ThreatBook

聚焦威胁 情报驱动

2018 网络安全分析与情报大会

ThreatBook

智能驱动的安全协调和自动相应

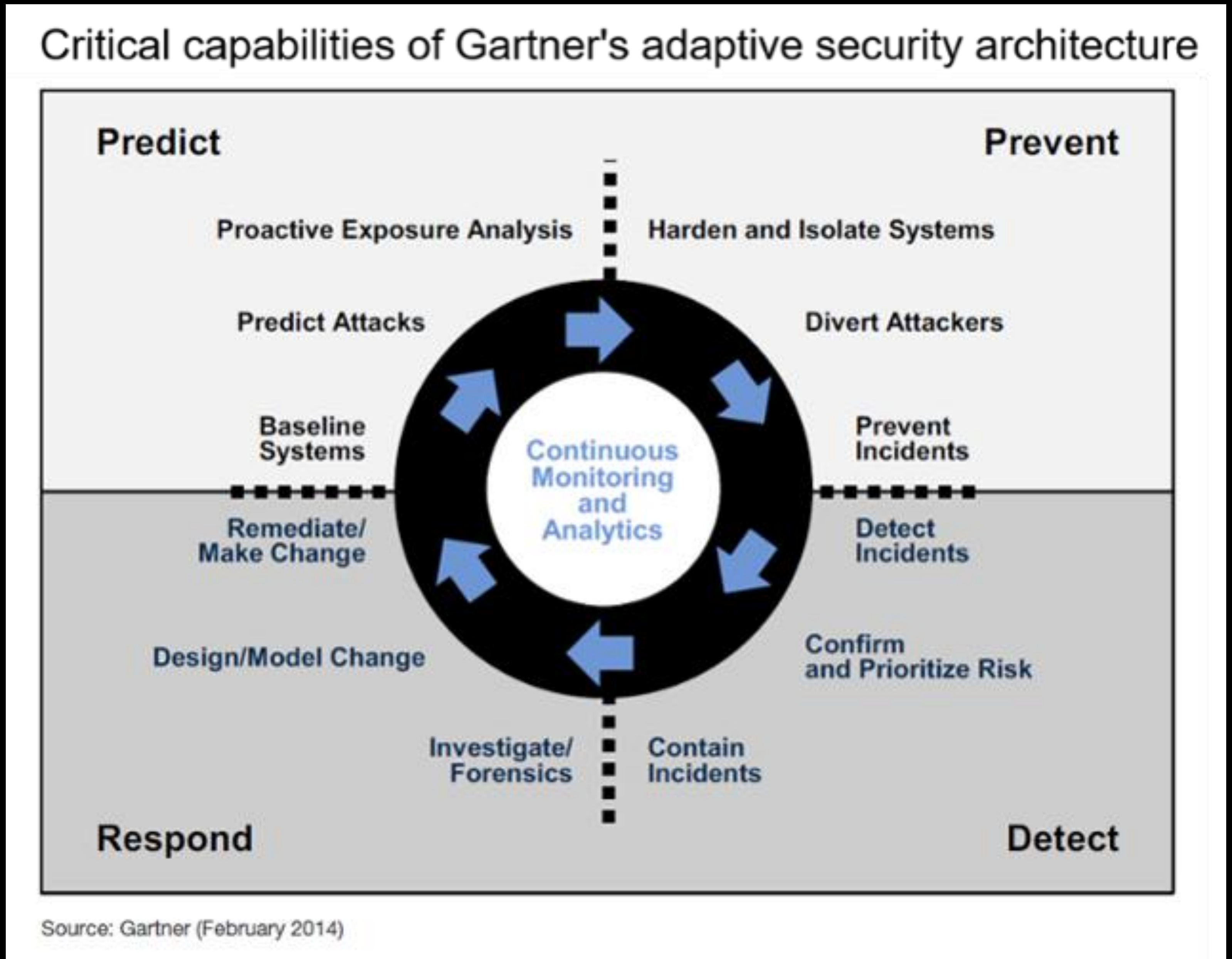
2018 网络安全分析与情报大会

-- 郑聿铭 --

Splunk北方区技术顾问

ISOC

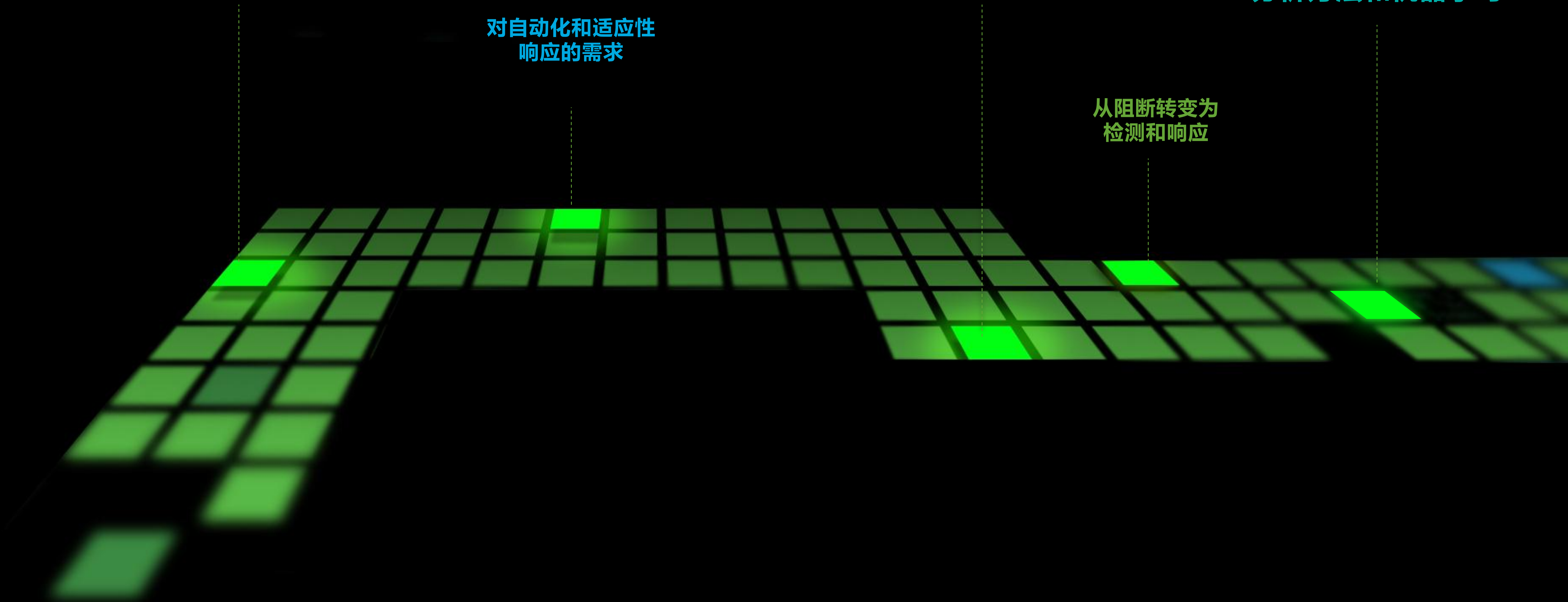
