打造由情报分析驱动的ISOC

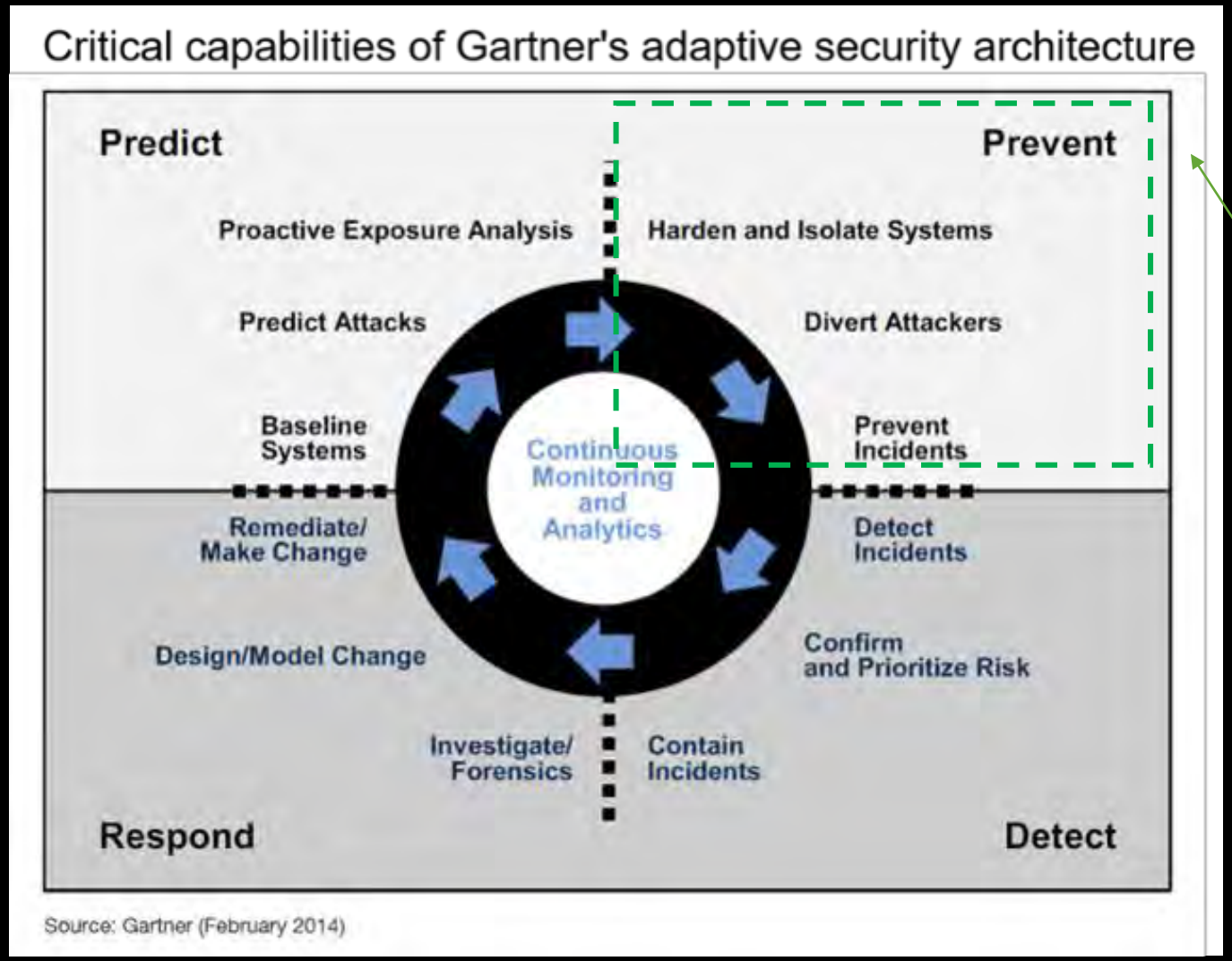
郑聿铭

Splunk中国区高级架构师

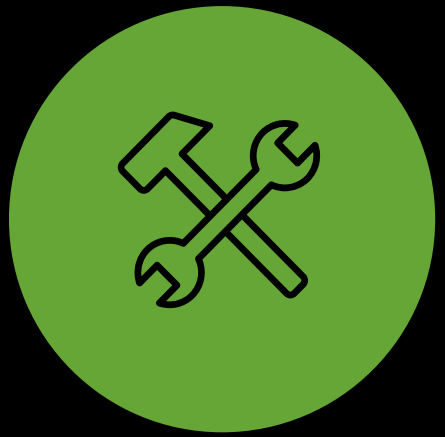
何谓ISOC

- 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

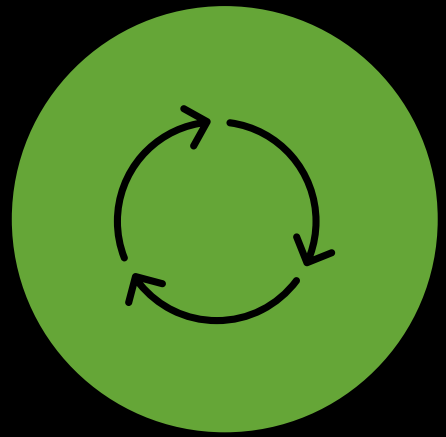


安全仍然处于被动防御的形式



工具

仅仅是“告警”
而不是“洞察”



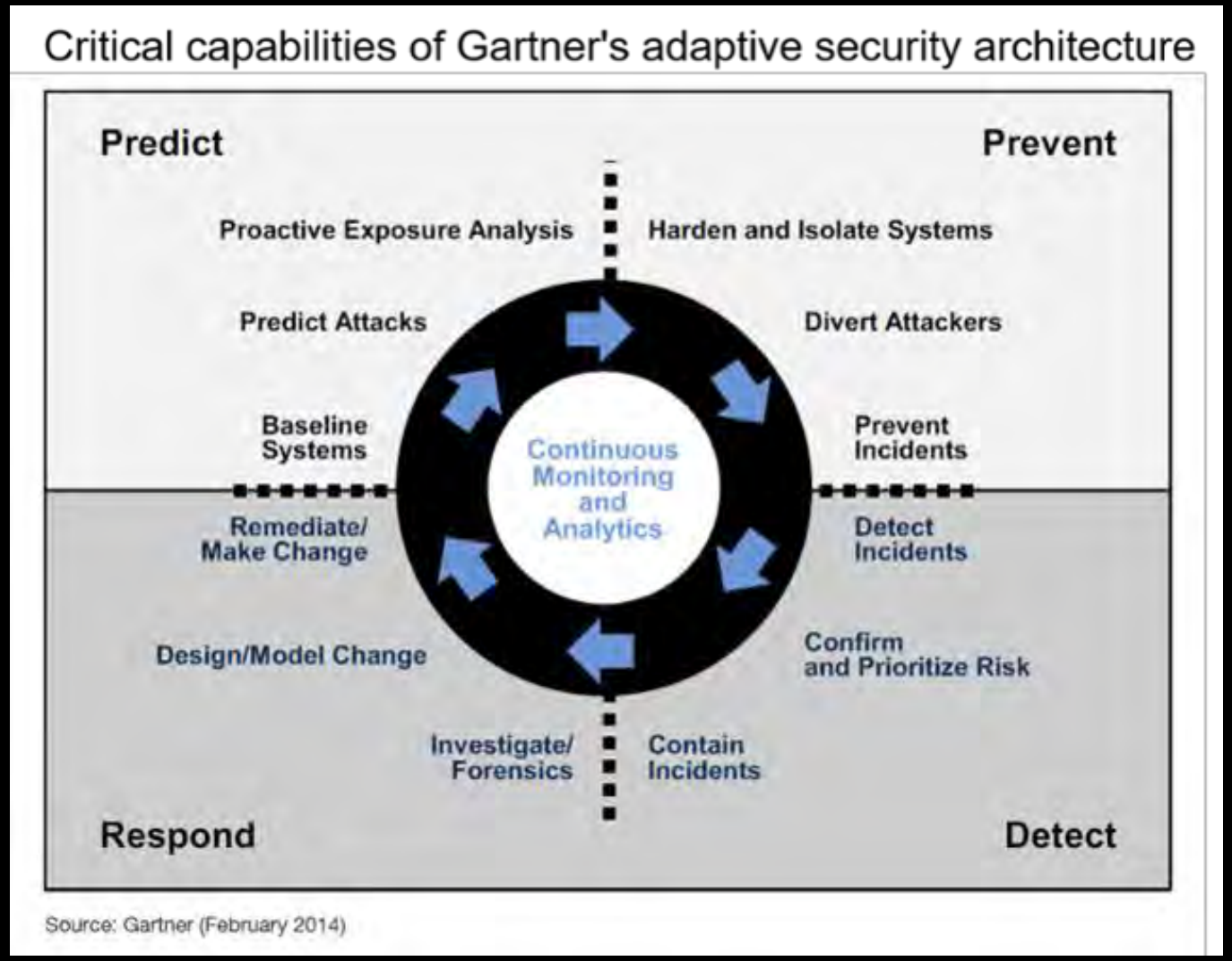
流程

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)



