

# 打造由情报分析驱动的ISOC

郑聿铭

Splunk中国区高级架构师

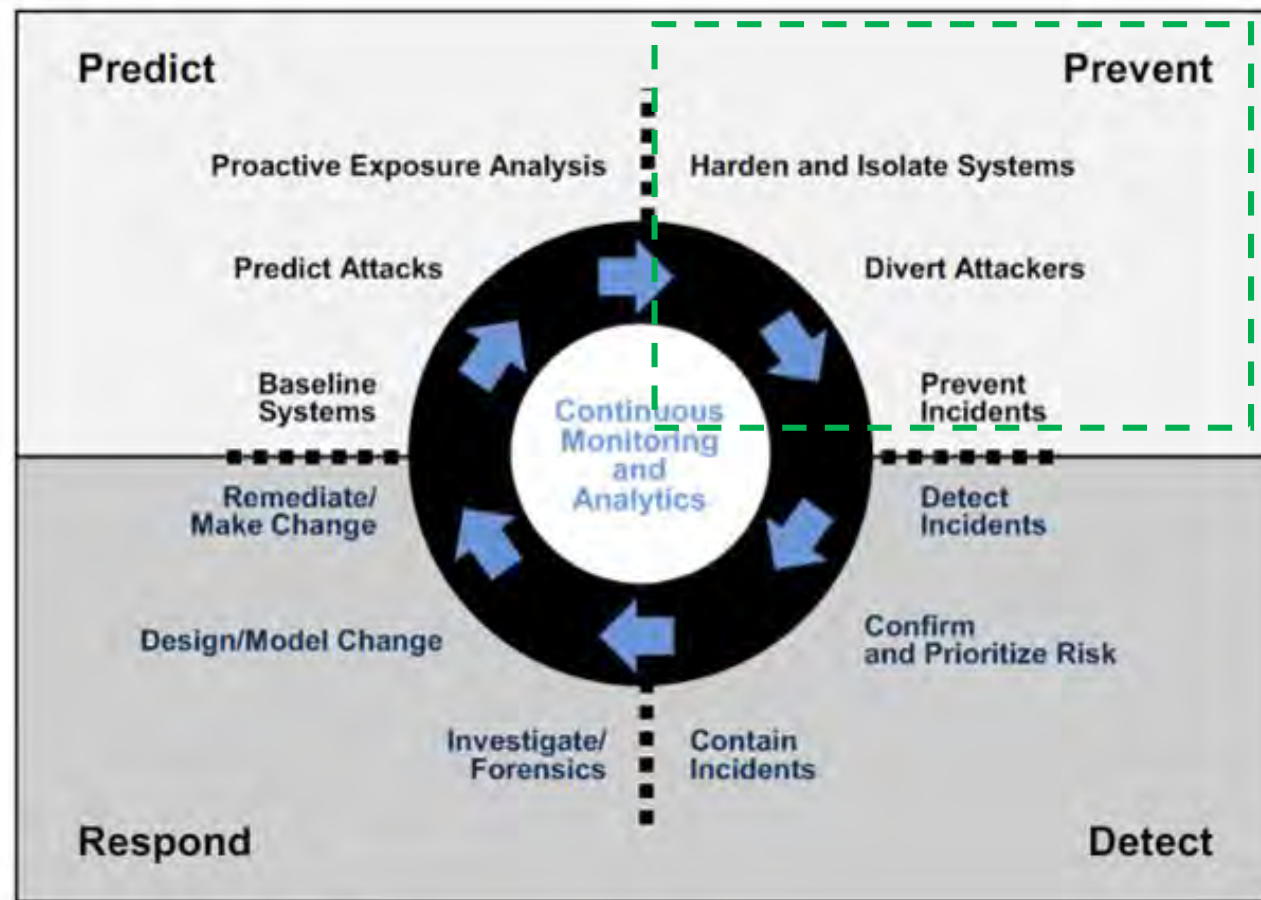
# 何谓ISOC

- ISOC = Intelligence-Driven Security Operations Center ,  
**智能化安全运营中心**



# 传统的“防御”手段不足以应对现今的高级威胁

Critical capabilities of Gartner's adaptive security architecture



Source: Gartner (February 2014)

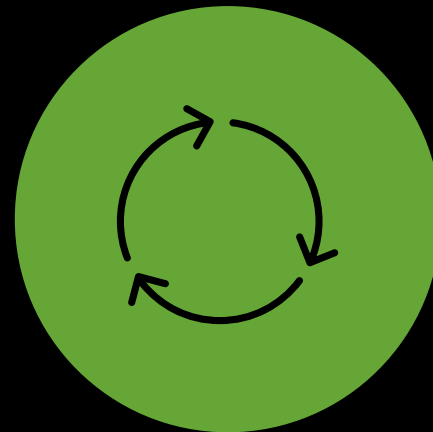


# 安全仍然处于被动防御的形式



## 工具

仅仅是“告警”  
而不是“洞察”



## 流程

调查过程  
不够优化

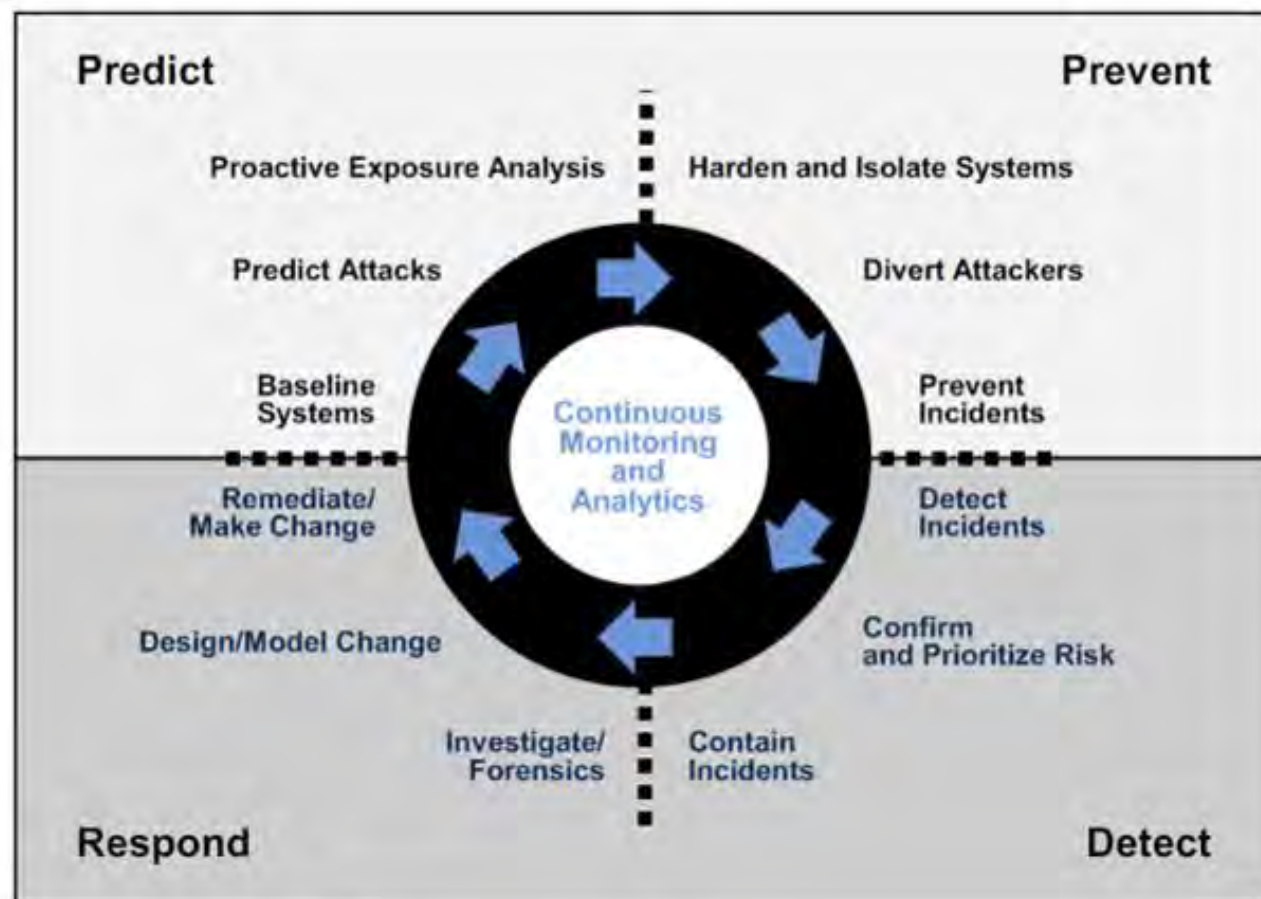


## 人员

告警泛滥  
疲于应对

# 如今我们需要利用情报与分析来提供智能驱动的安全 (检测, 响应和预测)

Critical capabilities of Gartner's adaptive security architecture



Source: Gartner (February 2014)