- ISOC = Intelligence-Driven Security Operations Center，智能化安全运营中心



Critical capabilities of Gartner's adaptive security architecture

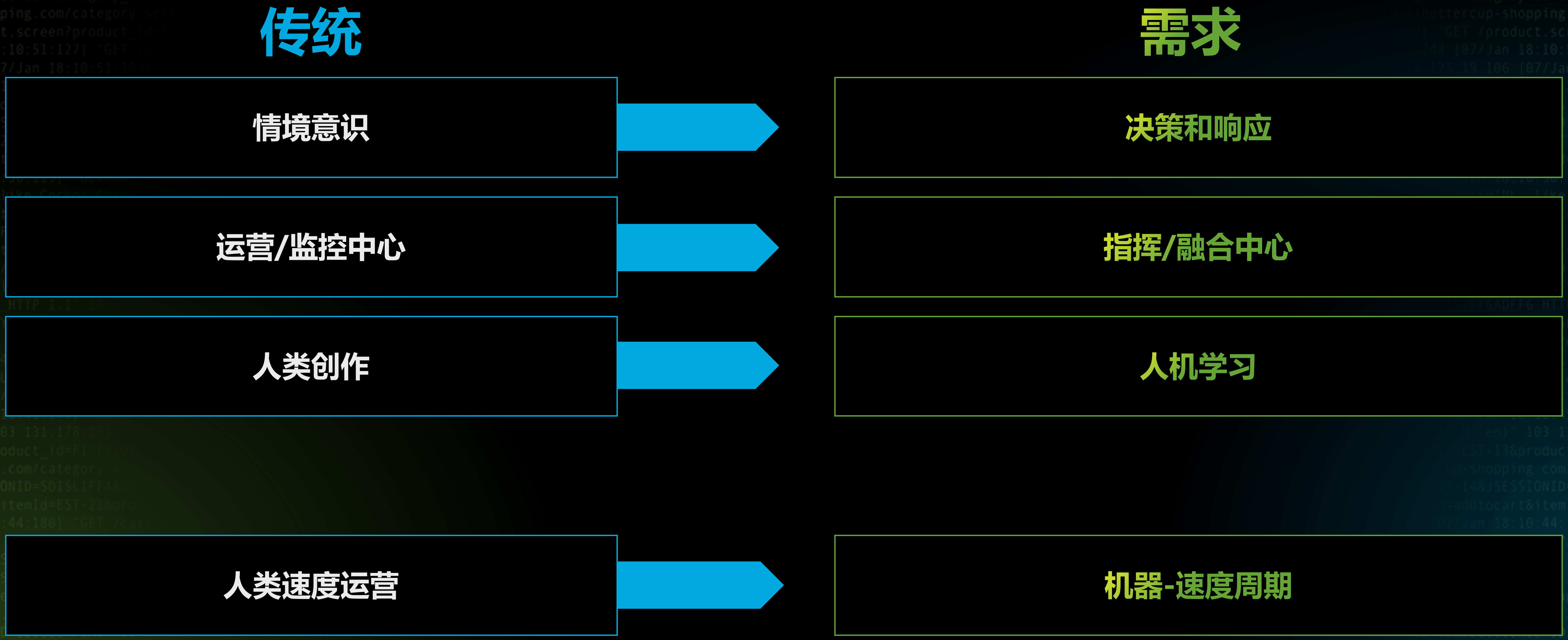
Source: Gartner (February 2014)

