2019-11-06
2019-11-07
Mail attachments graph
Files
All files
Unique files
Archive
Document
Java
Pdf
18
15
10
5
0
2019-11-01
2019-11-03
2019-11-05
Mail Received
PINBOX 0CC8J4HTWUISMUG5TTZY
129.5
120.0
100.0
80.0
60.0
40.0
20.0
0.0
2019-10-31
2019-11-01
2019-11-02
2019-11-03
2019-11-04
2019-11-05
2019-11-06
2019-11-07

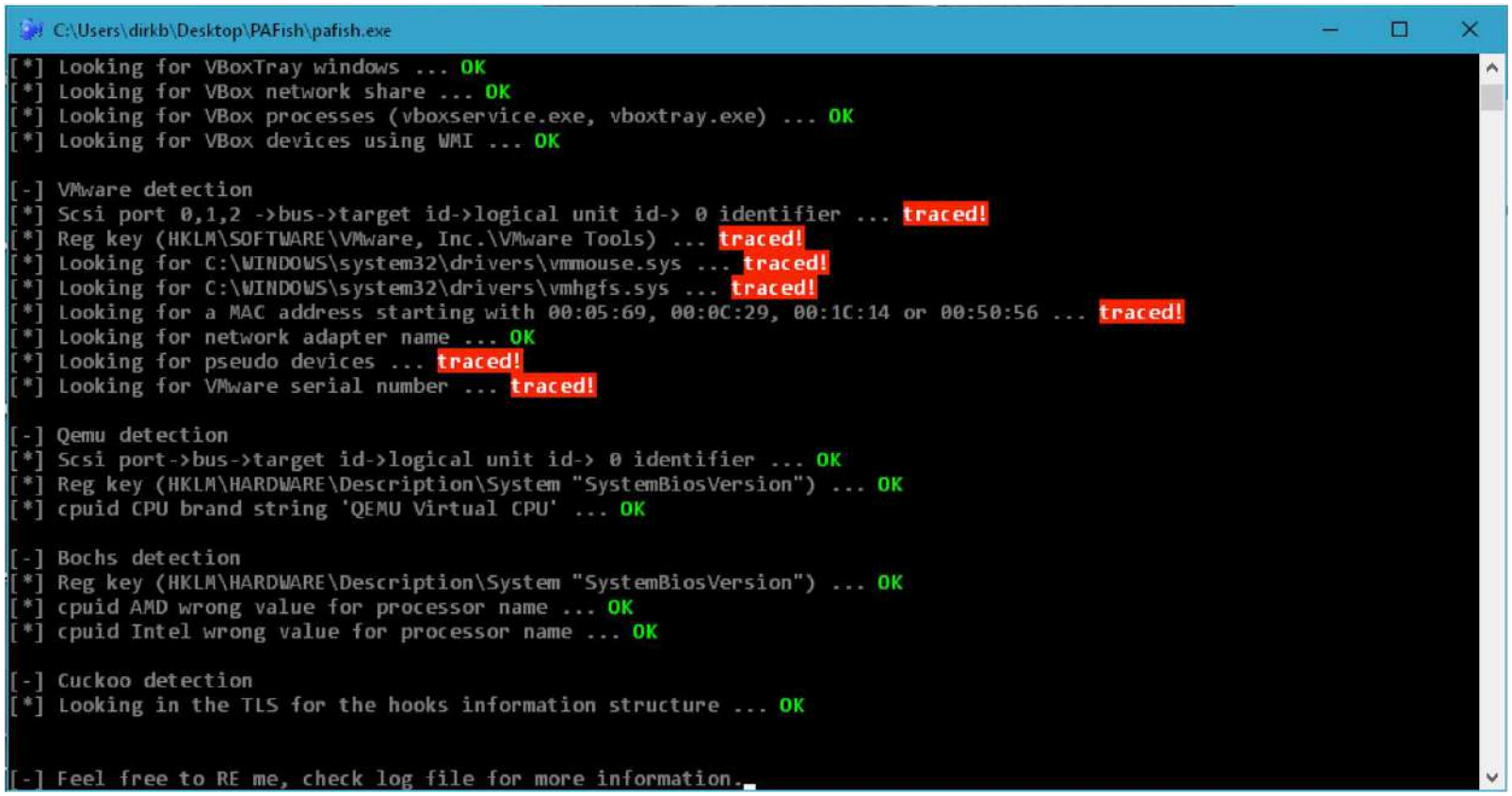

Network > Triage workboard
lastline
Martin Vozar
martin.vozar@soitron.com
Active intrusions in my network
3 ↓ 1
All active intrusions >
3 ↓ 1
Unassigned >
1 – 0
High impact unassigned
2 ↓ 1
Med/Low unassigned
Top 5 open & unassigned intrusions
92
Intrusion ID: 4881cd73731245fda50e34f020c0de34
November 02, 04:16:07
Stage 3 of 8
Command and Control
2
2
50
Intrusion ID: 673f50842261422fa2a95bd7c6b37eeb
September 12, 16:33:06
NaN
15
2
40
Intrusion ID: 3668802e4efd402695df14f3dbb070a8
October 30, 11:50:21
NaN
1
2
Showing 3 of 3 unassigned intrusions Go to Intrusions Overview >
My work
0 Assigned
No intrusions assigned
Hosts in my network
544 ↑ 3
Monitored hosts
43 ↓ 15
Hosts with threats >
5 – 0
High impact open >
Quick actions
Top open threats
Top 10 threats
8 - Unknown Crypto Miner
5 - URLhaus blacklisted host
4 - Potential ThinkPHP RCE Exploitation Attempt
4 - ETERNALBLUE
4 - Phishing
3 - SQL Injection


Network > Intrusions
lastline
Martin Vozar
martin.vozar@soitron.com
92
Intrusion ID: c0de34
2019-11-02 - 2019-11-06
Latest stage:
Command and control
Affected hosts:
2
Threats:
2
State: Open
Assignee: Unassigned
Overview
Hosts
Timeline
History
Evidence
Incidents
Mail
Overview
Threats and hosts
2
THREATS
Winnti 2 Hosts
Winnti Scanner 1 Host
View threats details
2
HOSTS
172.104.242.173
157.230.216.203
View hosts details
Impact: High Medium Low
Attack stages
delivery
exploitation
command and control 2 Hosts
credential access
discovery
lateral movement
collection
exfiltration
Activity No Activity
Intrusion blueprint
synth-domain-172-16-11-27.docker-host
157.230.216.203
172.104.242.173
172.16.11.27
Winnti
10.64.0.104