# ISOC的五大特征

- 部署自适应安全架构
- 在战略和战术上运营威胁情报
- 通过高级分析将安全智能落地
- 极尽所能地实现自动化
- 捕猎和调查（侦查与猎取）

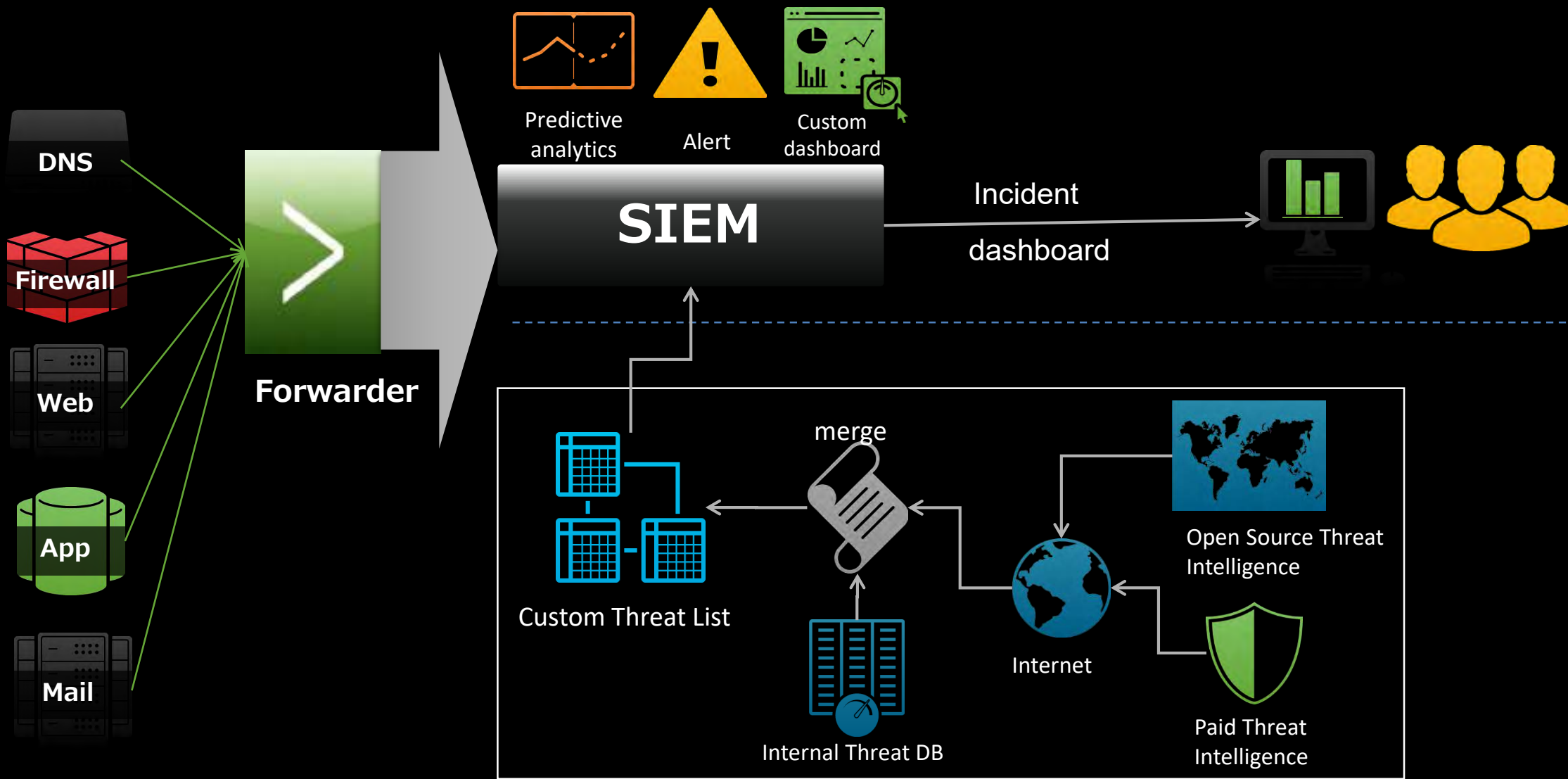
Hypothesis

IOC

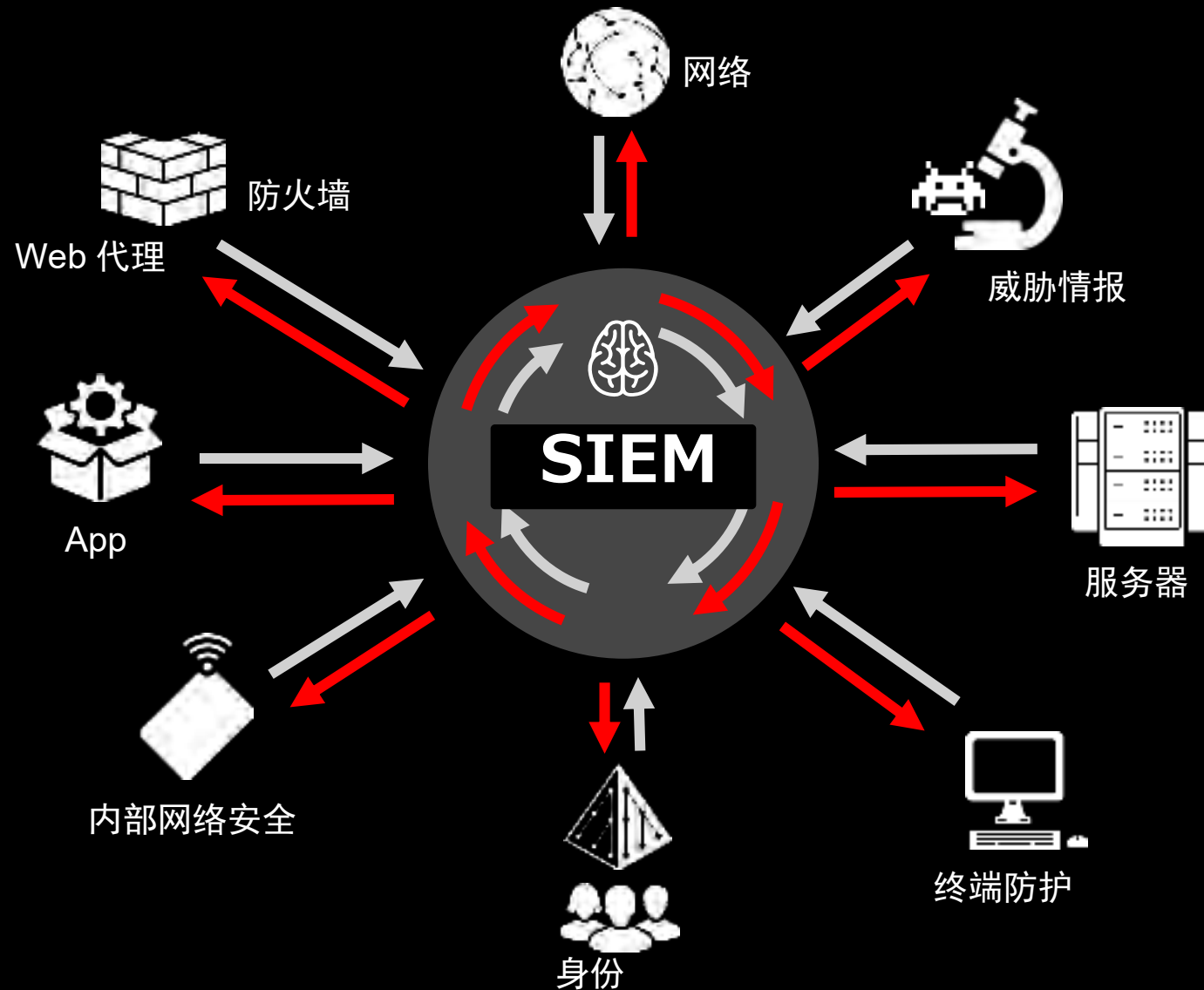
Analytics

Source : Gartner Nov2015, the five characteristics of an Intelligence-Driven Security Operations Center