splunk> listen to your data

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）

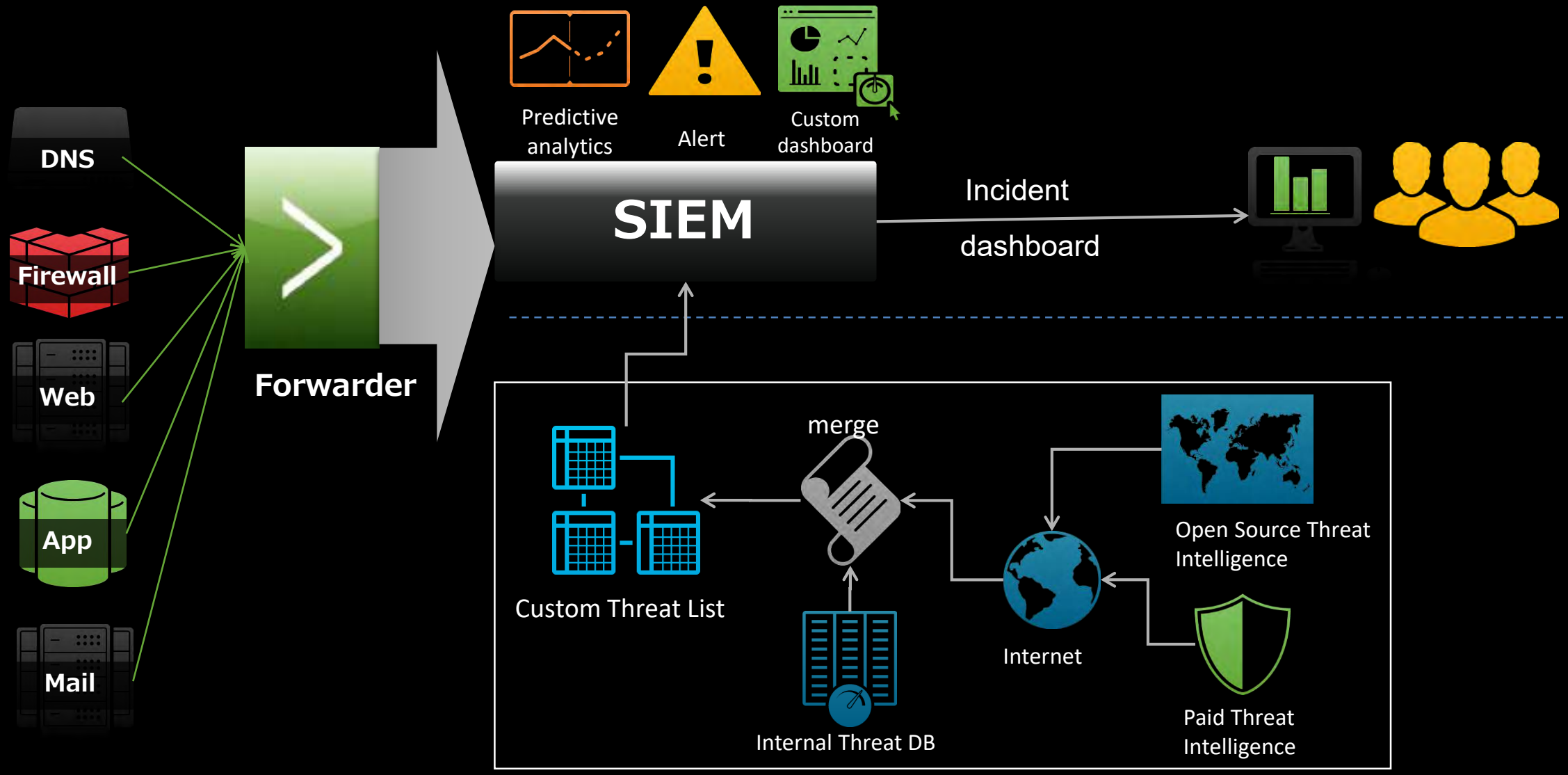
Hypothesis

IOC

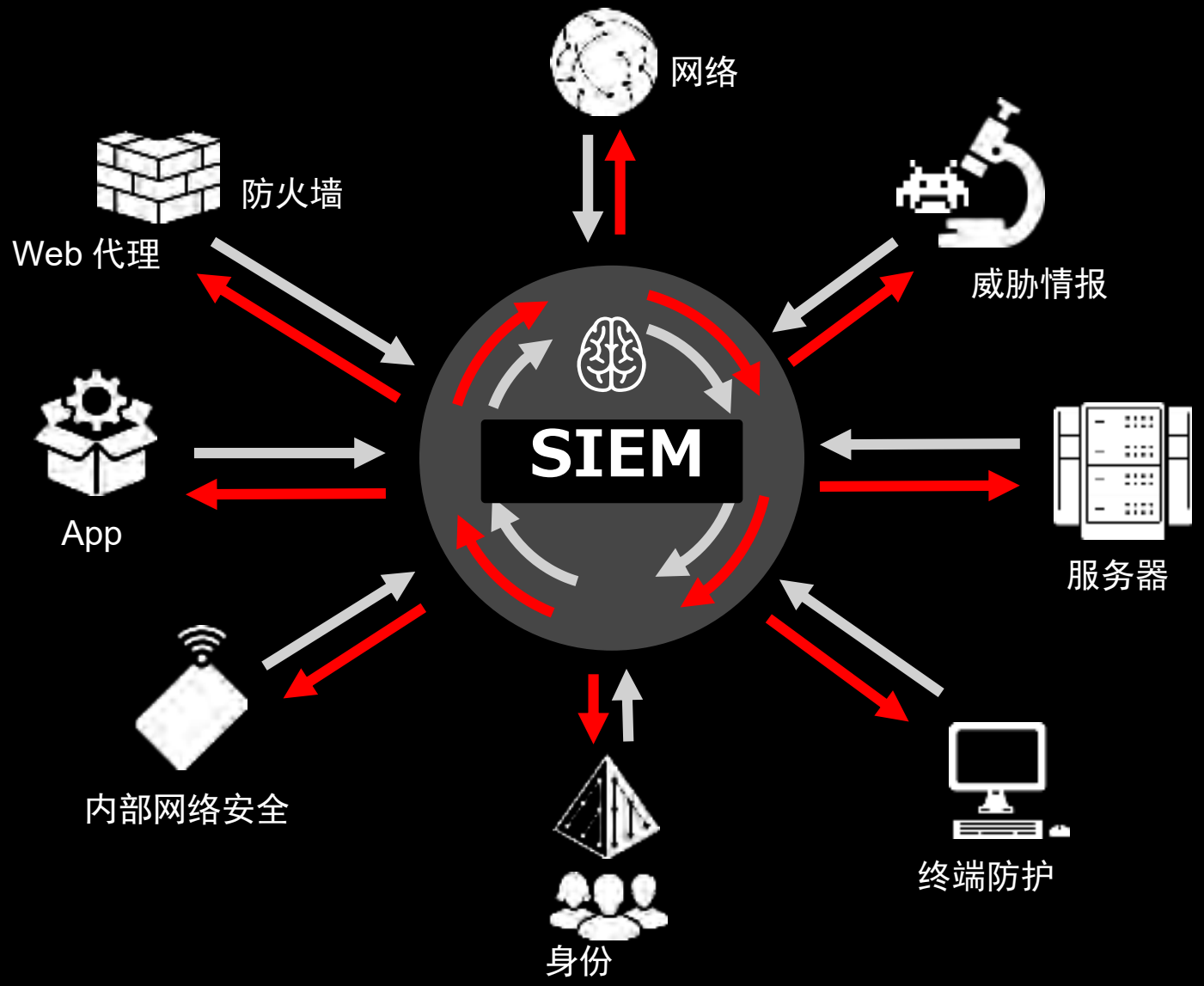
Analytics

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



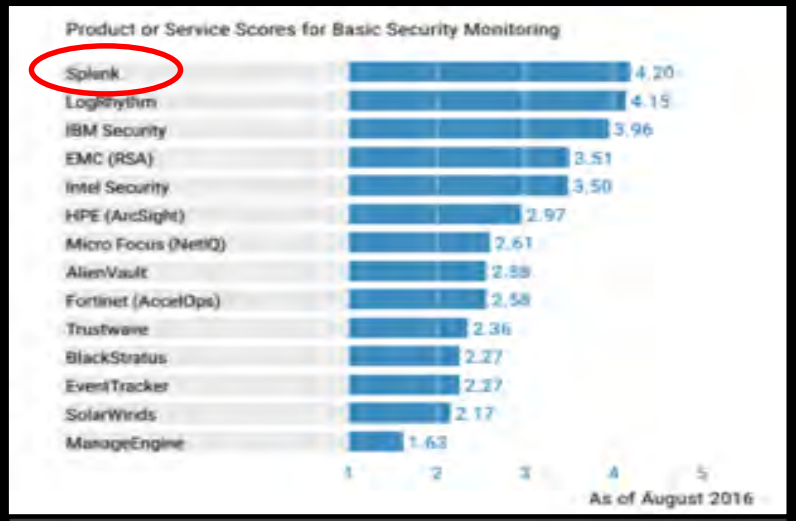
Gartner SIEM 魔力象限领导者

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）

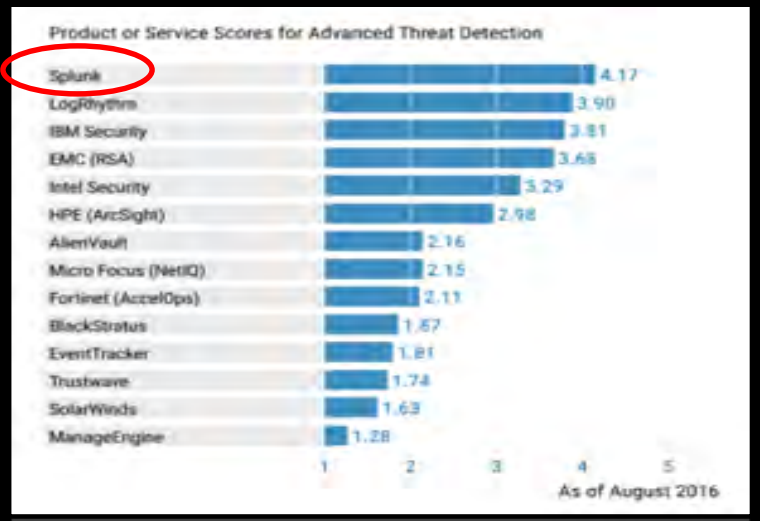