值得注意的趋势和转变



安全策略
依赖于数据策略
对自动化和适应性
响应的需求
威胁情报至关重要
从阻断转变为
检测和响应
用于威胁检测的
分析方法和机器学习

SOC转移的焦点和角色



传统

情境意识

运营/监控中心

人类创作

人类速度运营

需求

决策和响应

指挥/融合中心

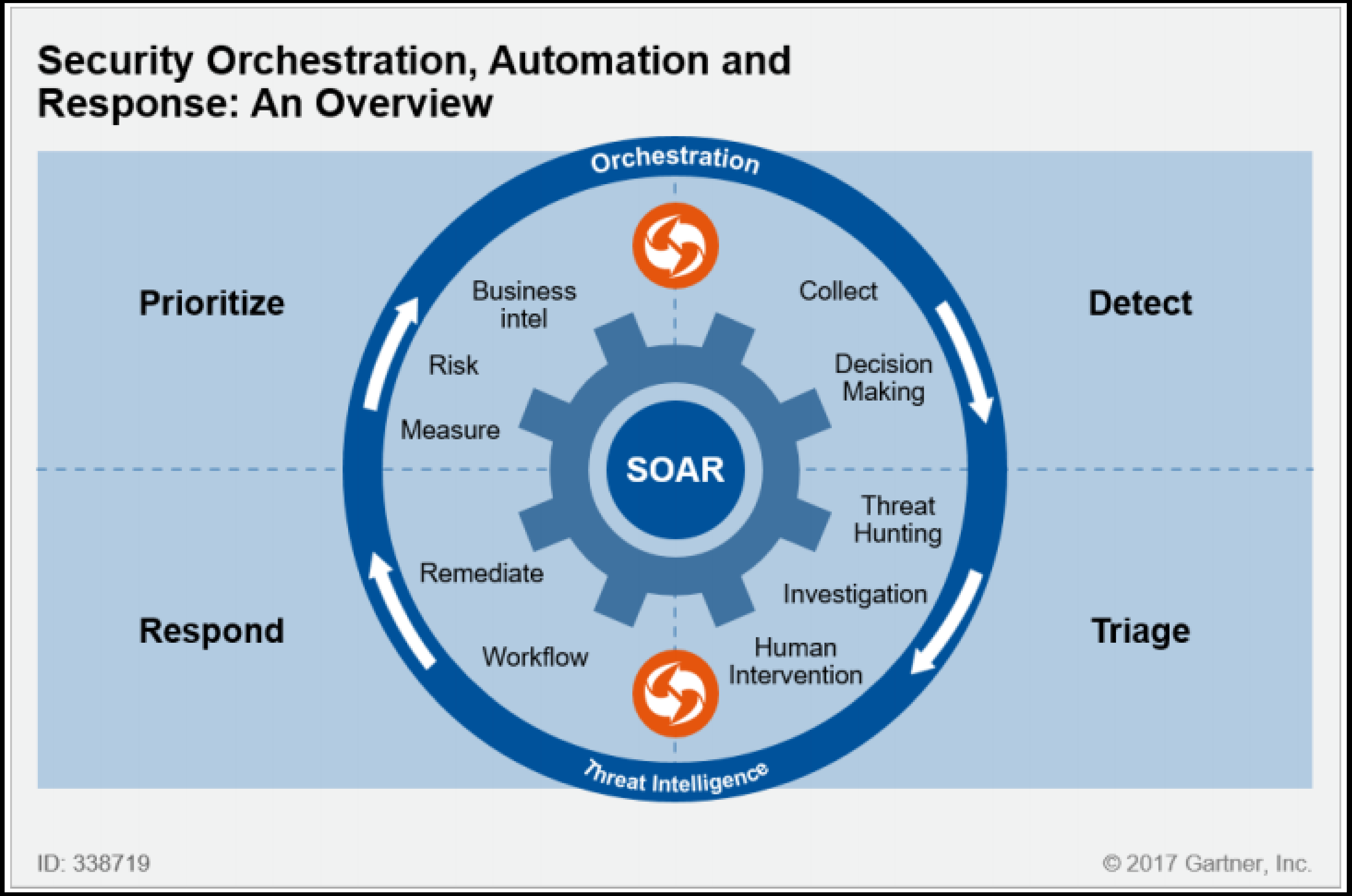
人机学习

机器-速度周期

什么是SOAR？

SOAR = Security Orchestration, Automation & Response

“...使相关组织能够收集来自不同来源的安全威胁数据和警报的技术，可以利用人机能力的结合执行事件分析和分类，以帮助根据标准工作流定义，优先化和驱动标准事件响应活动。”