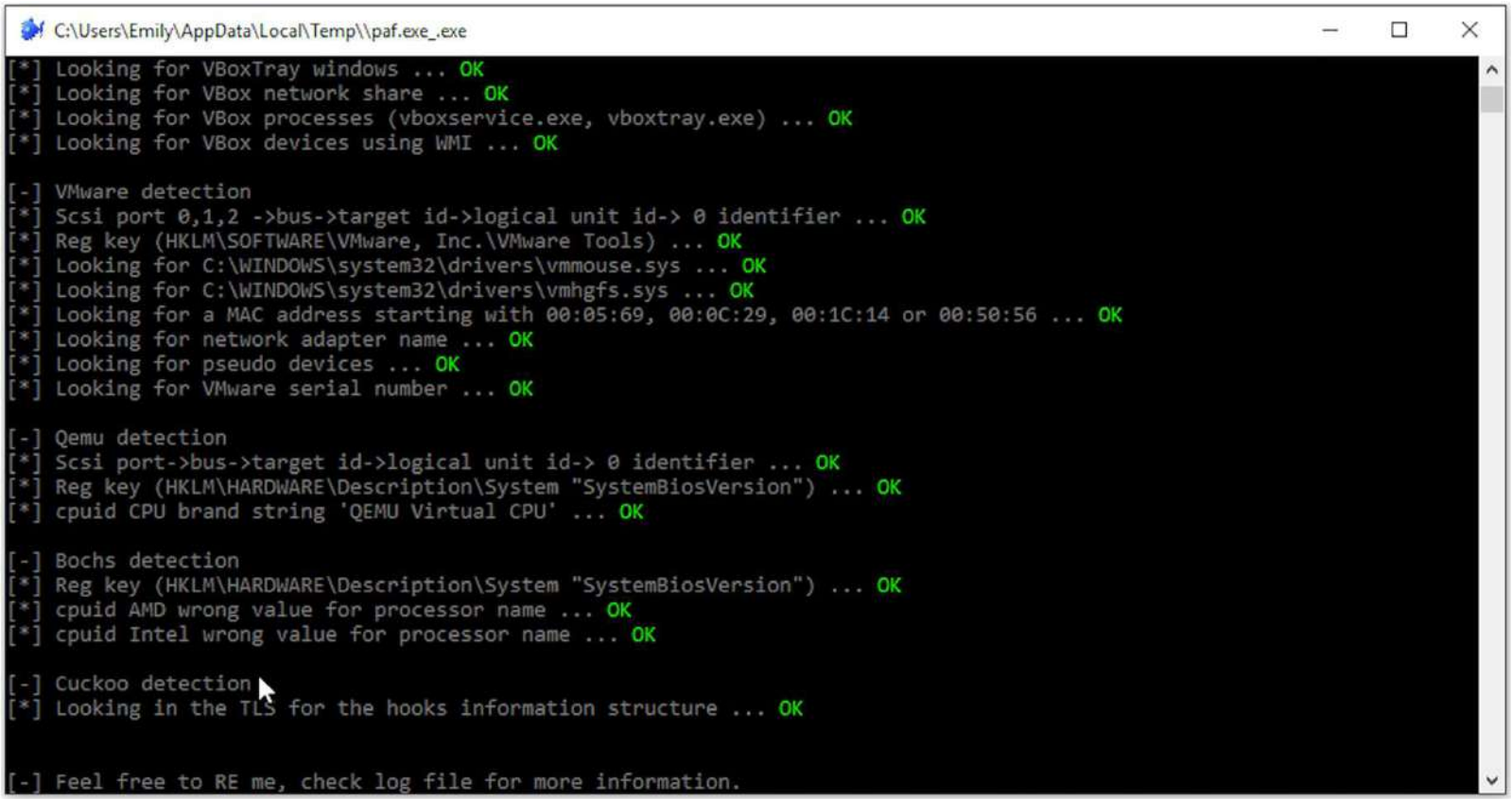
Kľúčové vlastnosti

1. Full System Emulation (FUSE)
2. Actionable Threat Intelligence
3. API (integrácia)

#1 FUSE: Príklad PAFISH (tradičný sandbox)



#1 FUSE: Príklad PAFISH (Lastline FUSE)



- PAFISH
- Bodové ohodnotenie každej podozrivej činnosti
- Výsledné skóre na základe jednotlivých bodov