Splunk从2011年起进入Gartner SIEM领域，并迅速发展，2013年进入SIEM领导者象限，并连续四年不断取得进步，2016年技术前瞻性维度排名第一。

Gartner2016年SIEM解决方案关键能力报告

基础安全监控



高级威胁检测

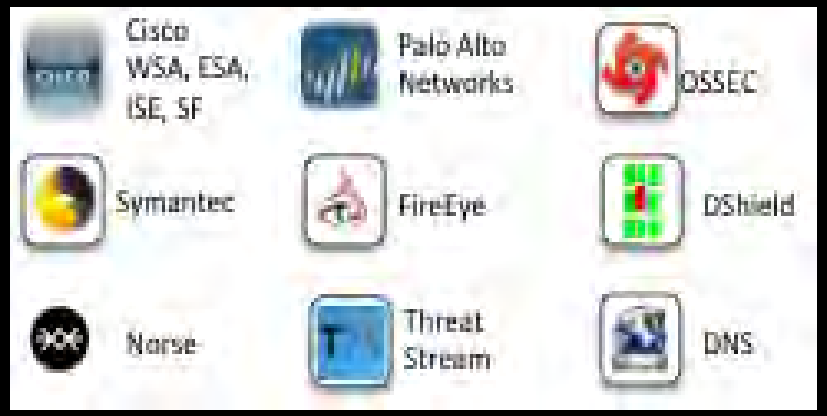


取证&事件响应

Splunk强大的安全智能平台

近500个
安全应用

安全厂商　　社群　　开源



SPLUNK FOR ENTERPRISE SECURITY

SPLUNK所打造的应用

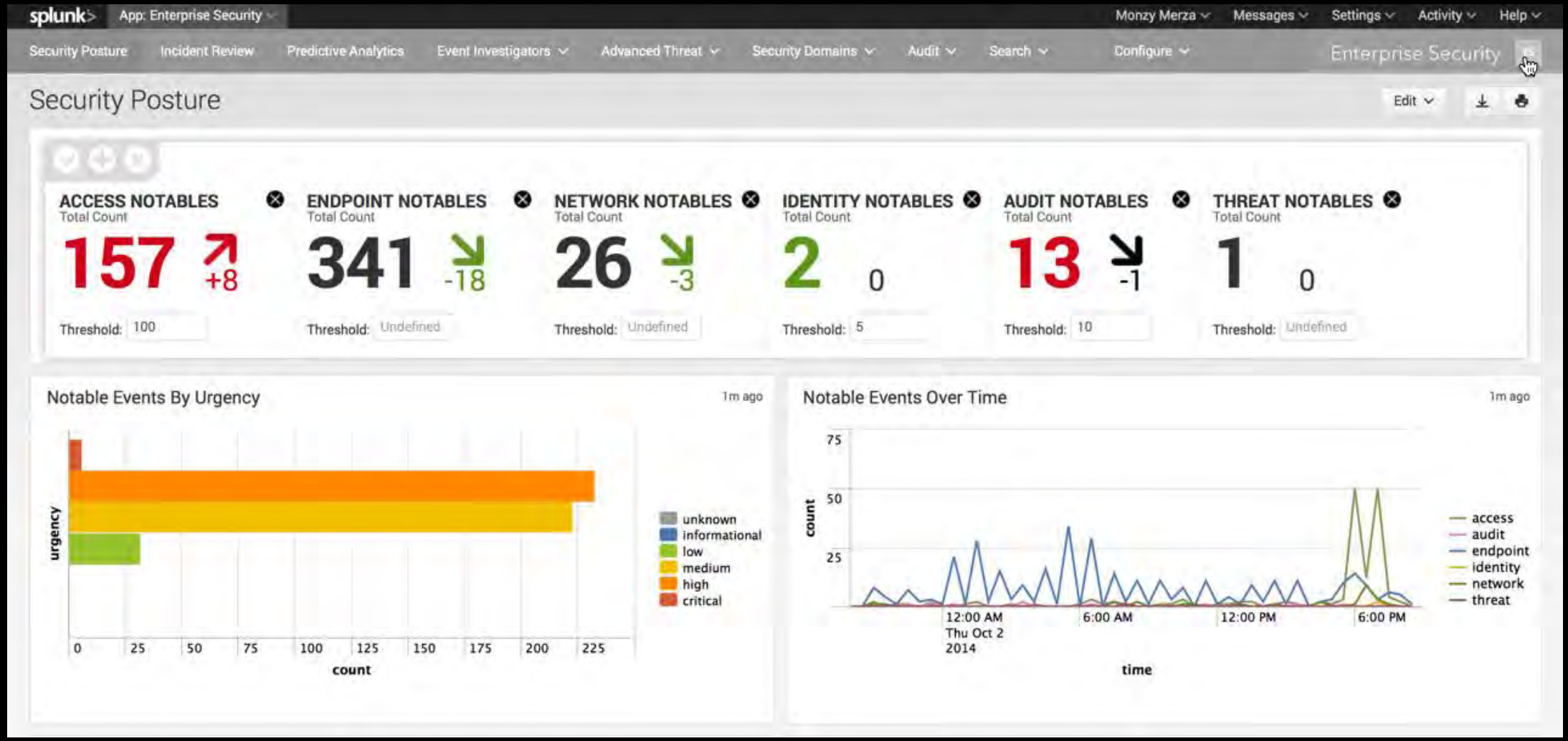
- STM — Wire (NFT) 数据
- INF — Windows (host/inf) 数据
- *nix — Unix与 Linux数据
- RDBMS (所有)数据
- EX — Exchange (email, inf)数据
- CEF — SIEM数据
- \> — 还有更多…

SPLUNK ENTERPRISE (核心)