# ISOC典型框架模型



# 新一代SIEM - 安全分析的中枢神经





# Gartner SIEM 魔力象限领导者

2016 领导者, 技术前瞻性第一位  
2015 领导者, 唯一在技术前瞻性维度取得进步的SIEM厂商  
2014 领导者, 执行能力第三位  
2013 领导者  
2012 挑战者  
2011 特定领域者 (Niche Player)

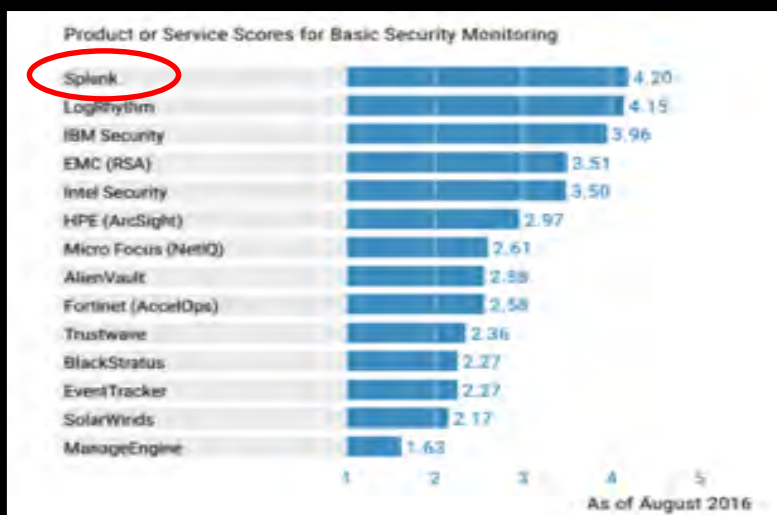
Splunk从2011年起进入Gartner SIEM领域, 并迅速发展, 2013年进入SIEM领导者象限, 并连续四年不断取得进步, 2016年技术前瞻性维度排名第一。