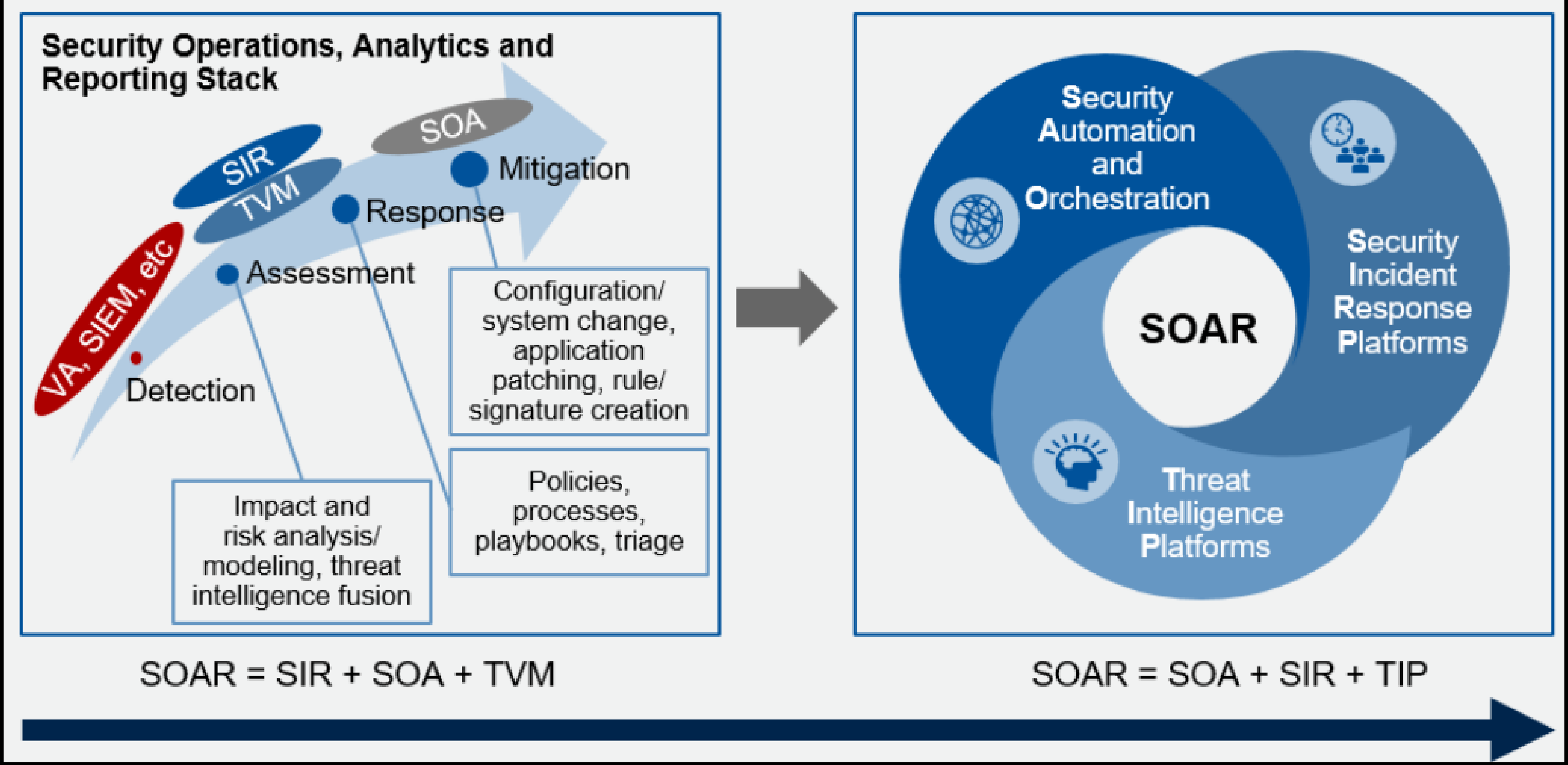
Security Orchestration, Automation and Response: An Overview

ID: 338719

© 2017 Gartner, Inc.