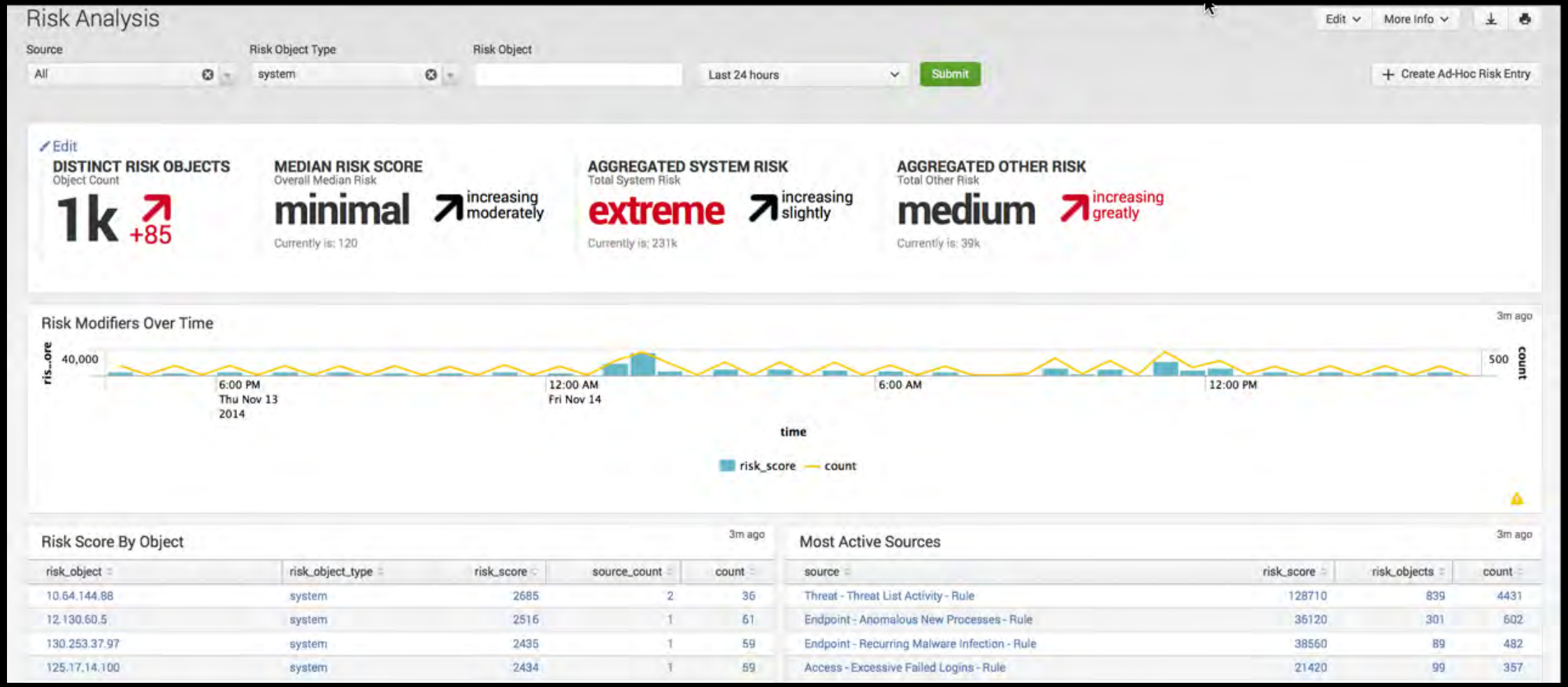
splunk>

splunk> listen to your data

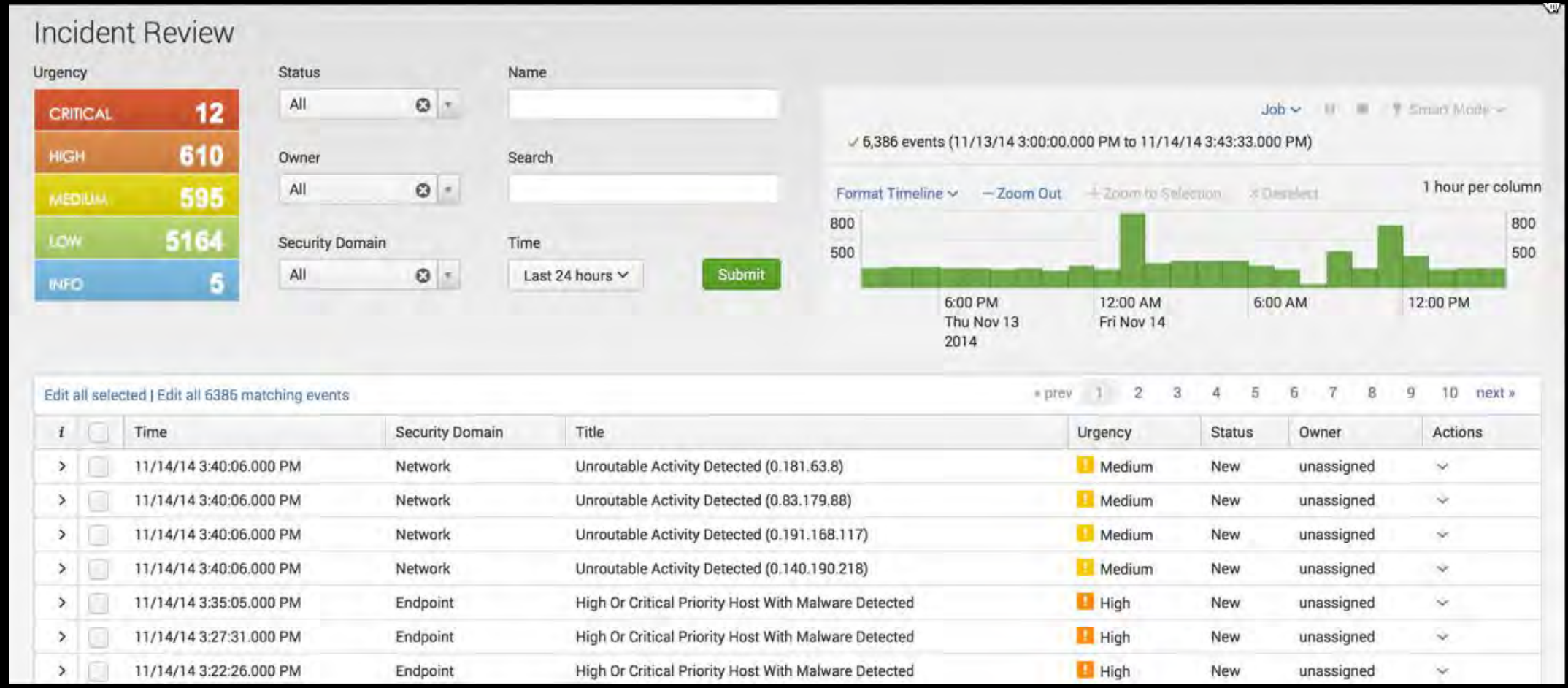
安全态势实时监控



基于风险的分析评估



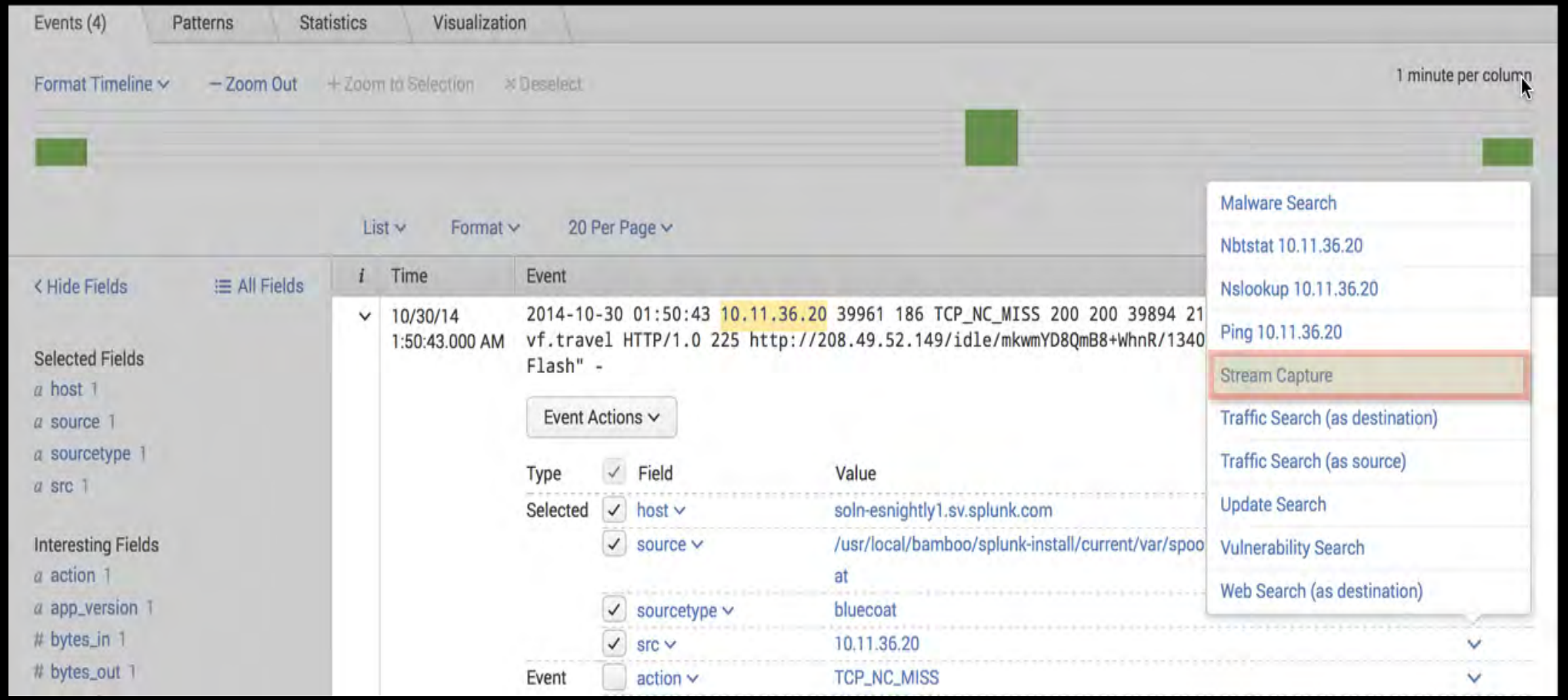
快速的事件审查及调查



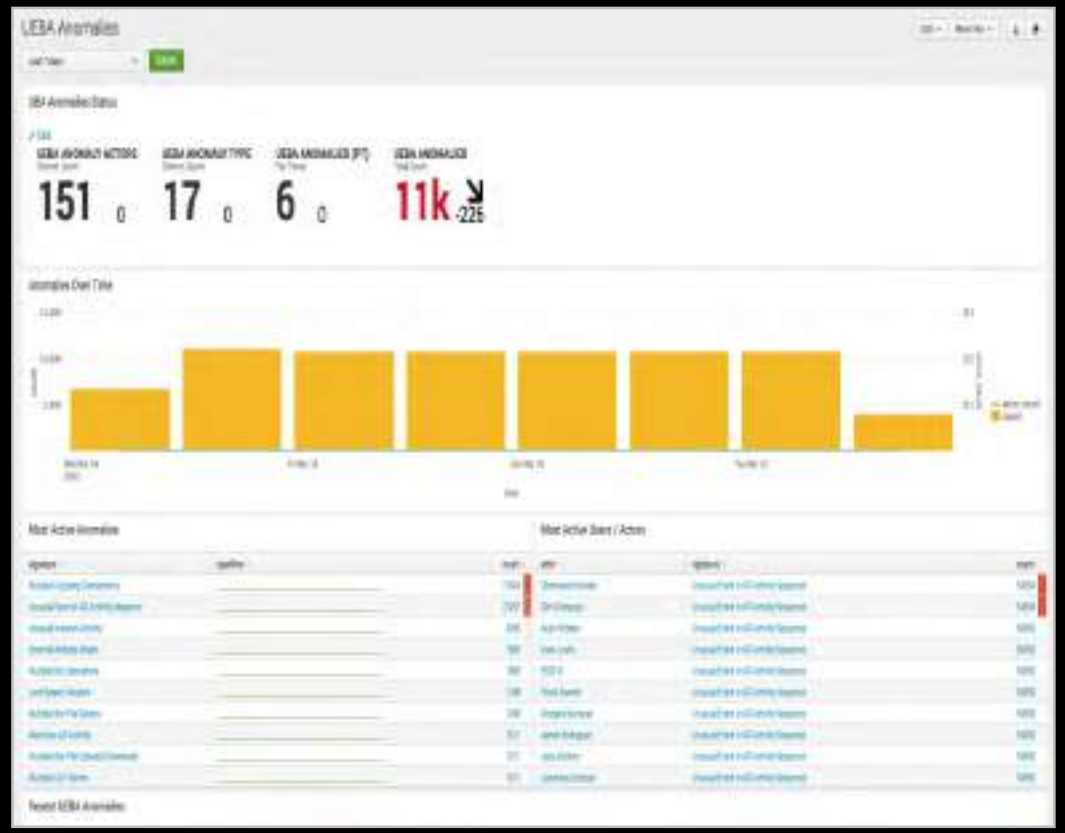
i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	11/14/14 3:40:06.000 PM	Network	Unroutable Activity Detected (0.181.63.8)	Medium	New	unassigned	
>	11/14/14 3:40:06.000 PM	Network	Unroutable Activity Detected (0.83.179.88)	Medium	New	unassigned	
>	11/14/14 3:40:06.000 PM	Network	Unroutable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