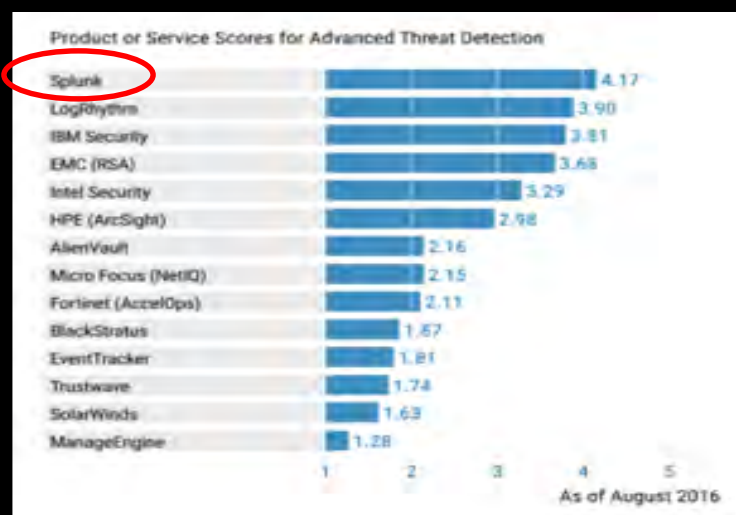
# Gartner 2016年SIEM解决方案关键能力报告



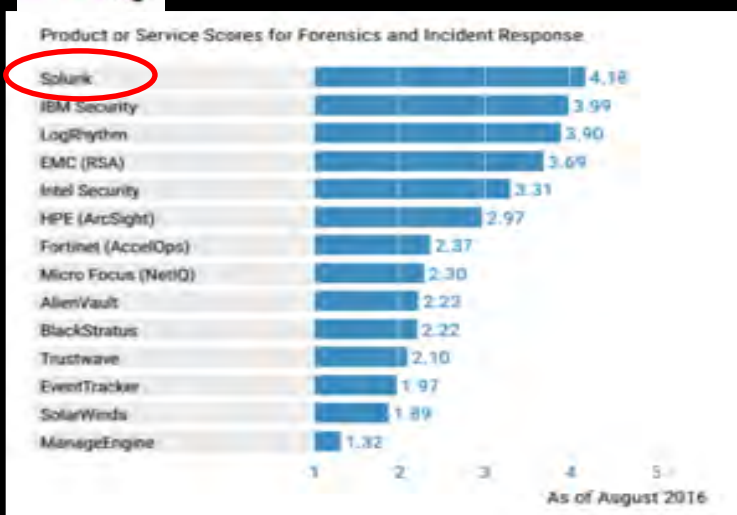
## 基础安全监控



## 高级威胁检测



## 取证&事件响应



# Splunk强大的安全智能平台

近500个  
安全应用

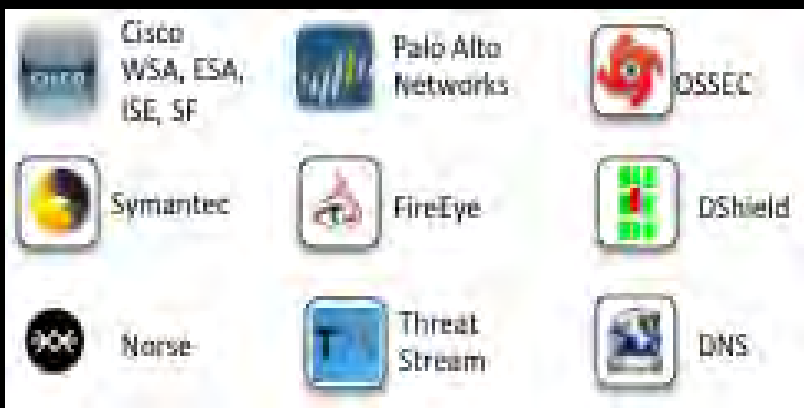
## SPLUNK FOR ENTERPRISE SECURITY

## SPLUNK所打造的应用

安全厂商

社群

开源

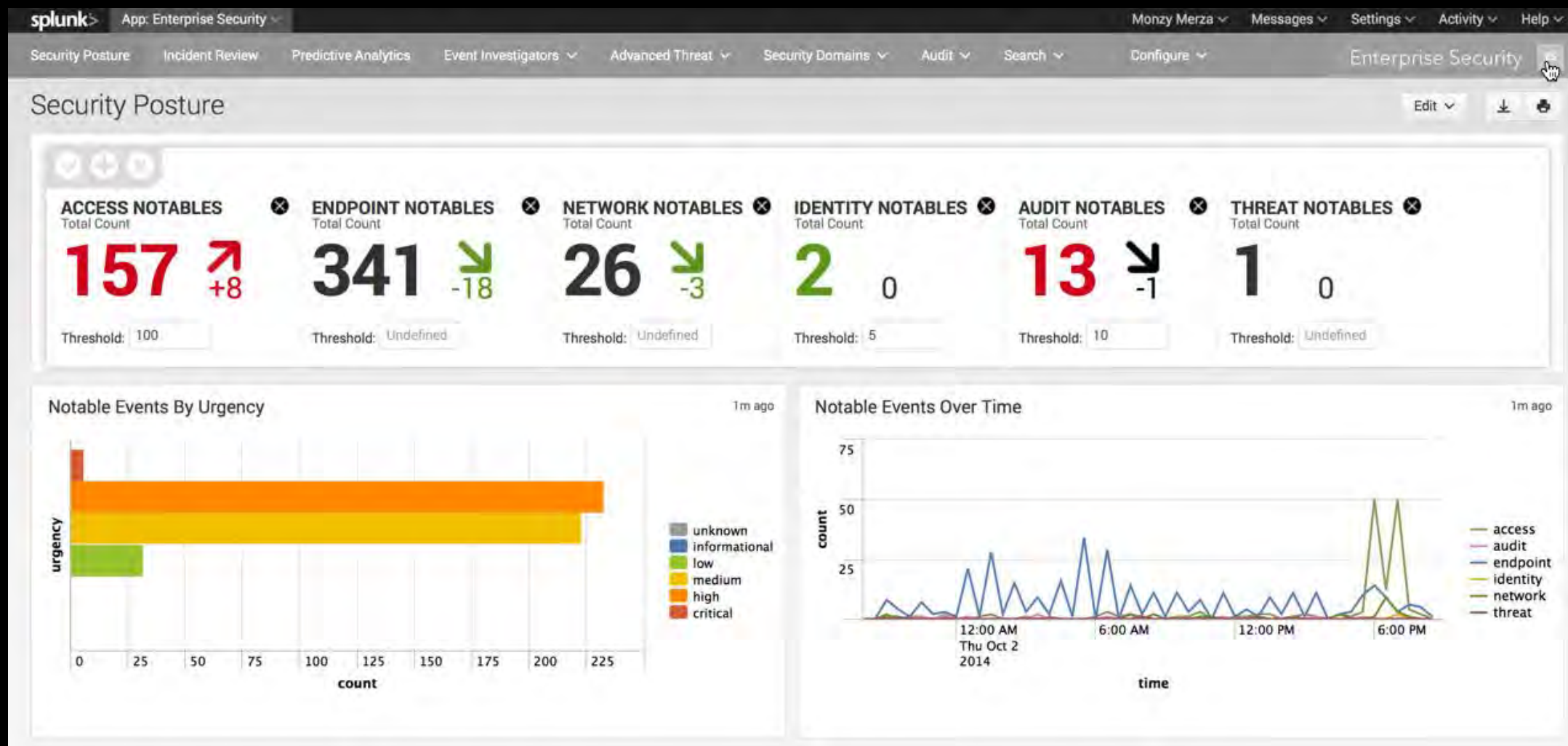


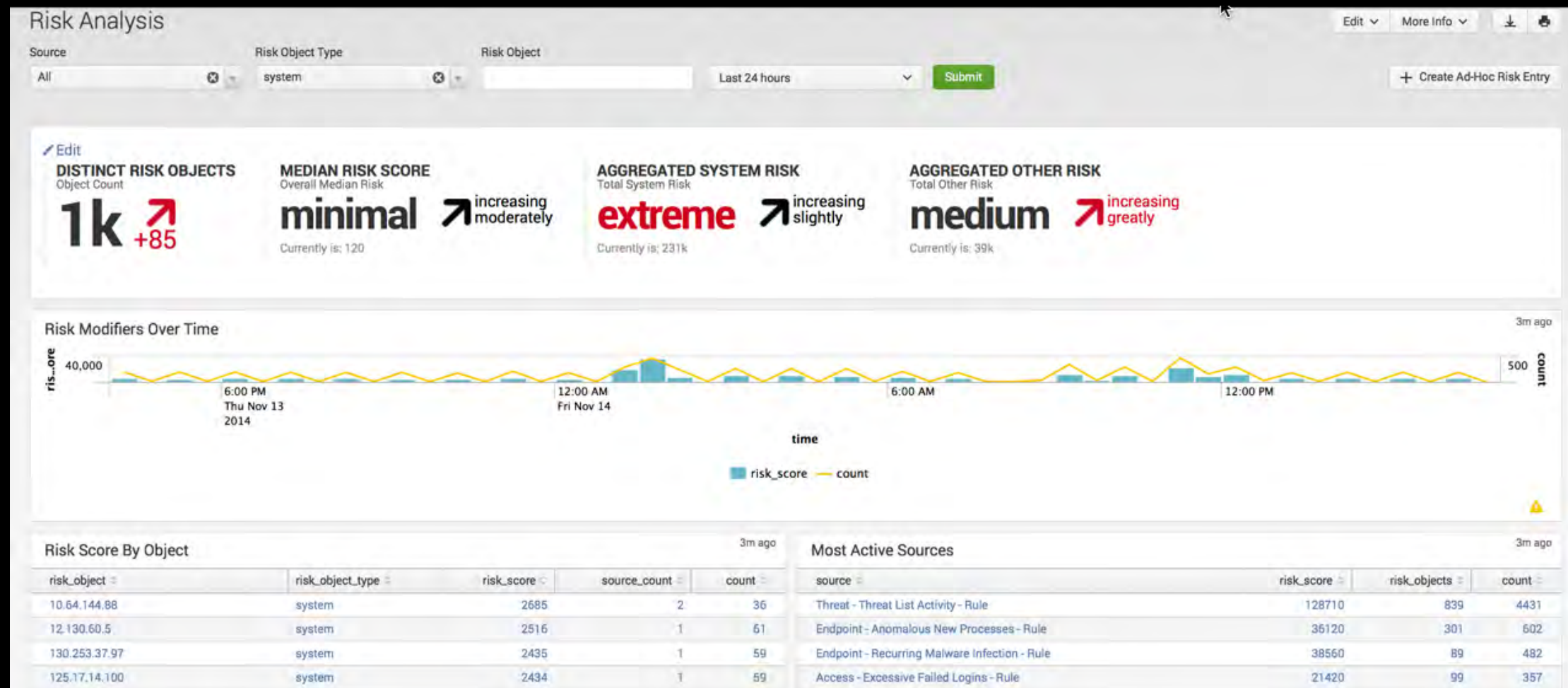
- STM** Wire (NFT) 数据
- INF** Windows (host/inf) 数据
- \*nix** Unix与 Linux数据
- RDBMS** (所有)数据
- EX** Exchange (email, inf)数据
- CEF** SIEM数据
- >** 还有更多...

## SPLUNK ENTERPRISE (核心)



# 安全态势实时监控





# 快速的事件审查及调查

## Incident Review

**Urgency**

CRITICAL	12
HIGH	610
MEDIUM	595
LOW	5164
INFO	5

**Status**  
All

**Owner**  
All

**Security Domain**  
All

**Name**

**Search**

**Time**  
Last 24 hours

Job

✓ 6,386 events (11/13/14 3:00:00.000 PM to 11/14/14 3:43:33.000 PM)

Format Timeline    1 hour per column

Edit all selected | Edit all 6386 matching events \* prev 1 2 3 4 5 6 7 8 9 10 next \*

i	<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	<input type="checkbox"/>	11/14/14 3:40:06.000 PM	Network	Unroutable Activity Detected (0.181.63.8)	Medium	New	unassigned	⌵
>	<input type="checkbox"/>	11/14/14 3:40:06.000 PM	Network	Unroutable Activity Detected (0.83.179.88)	Medium	New	unassigned	⌵
>	<input type="checkbox"/>	11/14/14 3:40:06.000 PM	Network	Unroutable Activity Detected (0.191.168.117)	Medium	New	unassigned	⌵
>	<input type="checkbox"/>	11/14/14 3:40:06.000 PM	Network	Unroutable Activity Detected (0.140.190.218)	Medium	New	unassigned	⌵
>	<input type="checkbox"/>	11/14/14 3:35:05.000 PM	Endpoint	High Or Critical Priority Host With Malware Detected	High	New	unassigned	⌵
>	<input type="checkbox"/>	11/14/14 3:27:31.000 PM	Endpoint	High Or Critical Priority Host With Malware Detected	High	New	unassigned	⌵
>	<input type="checkbox"/>	11/14/14 3:22:26.000 PM	Endpoint	High Or Critical Priority Host With Malware Detected	High	New	unassigned	⌵

# 直观的可视化事件调查



# 快速灵活地响应操作

The screenshot displays the Splunk interface with a search results table. The selected event is expanded, showing its details and a list of available actions. The 'Stream Capture' action is highlighted with a red border.

Events (4) | Patterns | Statistics | Visualization

Format Timeline ▾ | - Zoom Out | + Zoom to Selection | × Deselect | 1 minute per column

List ▾ | Format ▾ | 20 Per Page ▾

< Hide Fields | All Fields

i	Time	Event
▼	10/30/14 1:50:43.000 AM	2014-10-30 01:50:43 10.11.36.20 39961 186 TCP_NC_MISS 200 200 39894 21 vf.travel HTTP/1.0 225 http://208.49.52.149/idle/mkwmYD8QmB8+WhnR/1340 Flash" -