《安全编排、自动化与响应的创新洞察力》发表日期：2017年11月30日，ID：G00338719；分析员：Claudio Neiva, Craig Lawson, Toby Bussa, Gorka Sadowski

SOAR的演进



Security Operations, Analytics and Reporting Stack

VA, SIEM, etc

SIR

TVM

SOA

Detection

Assessment

Response

Mitigation

Configuration/ system change, application patching, rule/ signature creation

Policies, processes, playbooks, triage

Impact and risk analysis/ modeling, threat intelligence fusion

Security Automation and Orchestration

Security Incident Response Platforms

Threat Intelligence Platforms

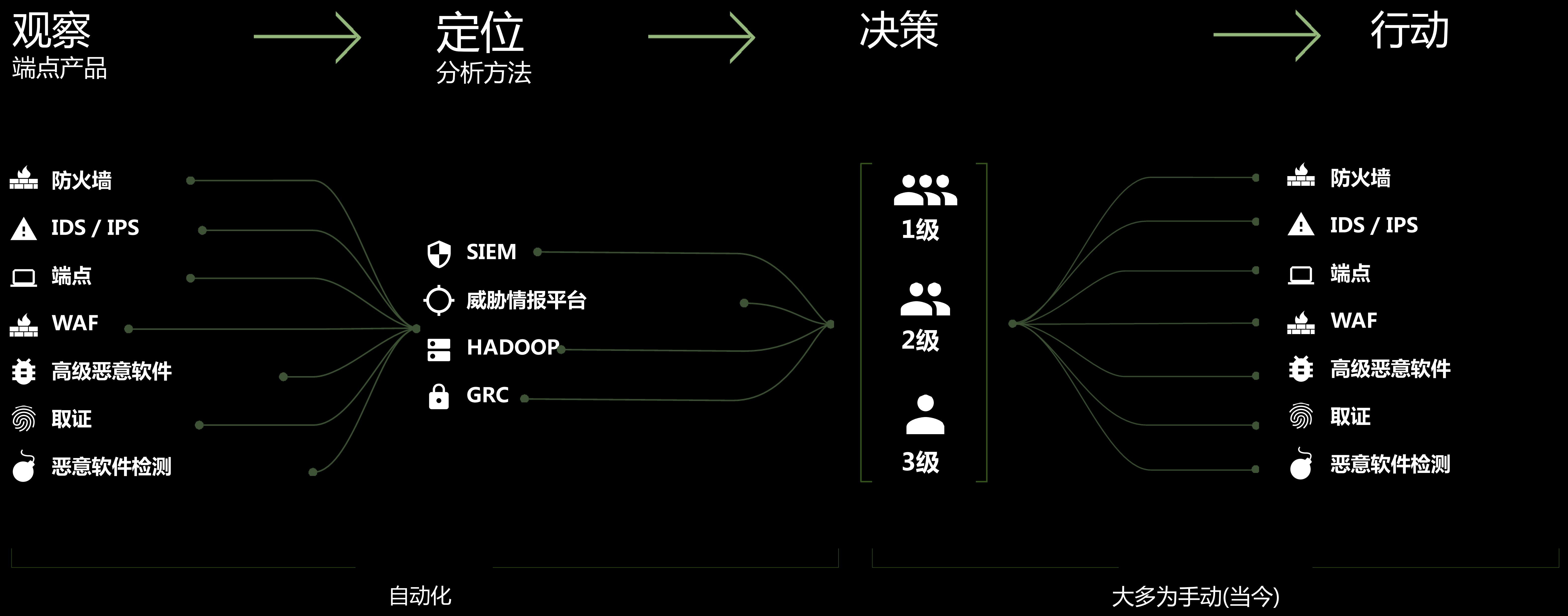
SOAR

SOAR = SIR + SOA + TVM

SOAR = SOA + SIR + TIP

自动化安全运营

了解SOAR



观察
端点产品

定位
分析方法

决策

行动

防火墙
IDS / IPS
端点
WAF
高级恶意软件
取证
恶意软件检测

SIEM
威胁情报平台
HADOOP
GRC

1级
2级
3级

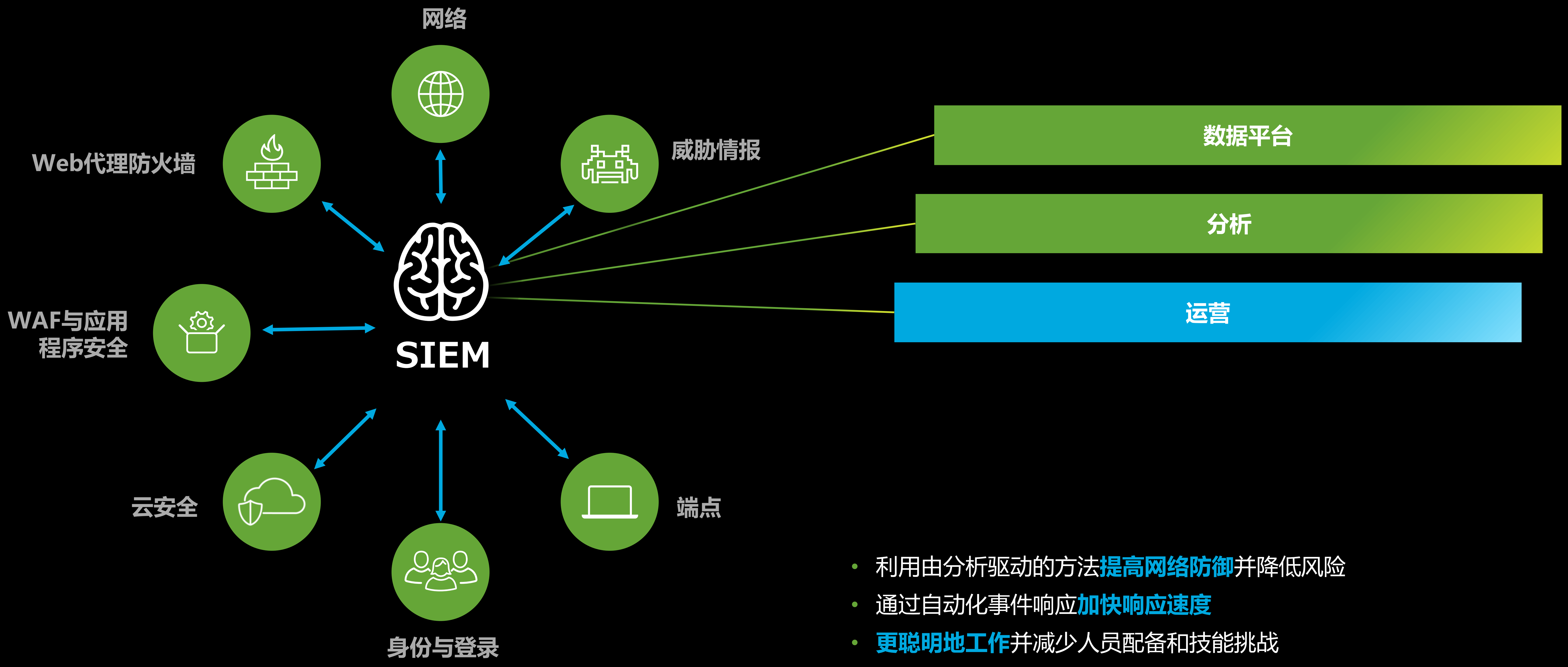
防火墙
IDS / IPS
端点
WAF
高级恶意软件
取证
恶意软件检测

自动化

大多为手动(当今)