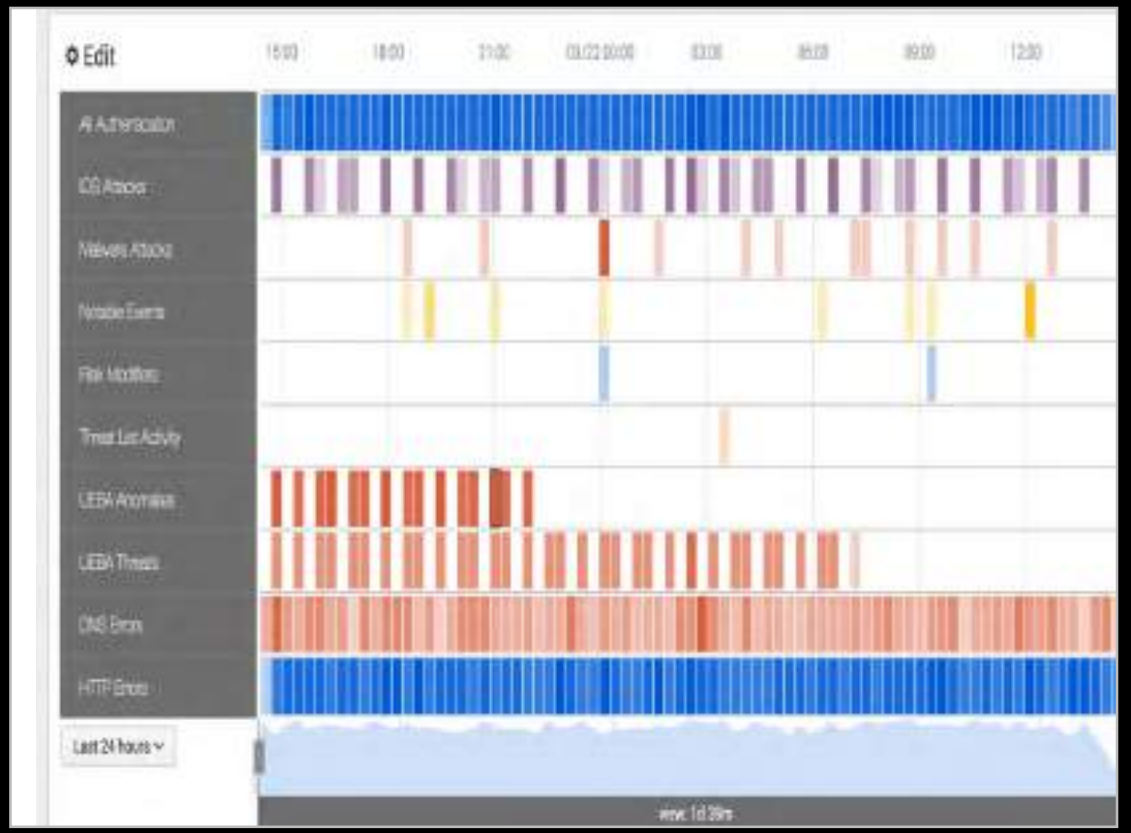
直观的可视化事件调查

快速灵活地响应操作

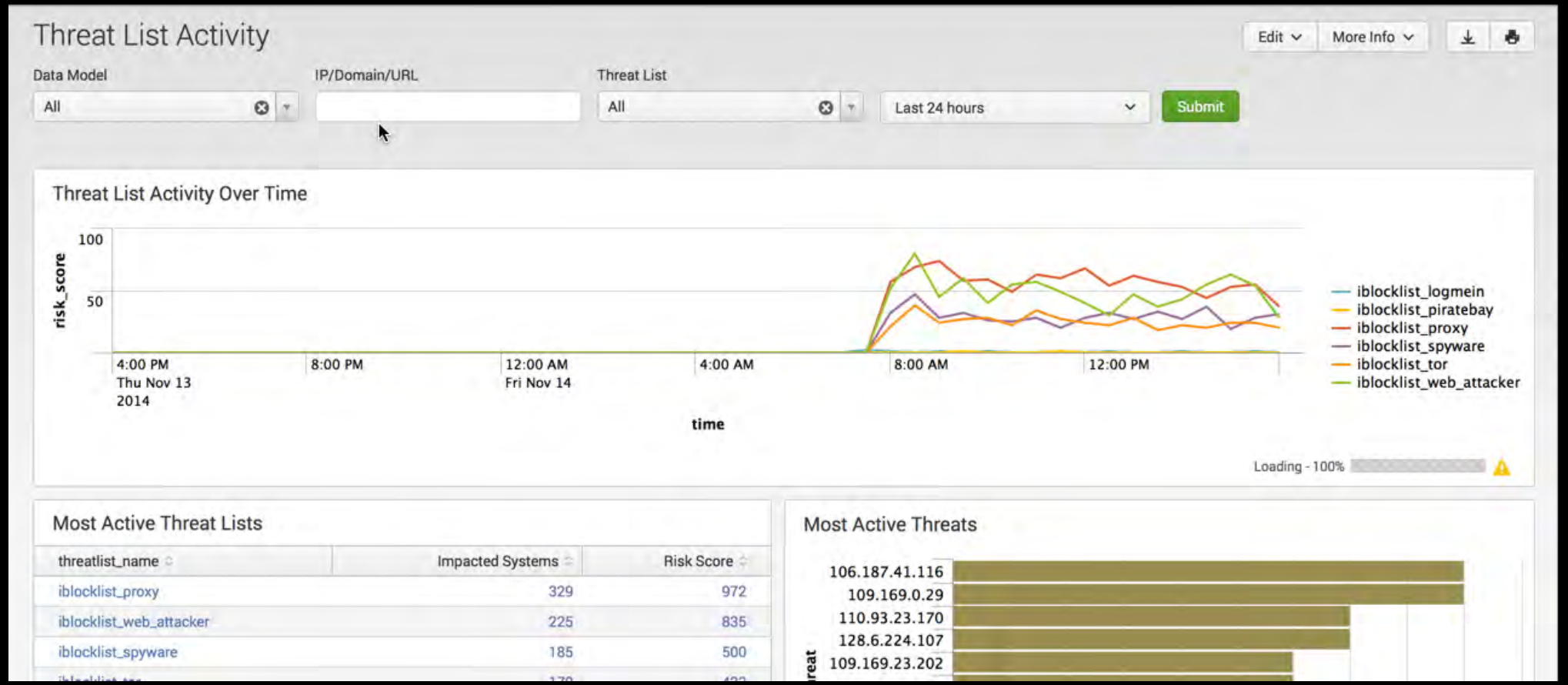


集成UEBA异常检测功能

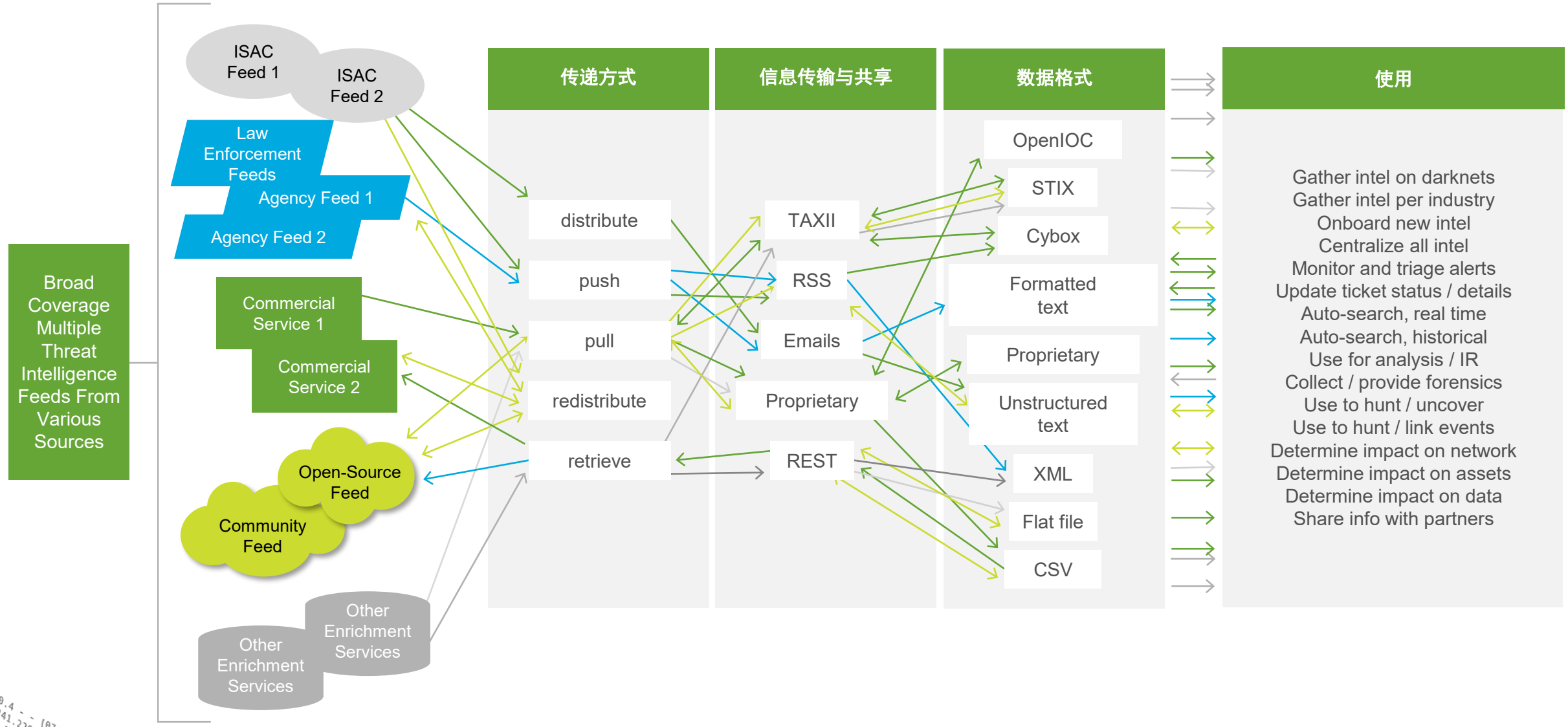




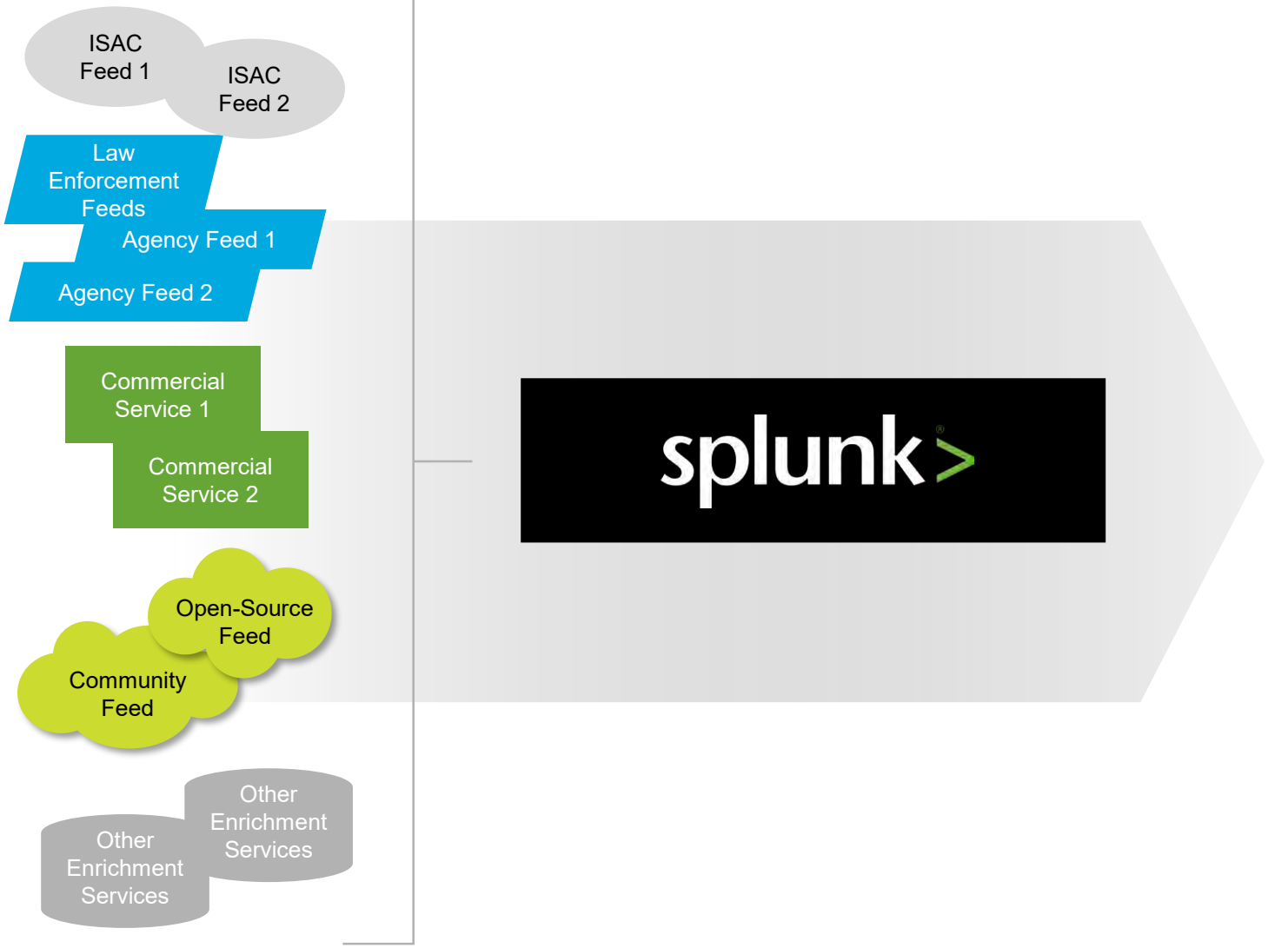
集成威胁情报的管理和使用



让威胁情报的管理和使用不再复杂



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

情报来源

- 多个来源
- 多种传输类型
- 多种传输手段
- 多种数据格式

收集管理

管理 / 审计
威胁情报源

- 列表状态
- 列表管理
- 列表位置

数据管理

分类

索引, 提取, 分类

1. IP
2. Emails
3. URLs
4. Files names/hashes
5. Processes names
6. Services
7. Registry entries
8. X509 Certificates
9. Users