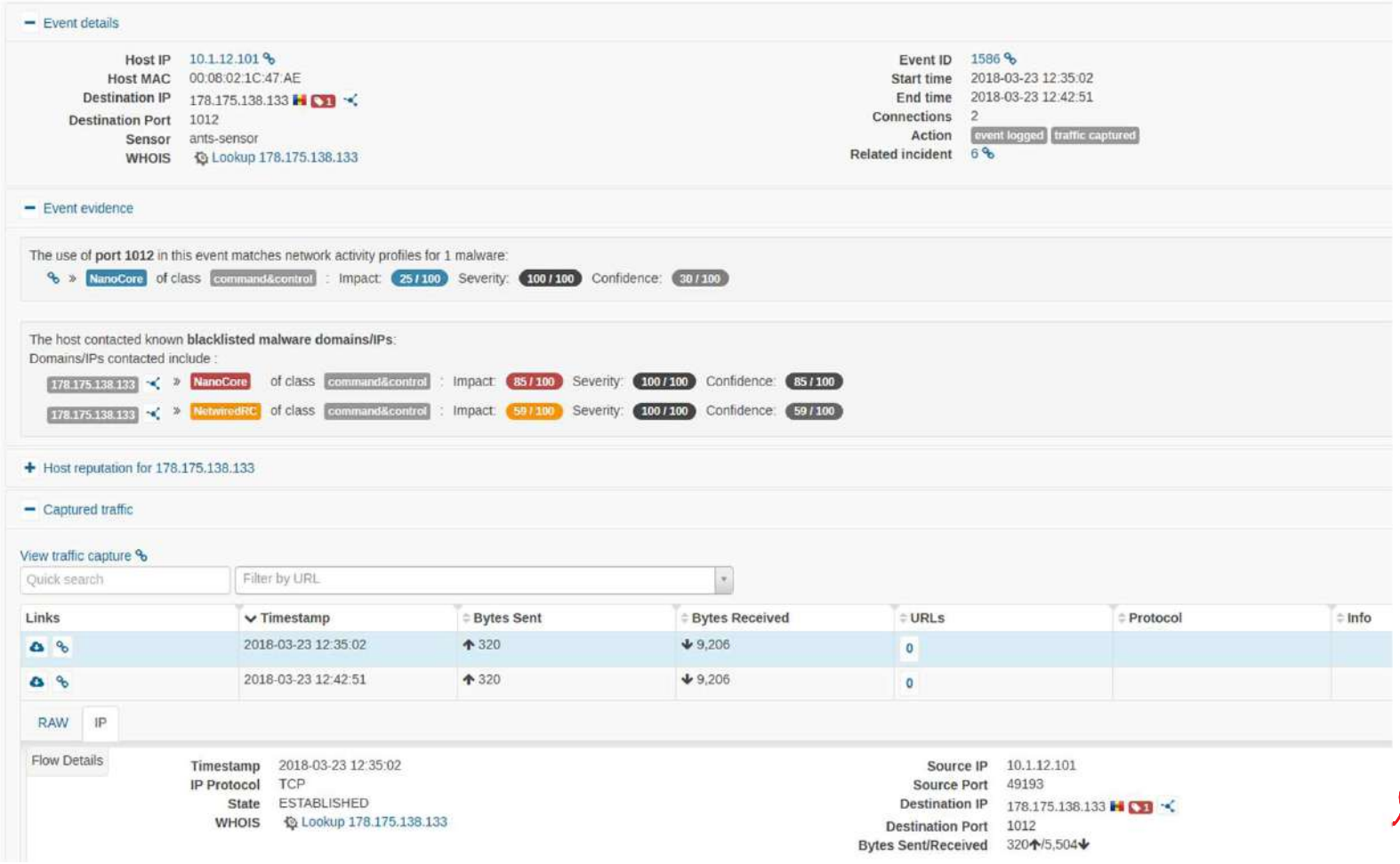
Analysis Overview

Severity	Type	Description
80	Evasion	Trying to detect analysis virtual environment (window name detection)
80	Evasion	Trying to detect analysis virtual environment (user detection)
80	Evasion	Trying to detect analysis virtual environment (malware analysis sandbox detection)
80	Evasion	Trying to detect analysis virtual environment (installed applications detection)
80	Evasion	Trying to detect analysis virtual environment (guest modules detection)
80	Evasion	Trying to detect analysis virtual environment (drivers detection)
80	Evasion	Trying to detect analysis virtual environment (analysis path detection)
80	Evasion	Trying to detect analysis virtual environment (HDD detection)
80	Evasion	Trying to detect analysis virtual environment (BIOS detection)
30	Search	Retrieving the user account name
30	Search	Enumerates running processes
30	Evasion	Timing Detection (rdtsc_GetTickCount)