Selected Fields

- a host 1
- a source 1
- a sourcetype 1
- a src 1

Interesting Fields

- a action 1
- a app\_version 1
- # bytes\_in 1
- # bytes\_out 1

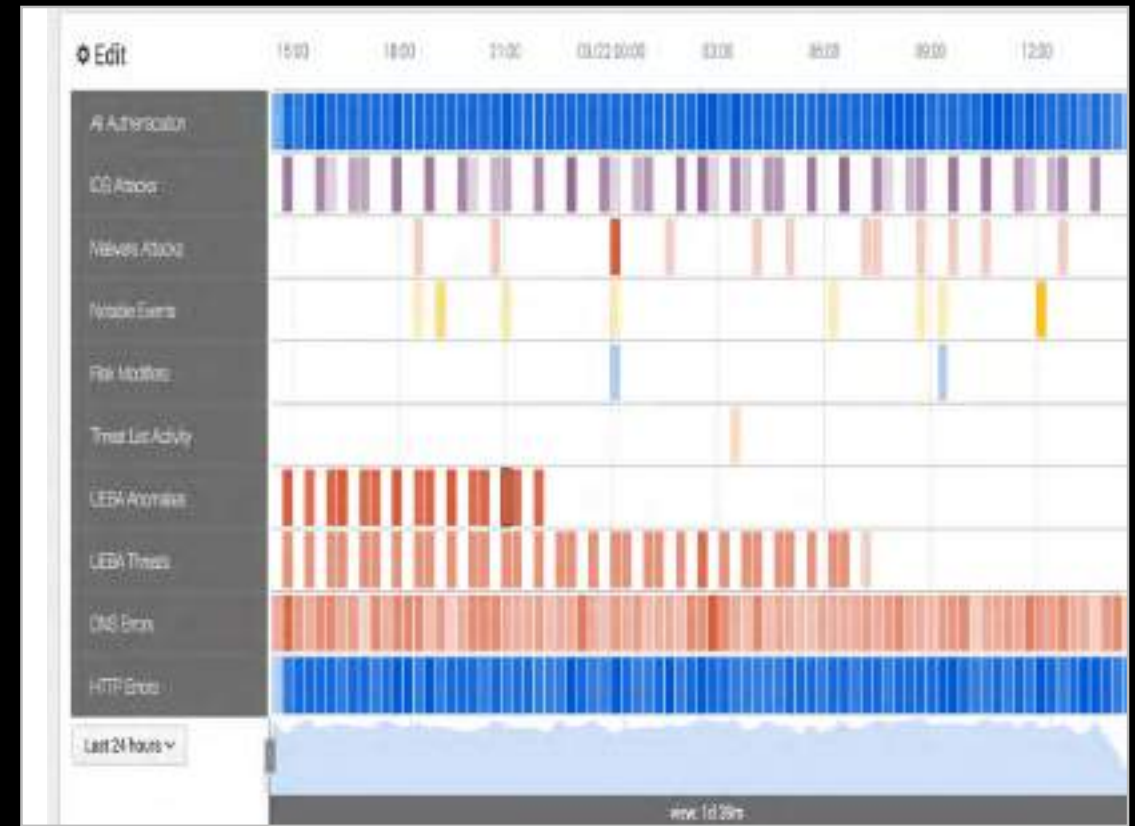
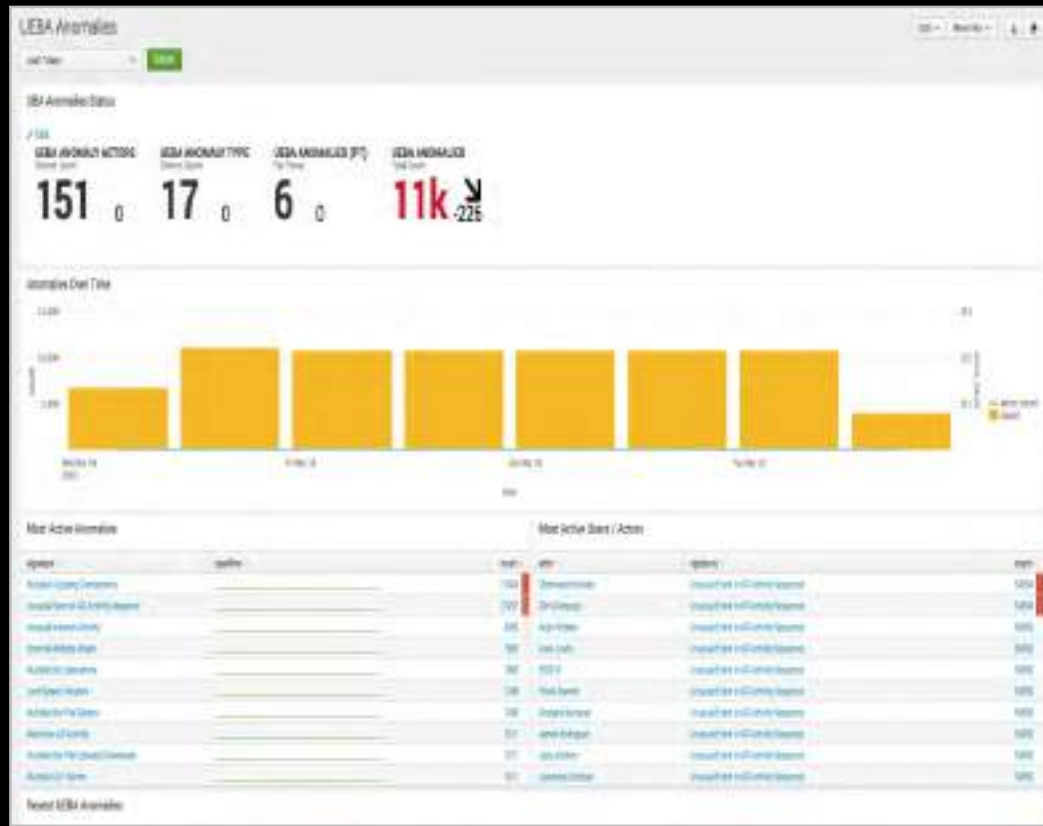
Event Actions ▾

Type	Field	Value
Selected	host ▾	soln-esnightly1.sv.splunk.com
	source ▾	/usr/local/bamboo/splunk-install/current/var/spool
		at
	sourcetype ▾	bluecoat
	src ▾	10.11.36.20
Event	action ▾	TCP_NC_MISS

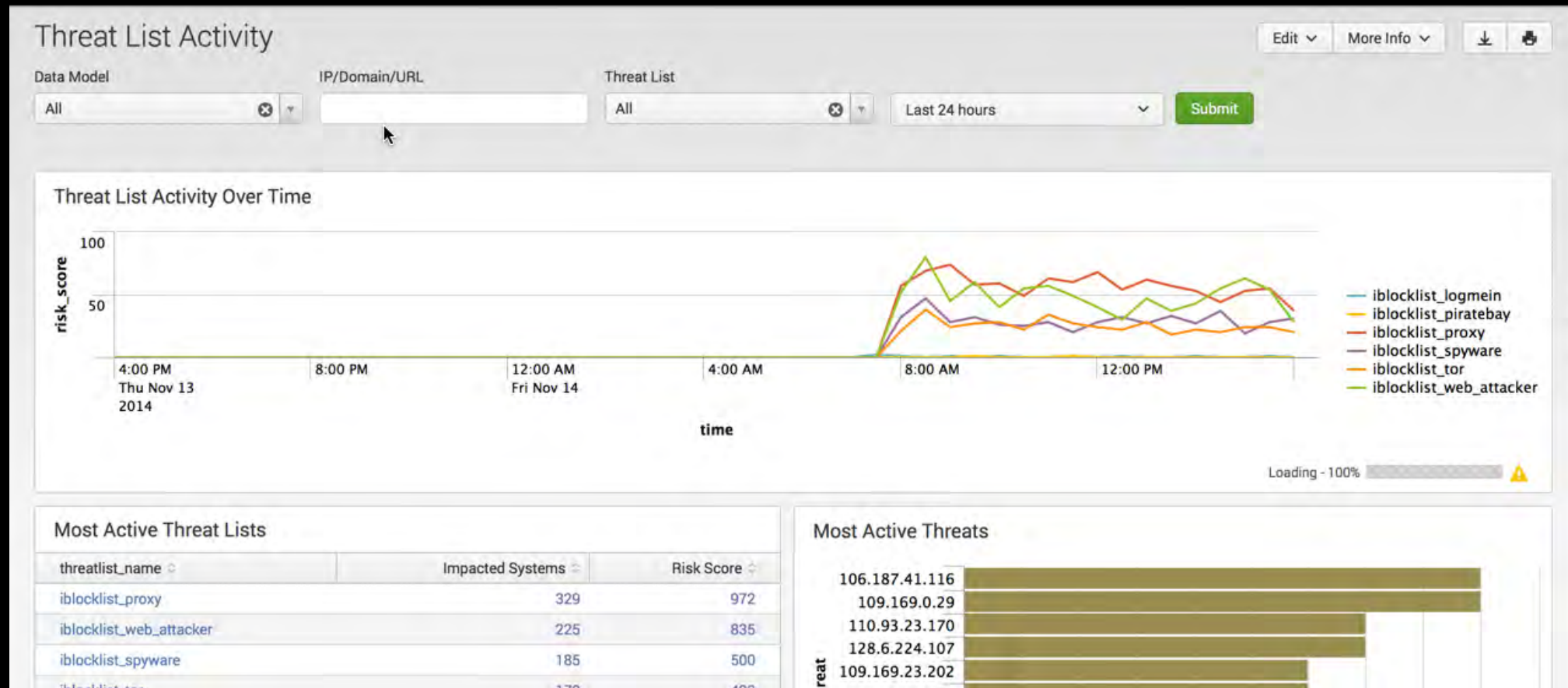
- Malware Search
- Nbtstat 10.11.36.20
- Nslookup 10.11.36.20
- Ping 10.11.36.20
- Stream Capture**
- Traffic Search (as destination)
- Traffic Search (as source)
- Update Search
- Vulnerability Search
- Web Search (as destination)