关联

在现有日志数据中匹配所有的IOC

有任何的匹配都会产生告警

安全指标(KSI)和安全趋势

安全仪表板

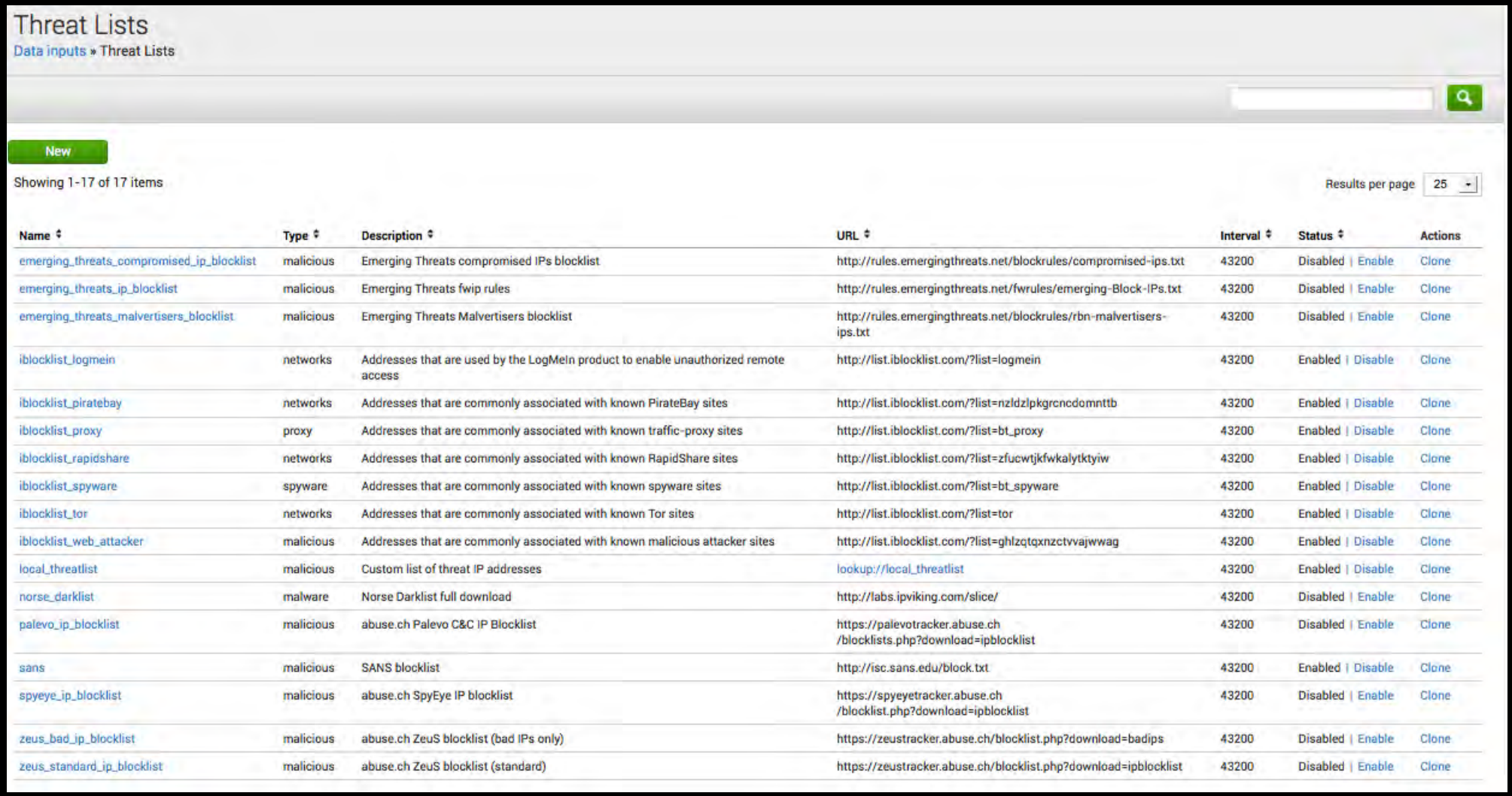
关联数据/ 关注事件

搜索

Ad-hoc 搜索, 分析, 调查, 优先级排序

数据搜索

多个威胁情报来源管理



Threat Lists

Data inputs » Threat Lists

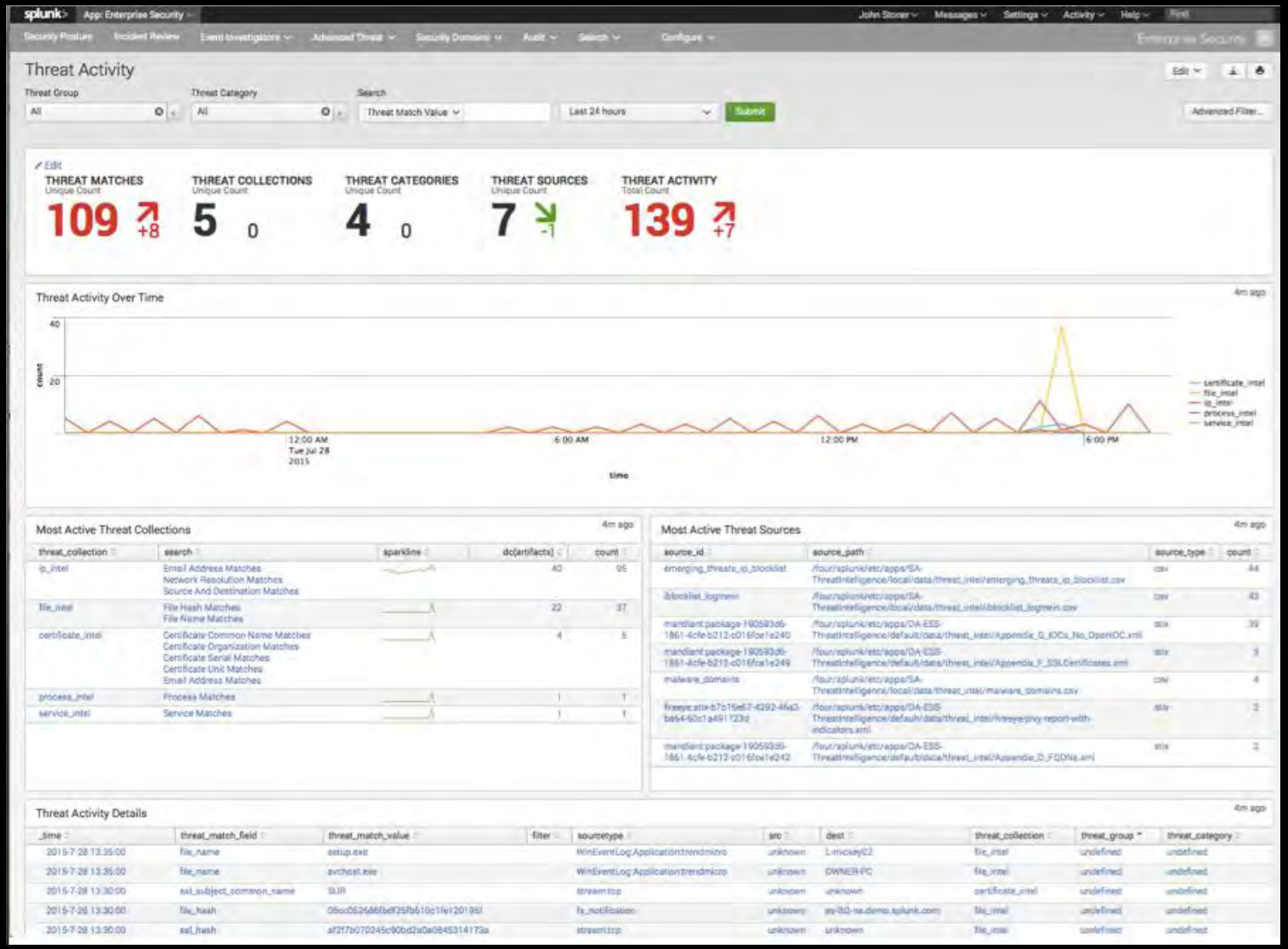
New

Showing 1-17 of 17 items

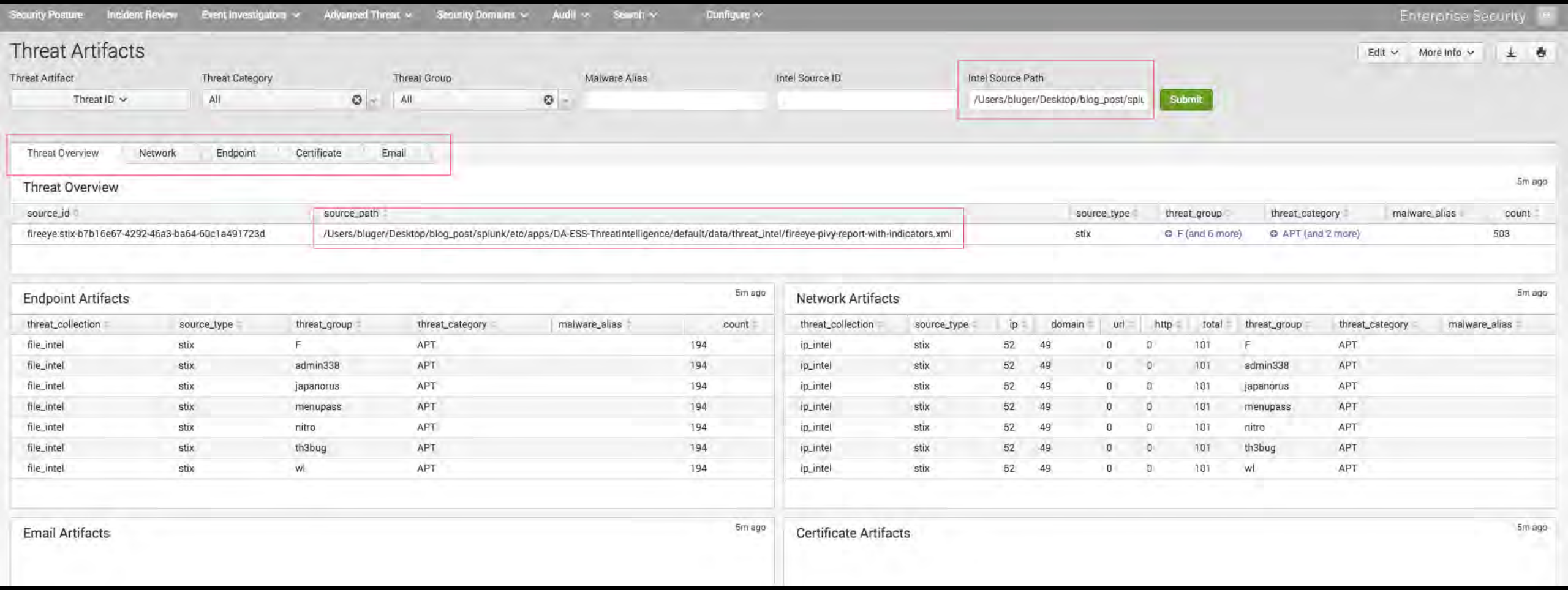
Results per page 25

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

威胁情报活跃度



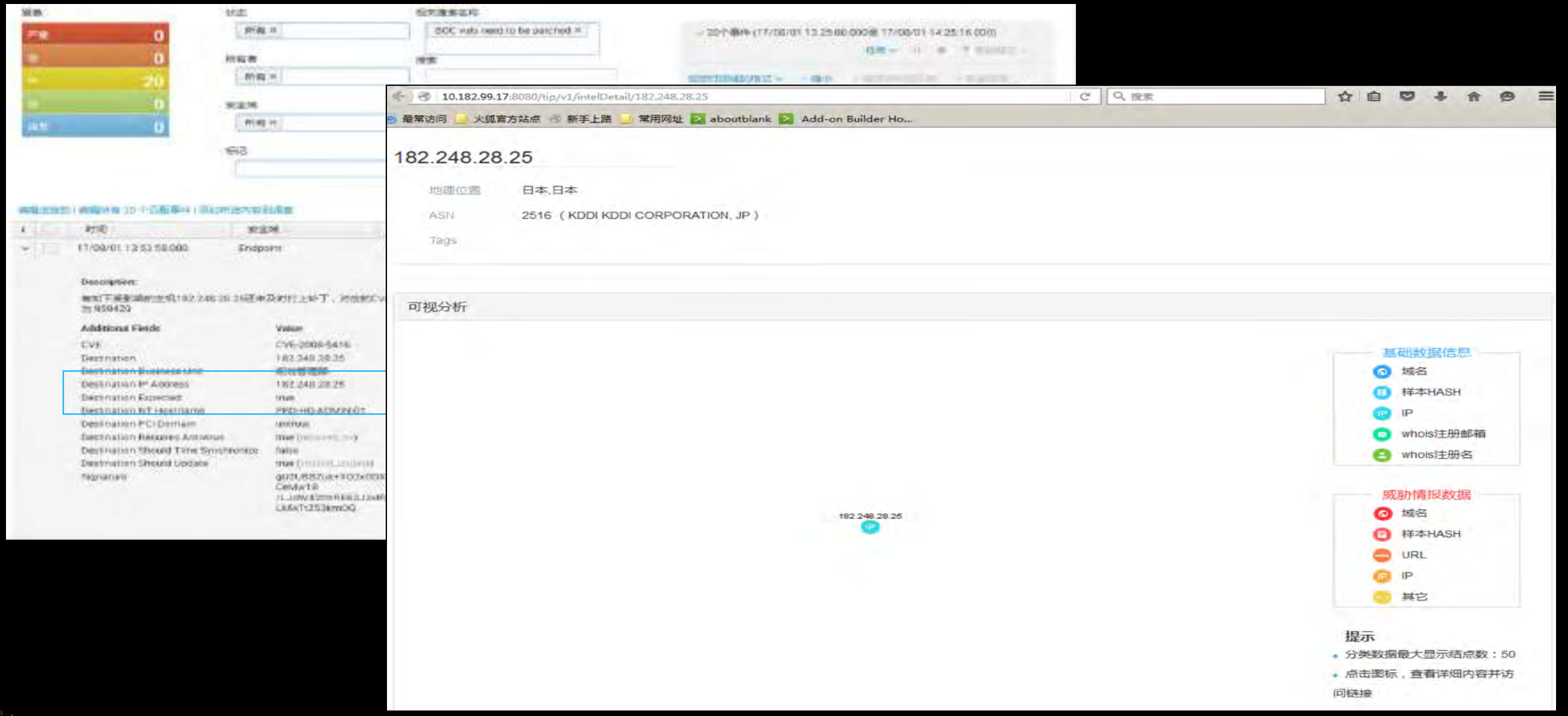
支持STIX/TAXII、OpenIOCs



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 70 85 75 75 75	2016-07-08 23:18:13 2016-05-17 20:17:47 2016-04-19 08:00:53 2016-04-19 07:04:04 2016-04-16 14:53:53 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 .0	洛杉矶
49 8	7752	false	false	dynamic_ip	80	2016-05-17 12:06:53	动态IP	ThreatBook Labs	电信	49 .8	南通
104 241	7726	true	false	idc compromised spam	90 70 75	2016-07-08 23:18:13 2016-05-17 20:16:19 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 90	2016-05-11 17:21:01 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	47 .15	深圳
198. 24	6299	true	false	idc compromised spam	90 75 70 75	2016-07-08 23:18:06 2016-06-21 10:26:41 2016-05-17 20:15:45 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 .3.24	洛杉矶