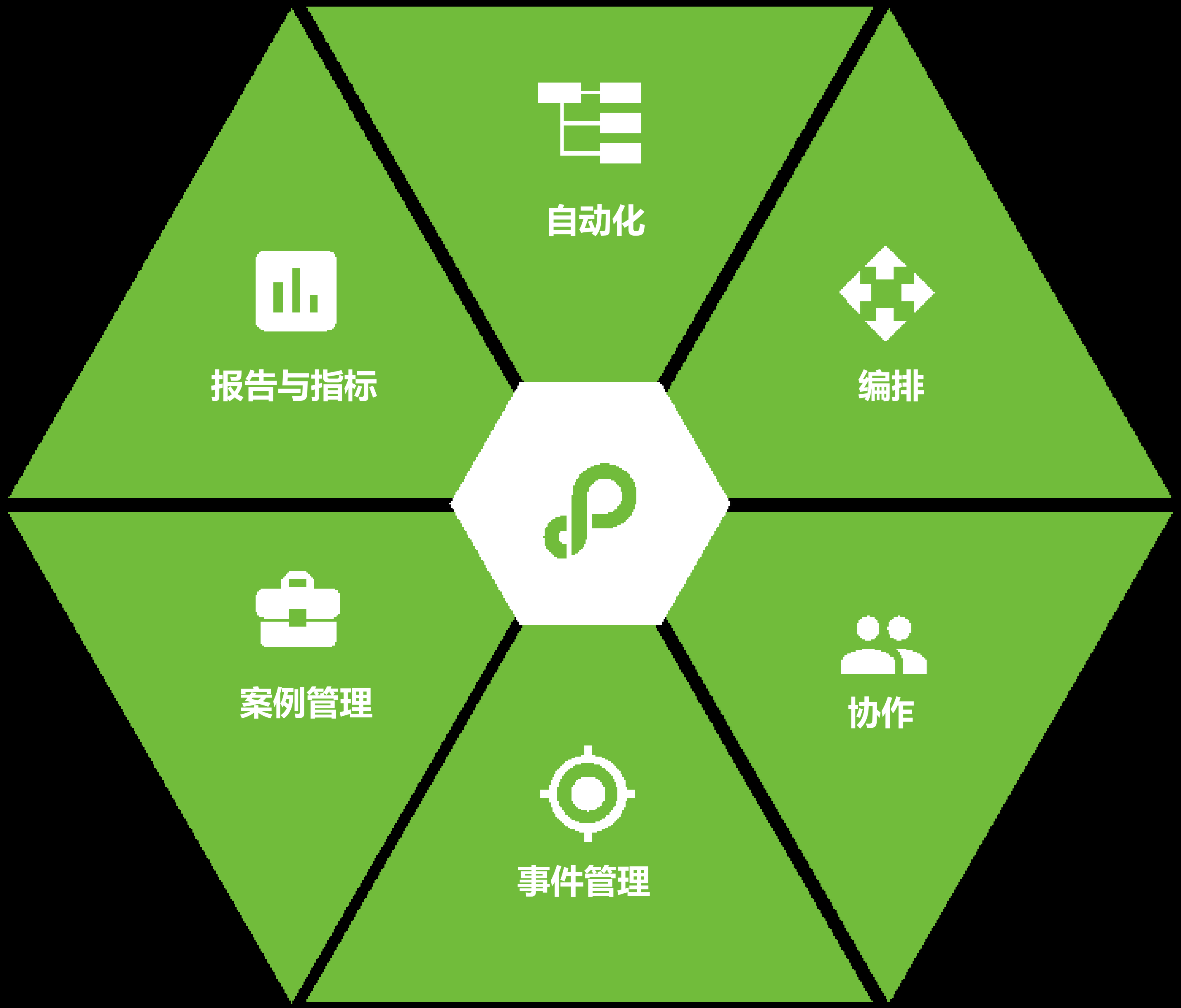
SOAR的价值

SOAR可以加速企业的神经中心安全愿景



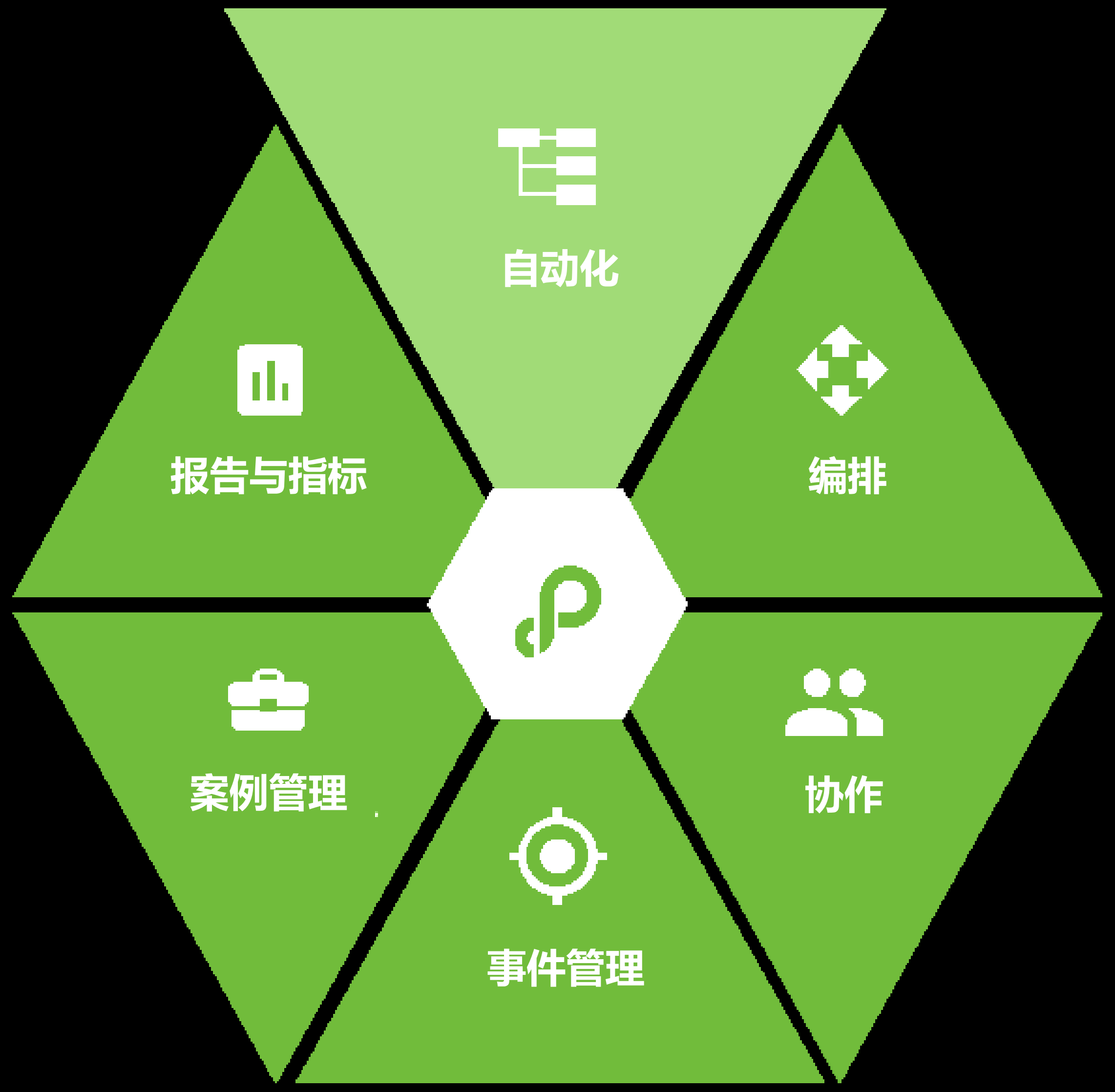
- 利用由分析驱动的方法**提高网络防御**并降低风险
- 通过自动化事件响应**加快响应速度**
- **更聪明地工作**并减少人员配备和技能挑战