30	Evasion	Potential detection of virtual environment (Sandboxie)
30	Evasion	Potential detection of virtual environment (IOCTL_DISK_GET_LENGTH_INFO)
30	Evasion	Detecting the presence of WINE
30	Evasion	Detecting sandboxes by checking registry keys artifacts
30	Evasion	Detecting analysis environment by checking sandbox name
30	Evasion	Ability to detect sandbox by checking mouse activity
30	Evasion	Ability to detect if Sleep() function is patched
20	Evasion	Searching for specific processes: vmmouse.sys (analysis tool detection)
1	Memory	Writing through direct access to physical drives

#2 Actionable Threat Intelligence

- Correlated APT information rolls up to network incidents provides drill down to individual malware events (multiple events – single incident)
- APT threat severity level identifies high priority infections
- Less noise means quicker remediation with fewer resources

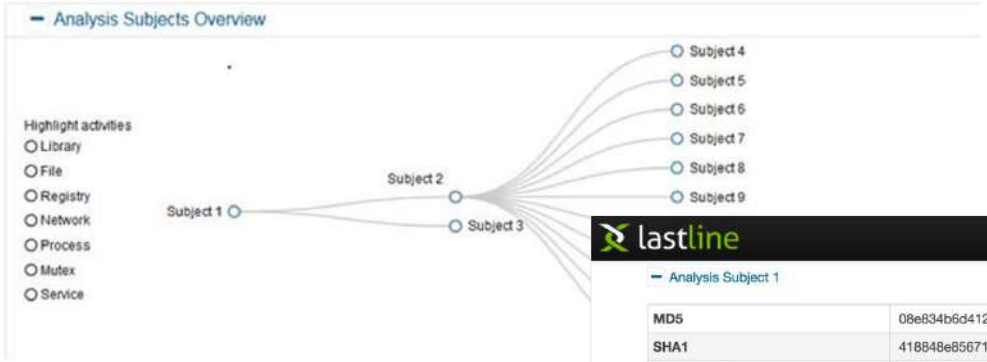
#2 Actionable Threat Intelligence – Detailný pohľad na incident