198. 8	5352	true	false	idc compromised spam	90 75 70 75	2016-07-08 23:18:06 2016-06-21 10:26:41 2016-05-17 20:15:45 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(.68	洛杉矶
63 226	4092	true	false	zombie idc compromised spam	85 65 80 25 55 85	2017-03-02 09:00:49 2017-03-01 16:53:36 2017-03-01 02:17:57 2017-02-27 20:34:17 2017-02-24 03:38:16 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



与国内威胁情报源集成

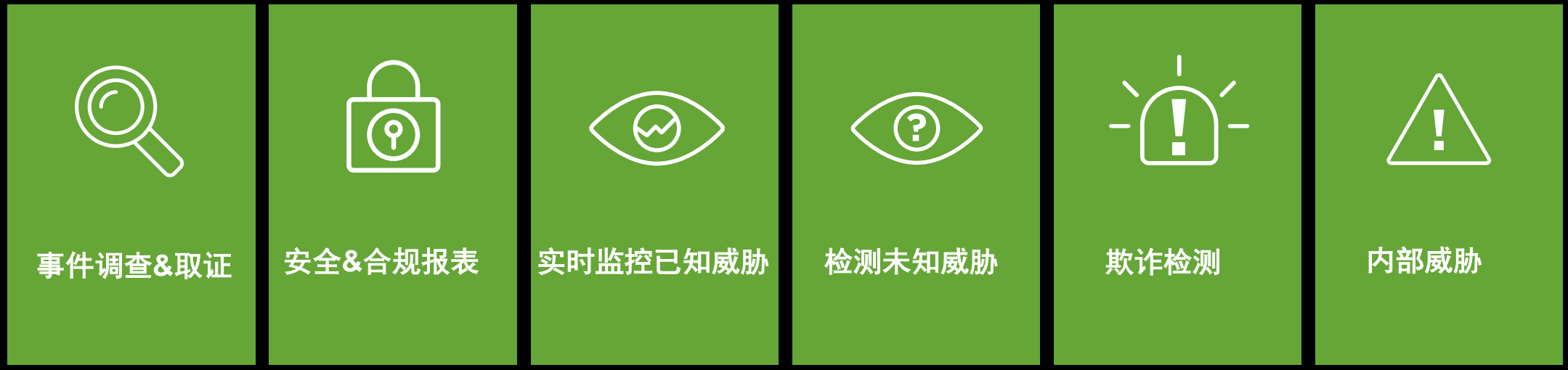
2017-06-27 17:55:13		次要告警	已关闭	211. 193[中国四川电信(IDC服务器)]正在对. 进行漏洞扫描 总计207次 (200响应0次 404响应207次 500响应0次 其它响应0次)
120.	164[中国广东湛江移动]正在对			发送验证码页面进行异常访问13次
120.2	164[中国广东湛江移动]正在对			发送验证码页面进行异常访问12次
120.2	164[中国广东湛江移动]正在对			送验证码页面进行异常访问39次
120.2	164[中国广东湛江移动]正在对			发送验证码页面进行异常访问13次
112.2	182[中国山东临沂联通(垃圾邮件、僵尸网络、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			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			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

alert
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 9[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 5[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板
- 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




谢谢！