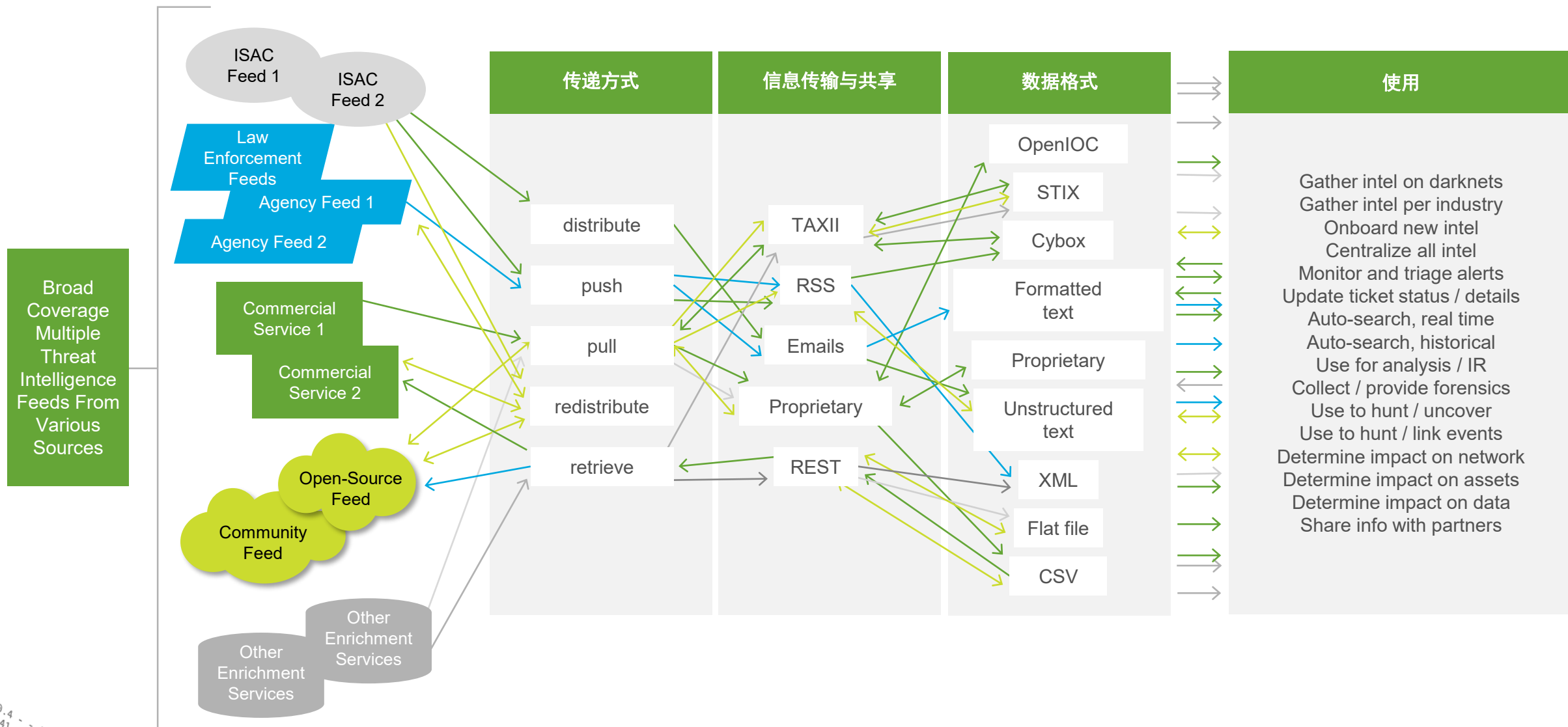
# 集成UEBA异常检测功能



# 集成威胁情报的管理和使用



# 让威胁情报的管理和使用不再复杂

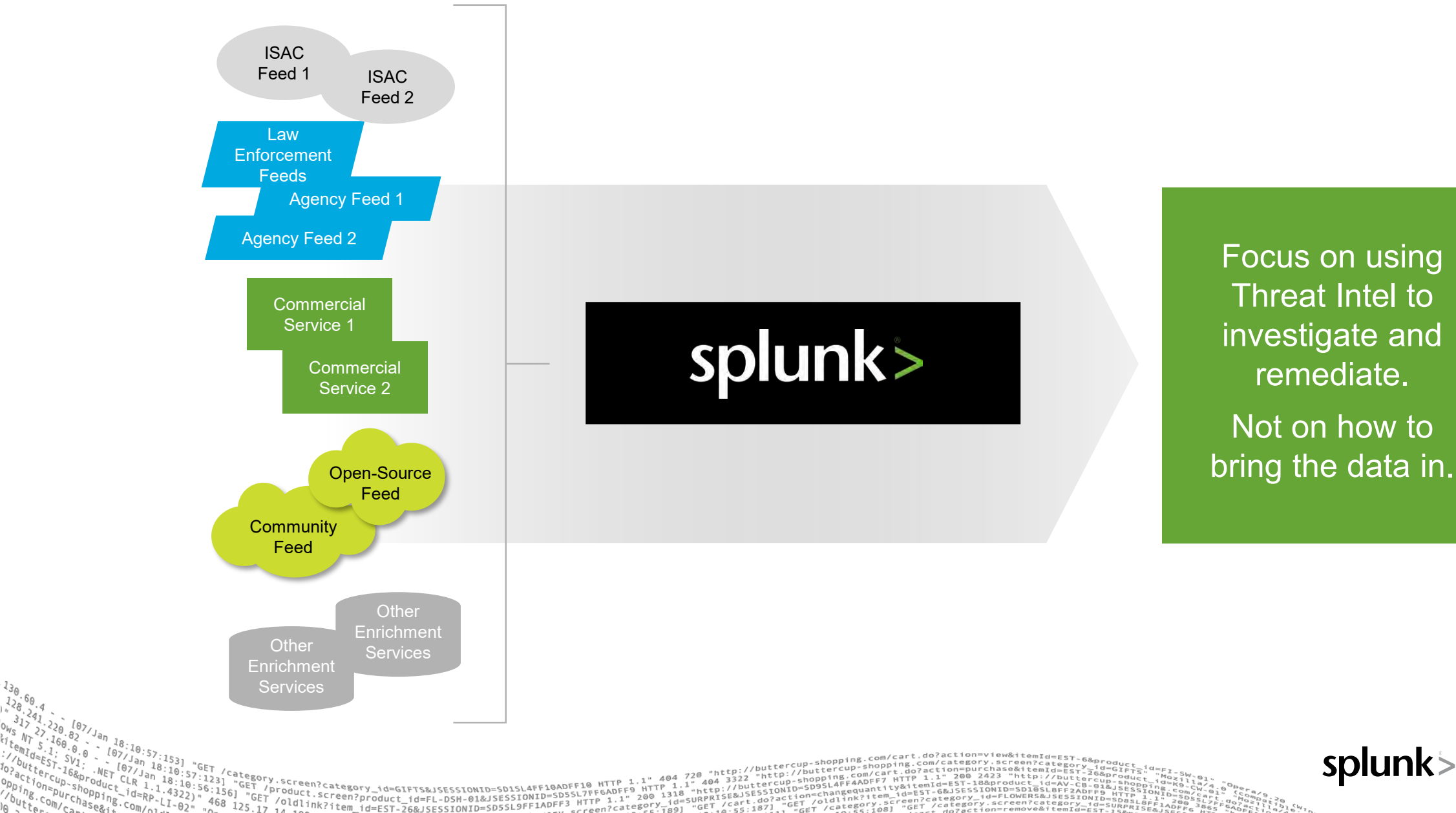


```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14.11link?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&is.com/c1"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/4.0 (compatible; MSNbot) 317 27.160.0.0 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14.11link?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&is.com/c1"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 14.11link?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&is.com/c1"

```

# 让威胁情报的管理和使用不再复杂



Focus on using  
Threat Intel to  
investigate and  
remediate.