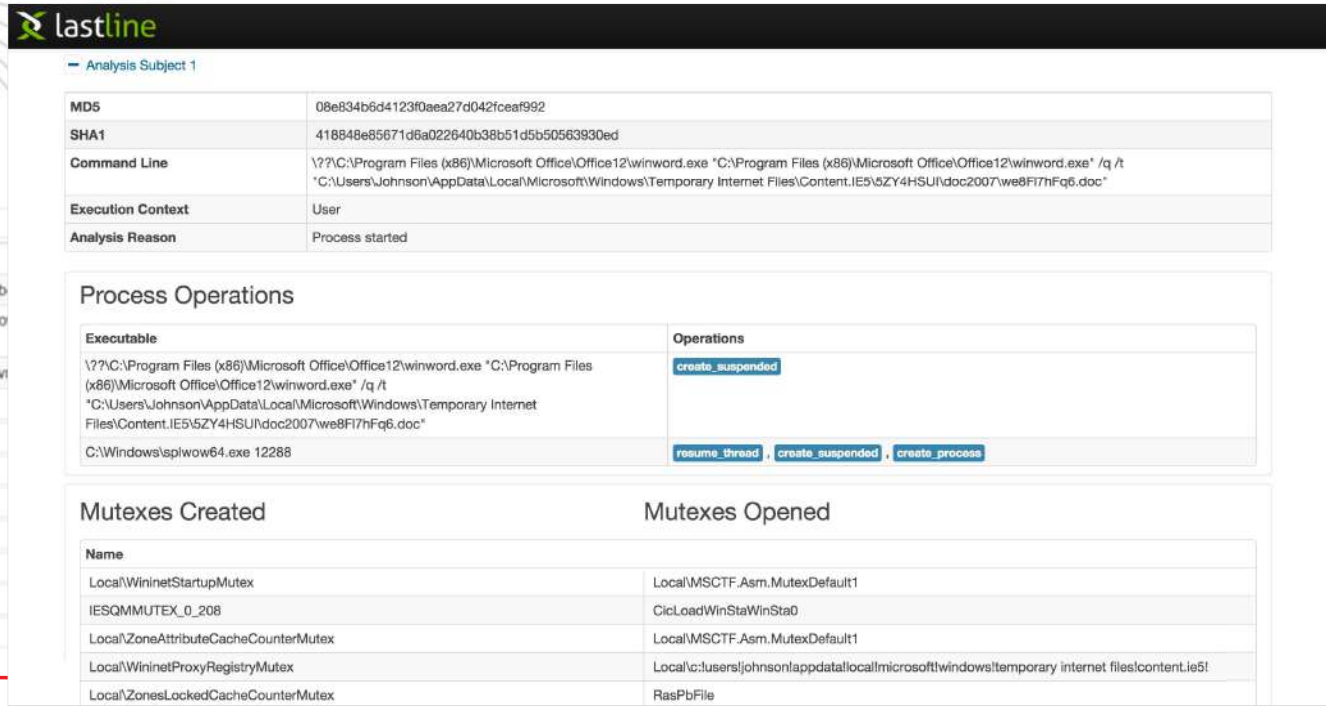
SOITRON

#2 Actionable Threat Intelligence – Forenzná analýza

Analysis Subjects Tree View:



Analysis Subject Details:

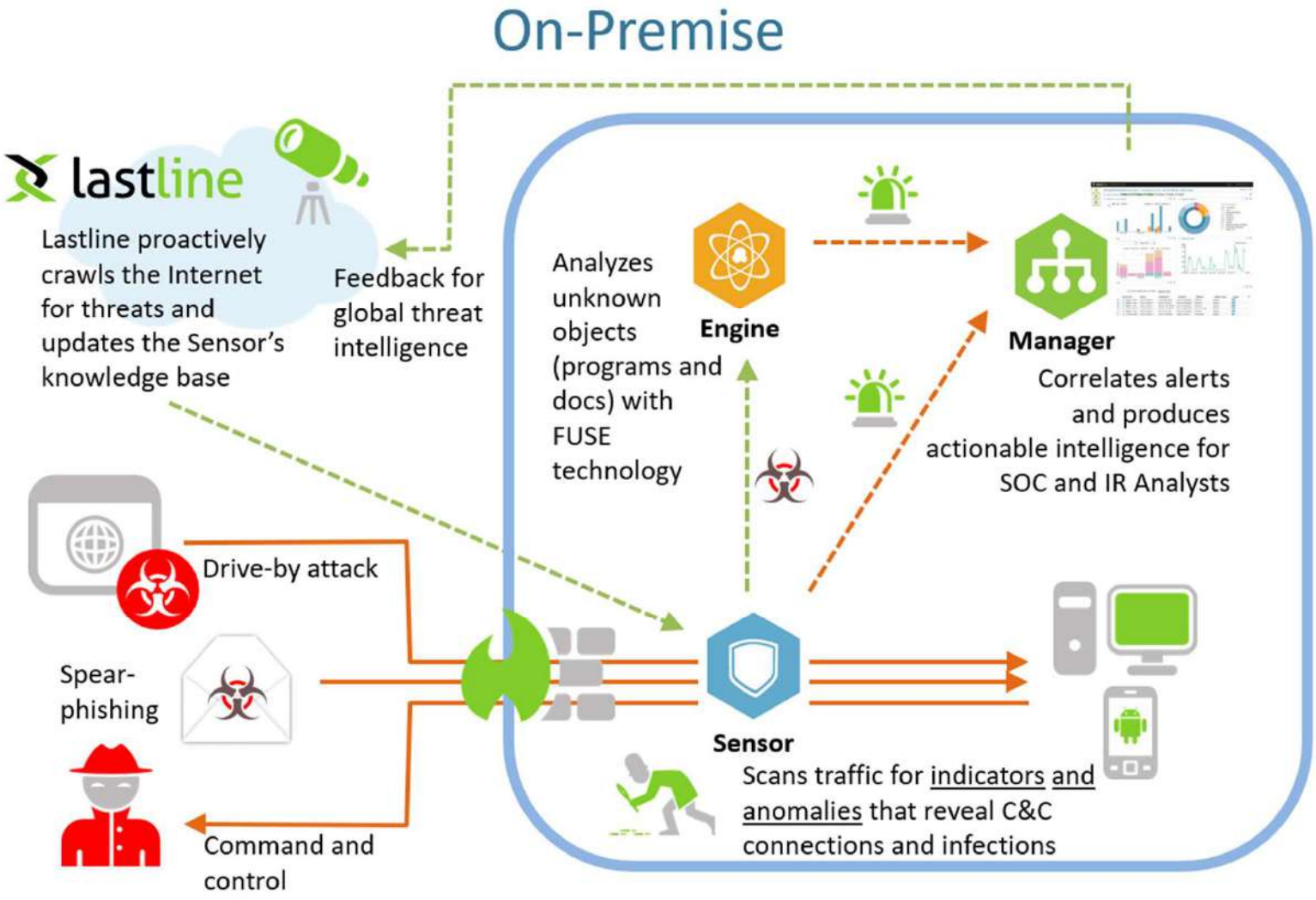


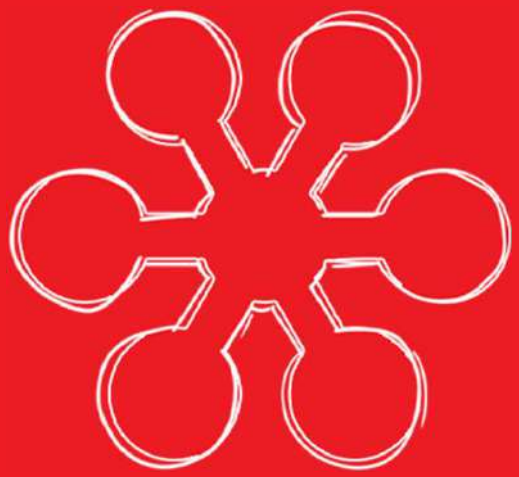
#2 Actionable Threat Intelligence – Activity Graph

#3 API

- ✓ Download malware analysis
- ✓ Integrate with network Firewall, IPS & e-mail security solutions
- ✓ Add FUSE to the Endpoint
- ✓ Events to SIEM visibility/workflow
- ✓ Can update Lastline Threat Intelligence (e.g. reputations)

Návrh vhodného riešenia (príďte s nami konzultovať)


On-Premise
lastline
Lastline proactively crawls the Internet for threats and updates the Sensor's knowledge base
Feedback for global threat intelligence
Analyzes unknown objects (programs and docs) with FUSE technology
Engine
Manager
Correlates alerts and produces actionable intelligence for SOC and IR Analysts
Drive-by attack
Spear-phishing
Command and control
Sensor
Scans traffic for indicators and anomalies that reveal C&C connections and infections



SOITRON