Not on how to  
bring the data in.

# Splunk内置威胁情报框架

## 使用全面匹配的威胁情报来找到隐藏的 IOC



# 多个威胁情报来源管理

## Threat Lists

Data inputs » Threat Lists

New

Showing 1-17 of 17 items

Results per page 25

Name	Type	Description	URL	Interval	Status	Actions
<a href="#">emerging_threats_compromised_ip_blocklist</a>	malicious	Emerging Threats compromised IPs blocklist	<a href="http://rules.emergingthreats.net/blockrules/compromised-ips.txt">http://rules.emergingthreats.net/blockrules/compromised-ips.txt</a>	43200	Disabled   <a href="#">Enable</a>	<a href="#">Clone</a>
<a href="#">emerging_threats_ip_blocklist</a>	malicious	Emerging Threats fwip rules	<a href="http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt">http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt</a>	43200	Disabled   <a href="#">Enable</a>	<a href="#">Clone</a>
<a href="#">emerging_threats_malvertisers_blocklist</a>	malicious	Emerging Threats Malvertisers blocklist	<a href="http://rules.emergingthreats.net/blockrules/rbn-malvertisers-ips.txt">http://rules.emergingthreats.net/blockrules/rbn-malvertisers-ips.txt</a>	43200	Disabled   <a href="#">Enable</a>	<a href="#">Clone</a>
<a href="#">iblocklist_logmein</a>	networks	Addresses that are used by the LogMeIn product to enable unauthorized remote access	<a href="http://list.iblocklist.com/?list=logmein">http://list.iblocklist.com/?list=logmein</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">iblocklist_piratebay</a>	networks	Addresses that are commonly associated with known PirateBay sites	<a href="http://list.iblocklist.com/?list=nzldzlpkgrcndomnttb">http://list.iblocklist.com/?list=nzldzlpkgrcndomnttb</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">iblocklist_proxy</a>	proxy	Addresses that are commonly associated with known traffic-proxy sites	<a href="http://list.iblocklist.com/?list=bt_proxy">http://list.iblocklist.com/?list=bt_proxy</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">iblocklist_rapidshare</a>	networks	Addresses that are commonly associated with known RapidShare sites	<a href="http://list.iblocklist.com/?list=zfcuwtkjfwkalytktyiw">http://list.iblocklist.com/?list=zfcuwtkjfwkalytktyiw</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">iblocklist_spyware</a>	spyware	Addresses that are commonly associated with known spyware sites	<a href="http://list.iblocklist.com/?list=bt_spyware">http://list.iblocklist.com/?list=bt_spyware</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">iblocklist_tor</a>	networks	Addresses that are commonly associated with known Tor sites	<a href="http://list.iblocklist.com/?list=tor">http://list.iblocklist.com/?list=tor</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">iblocklist_web_attacker</a>	malicious	Addresses that are commonly associated with known malicious attacker sites	<a href="http://list.iblocklist.com/?list=ghlzqtqxnzctvjvjjwag">http://list.iblocklist.com/?list=ghlzqtqxnzctvjvjjwag</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">local_threatlist</a>	malicious	Custom list of threat IP addresses	<a href="#">lookup://local_threatlist</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">norse_darklist</a>	malware	Norse Darklist full download	<a href="http://labs.ipviking.com/slice/">http://labs.ipviking.com/slice/</a>	43200	Disabled   <a href="#">Enable</a>	<a href="#">Clone</a>
<a href="#">palevo_ip_blocklist</a>	malicious	abuse.ch Palevo C&C IP Blocklist	<a href="https://palevotracker.abuse.ch/blocklists.php?download=ipblocklist">https://palevotracker.abuse.ch/blocklists.php?download=ipblocklist</a>	43200	Disabled   <a href="#">Enable</a>	<a href="#">Clone</a>
<a href="#">sans</a>	malicious	SANS blocklist	<a href="http://isc.sans.edu/block.txt">http://isc.sans.edu/block.txt</a>	43200	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>
<a href="#">spyeye_ip_blocklist</a>	malicious	abuse.ch SpyEye IP blocklist	<a href="https://spyeyetracker.abuse.ch/blocklist.php?download=ipblocklist">https://spyeyetracker.abuse.ch/blocklist.php?download=ipblocklist</a>	43200	Disabled   <a href="#">Enable</a>	<a href="#">Clone</a>
<a href="#">zeus_bad_ip_blocklist</a>	malicious	abuse.ch Zeus blocklist (bad IPs only)	<a href="https://zeustracker.abuse.ch/blocklist.php?download=badips">https://zeustracker.abuse.ch/blocklist.php?download=badips</a>	43200	Disabled   <a href="#">Enable</a>	<a href="#">Clone</a>
<a href="#">zeus_standard_ip_blocklist</a>	malicious	abuse.ch Zeus blocklist (standard)	<a href="https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist">https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist</a>	43200	Disabled   <a href="#">Enable</a>	<a href="#">Clone</a>

# 威胁情报活跃度

splunk App: Enterprise Security
John Stoner Messages Settings Activity Help

Security Posture Incident Review Event Investigations Advanced Threat Security Domains Audit Search Configure
Enterprise Security

### Threat Activity

Threat Group: All

Threat Category: All

Search: Threat Match Value

Last 24 hours

**Submit**

Advanced Filter

**THREAT MATCHES**  
Unique Count

**109** ↑8

**THREAT COLLECTIONS**  
Unique Count

**5** 0

**THREAT CATEGORIES**  
Unique Count

**4** 0

**THREAT SOURCES**  
Unique Count

**7** ↓1

**THREAT ACTIVITY**  
Total Count

**139** ↑7

#### Threat Activity Over Time

4m ago

#### Most Active Threat Collections

threat_collection	search	sparkline	dc(certifact)	count
ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		40	95
file_intel	File Hash Matches File Name Matches		22	37
certificate_intel	Certificate Common Name Matches Certificate Organization Matches Certificate Serial Matches Certificate Unit Matches Email Address Matches		4	5
process_intel	Process Matches		1	1
service_intel	Service Matches		1	1

4m ago

#### Most Active Threat Sources

source_id	source_path	source_type	count
emerging_threats_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv	csv	44
blocklist_logname	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/blocklist_logname.csv	csv	43
mandiant.package-1905936-1861-4cfe-b213-c016fce1e249	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_D_IDCs_No_OpenOC.xml	xml	35
mandiant.package-1905936-1861-4cfe-b213-c016fce1e249	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_F_IDCs_Certificates.xml	xml	3
malware_domains	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/malware_domains.csv	csv	4
freegc.stx-67015e67-4292-4463-b654-60c1a491723c	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/freegc-stx-report-with-indicators.xml	xml	2
mandiant.package-1905936-1861-4cfe-b213-c016fce1e242	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_D_F2DNg.xml	xml	2

4m ago

#### Threat Activity Details

time	threat_match_field	threat_match_value	filter	sourcetype	src	dest	threat_collection	threat_group	threat_category
2015-7-28 13:35:00	file_name	setup.exe		WinEventLog:Application:trendmicro	unknown	L-mcay02	file_intel	undefined	undefined
2015-7-28 13:35:00	file_name	svchost.exe		WinEventLog:Application:trendmicro	unknown	DWHEIP0C	file_intel	undefined	undefined
2015-7-28 13:30:00	ssl_subject_common_name	0J8J		stream:tcp	unknown	unknown	certificate_intel	undefined	undefined
2015-7-28 13:30:00	file_hash	06cd52566bf25b610c1fe120195f		file_notification	unknown	sv-03-sa-demo.splunk.com	file_intel	undefined	undefined
2015-7-28 13:30:00	ssl_hash	a72170770245c90bd23a0a0845314173a		stream:tcp	unknown	unknown	file_intel	undefined	undefined

139.60.4... [07/Jan 18 10:57:153] "GET /category screen?category\_id=G1F15&SESSIONID=5D5SLAF10ADEF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-05&product\_id=128...&itemId=EST-16&product\_id=RP-LI-02" 468 125 17 10...

splunk listen to your data

# 支持STIX/TAXII、OpenIOCs

Enterprise Security

## Threat Artifacts

Threat Artifact Threat Category Threat Group Malware Alias Intel Source ID Intel Source Path

Threat ID All All Submit

Threat Overview Network Endpoint Certificate Email

### Threat Overview

source_id	source_path	source_type	threat_group	threat_category	malware_alias	count
fireeye.stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/Users/bluger/Desktop/blog_post/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F (and 6 more)	APT (and 2 more)		503

### Endpoint Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
file_intel	stix	F	APT		194
file_intel	stix	admin338	APT		194
file_intel	stix	japanorus	APT		194
file_intel	stix	menupass	APT		194
file_intel	stix	nitro	APT		194
file_intel	stix	th3bug	APT		194
file_intel	stix	wl	APT		194

### Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category	malware_alias
ip_intel	stix	52	49	0	0	101	F	APT	
ip_intel	stix	52	49	0	0	101	admin338	APT	
ip_intel	stix	52	49	0	0	101	japanorus	APT	
ip_intel	stix	52	49	0	0	101	menupass	APT	
ip_intel	stix	52	49	0	0	101	nitro	APT	
ip_intel	stix	52	49	0	0	101	th3bug	APT	
ip_intel	stix	52	49	0	0	101	wl	APT	

### Email Artifacts

### Certificate Artifacts



## 与国内威胁情报源集成

client_ip	count	hit.detected	hit.expired	hit.info	intelligences.confidence	intelligences.find_time	intelligences.intel_types	intelligences.source	ip.carrier	ip.ip	ip.location	
104	110	7752	true	false	idc compromised spam	90 2016-07-08 23:18:13 70 2016-05-17 20:17:47 85 2016-04-19 08:00:53 75 2016-04-19 07:04:04 75 2016-04-16 14:53:53 75 2016-02-19 12:16:51	IDC服务器 IDC服务器 垃圾邮件 垃圾邮件 垃圾邮件 垃圾邮件	ThreatBook Labs ThreatBook Labs ThreatBook Labs ThreatBook Labs ThreatBook Labs ThreatBook Labs		10	10	洛杉矶
49	8	7752	false	false	dynamic_ip	80 2016-05-17 12:06:53	动态IP	ThreatBook Labs	电信	40	98	南通
104	241	7726	true	false	idc compromised spam	90 2016-07-08 23:18:13 70 2016-05-17 20:16:19 75 2016-02-19 12:16:51	IDC服务器 IDC服务器 垃圾邮件	ThreatBook Labs ThreatBook Labs ThreatBook Labs		10	241	洛杉矶
47	5	6694	true	false	idc	90 2016-05-11 17:21:01 90 2016-05-11 17:21:01	IDC服务器 IDC服务器	ThreatBook Labs ThreatBook Labs	阿里云/电信/ 联通/移动/铁 通/教育网	40	15	深圳
198	24	6299	true	false	idc compromised spam	90 2016-07-08 23:18:06 75 2016-06-21 10:26:41 70 2016-05-17 20:15:45 75 2016-02-19 12:16:51	IDC服务器 扫描 IDC服务器 垃圾邮件	ThreatBook Labs 开源情报 ThreatBook Labs ThreatBook Labs		19	324	洛杉矶
198	8	5352	true	false	idc compromised spam	90 2016-07-08 23:18:06 75 2016-06-21 10:26:41 70 2016-05-17 20:15:45 75 2016-02-19 12:16:51	IDC服务器 扫描 IDC服务器 垃圾邮件	ThreatBook Labs 开源情报 ThreatBook Labs ThreatBook Labs		19	58	洛杉矶
63	226	4092	true	false	zombie idc compromised spam	85 2017-03-02 09:00:49 65 2017-03-01 16:53:36 80 2017-03-01 02:17:57 25 2017-02-27 20:34:17 55 2017-02-24 03:38:16 85 2017-02-16 04:53:53	垃圾邮件 可疑 恶意软件 漏洞利用 恶意软件 漏洞利用	ThreatBook Labs 开源情报 开源情报 开源情报 开源情报 ThreatBook Labs	datashack.net	6	26	堪萨斯城

# 与国内威胁情报源集成

The screenshot displays the Splunk ThreatBook interface for the IP address 182.248.28.25. On the left, a sidebar shows a list of threat events with a table of details. The main content area is divided into several sections:

- 基础数据信息 (Basic Data Information):**
  - 地理位置: 日本, 日本
  - ASN: 2516 ( KDDI KDDI CORPORATION, JP )
  - Tags: (empty)
- 可视分析 (Visual Analysis):** A map showing the location of 182.248.28.25 in Japan.
- 基础数据信息 (Basic Data Information) Legend:**
  - 域名 (Domain)
  - 样本HASH (Sample Hash)
  - IP (IP)
  - whois注册邮箱 (Whois Registration Email)
  - whois注册名 (Whois Registration Name)
- 威胁情报数据 (Threat Intelligence Data) Legend:**
  - 域名 (Domain)
  - 样本HASH (Sample Hash)
  - URL (URL)
  - IP (IP)
  - 其它 (Other)
- 提示 (Tips):**
  - 分类数据最大显示结点数: 50
  - 点击图标, 查看详细内容并访问链接

The left sidebar table shows the following details for the event:

时间	安全域
17/08/01 12:53:58.000	Endpoint

**Additional Fields:**

Field	Value
CVE	CVE-2008-5416
Destination	182.248.28.25
Destination Business Unit	未知管理单元
Destination IP Address	182.248.28.25
Destination Expected	true
Destination Host-Header	995-HQ-ADMIN01
Destination PCI Domain	UNKNOWN
Destination Requires Antivirus	true (UNKNOWN)
Destination Should Time Synchronize	false
Destination Should Update	true (UNKNOWN)
Filename	gfl18570k1303x003Cmsv18... JLJ0N42m866313w8L8&T253kmOQ

# 与国内威胁情报源集成

IP	来源/描述	状态	次数	备注
2017-06-27 17:55:13	次要告警	已关闭	211	193[中国四川电信(IDC服务器)]正在对... 并行漏洞扫描 总计207次 (200响应0次 404响应207次 500响应0次 其它响应0次)
120.7	164[中国广东湛江移动]正在对			发送验证码页面进行异常访问13次
120.2	164[中国广东湛江移动]正在对			发送验证码页面进行异常访问12次
120.2	164[中国广东湛江移动]正在对			发送验证码页面进行异常访问39次
120.2	164[中国广东湛江移动]正在对			发送验证码页面进行异常访问13次
112.25	182[中国山东临沂联通(垃圾邮件、僵尸网络、动态IP)]正在对			发送验证码页面进行异常访问11次
117.62	8[中国江苏苏州电信(垃圾邮件、僵尸网络、动态IP)]正在对			发送验证码页面进行异常访问11次
112.23	182[中国山东临沂联通(垃圾邮件、僵尸网络、动态IP)]正在对			发送验证码页面进行异常访问23次
114.24	215[中国北京北京联通]正在对			发送验证码页面进行异常访问21次
115.15	46[中国江西上饶电信(动态IP)]正在对			发送验证码页面进行异常访问14次
117.62	3[中国江苏苏州电信(垃圾邮件、僵尸网络、动态IP)]正在对			发送验证码页面进行异常访问18次
117.90	30[中国江苏镇江电信(僵尸网络、垃圾邮件、动态IP)]正在对			发送验证码页面进行异常访问13次

IP	来源/描述	次数	备注
113.	40[中国广东茂名电信(垃圾邮件、IDC服务器)]扫描:	207次, 已被阻断。(30分钟后解封, 仅保持持续关注)	
188	29[法国北部- 加来海峡大区鲁贝ovh.com(僵尸网络、垃圾邮件、扫描、IDC服务器)]扫描:	207次, 已被阻断。(30分钟后解封, 仅保持持续关注)	
47	15[中国广东深圳阿里云/电信/联通/移动/铁通/教育网(IDC服务器)]扫描:	344次, 已被阻断。(30分钟后解封, 仅保持持续关注)	

# 总结：Splunk帮助您将威胁情报使用落地

- ▶ 从广泛的数据源自动化收集、整合威胁情报数据并进行去重处理
- ▶ 支持STIX/TAXII、OpenIOC等标准
- ▶ 快速上手开箱即用的威胁情报管理器和仪表盘
- ▶ 通过威胁情报来丰富数据、提供上下文情境，从而为威胁分析、快速响应提供帮助

# 利用情报+分析打造智能驱动的ISOC



事件调查&取证



安全&合规报表



实时监控已知威胁



检测未知威胁



欺诈检测



内部威胁

ThreatBook

splunk >

谢谢！