SOAR平台落地的关键点



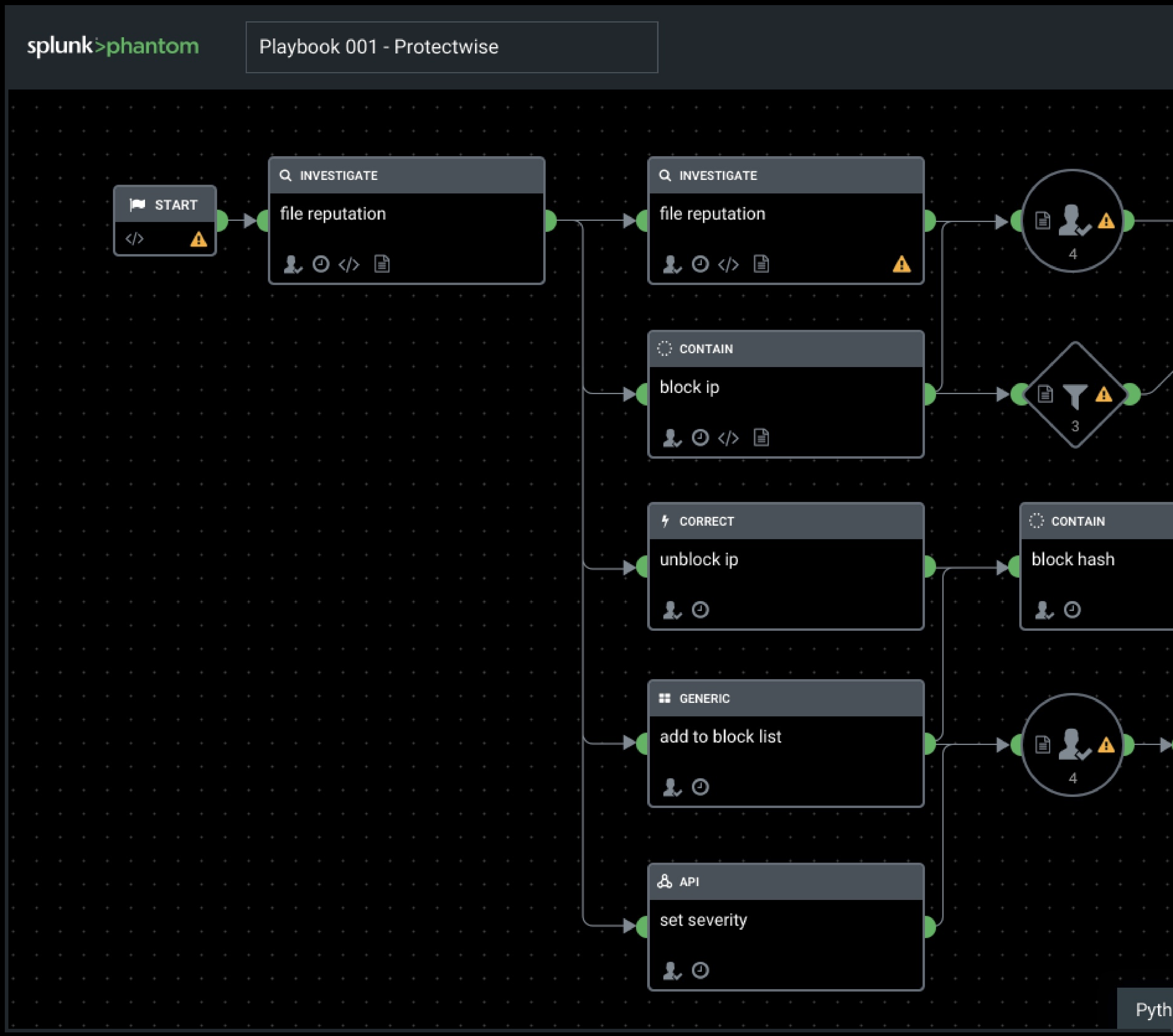
将您的团队、流程和工具整合在一起。

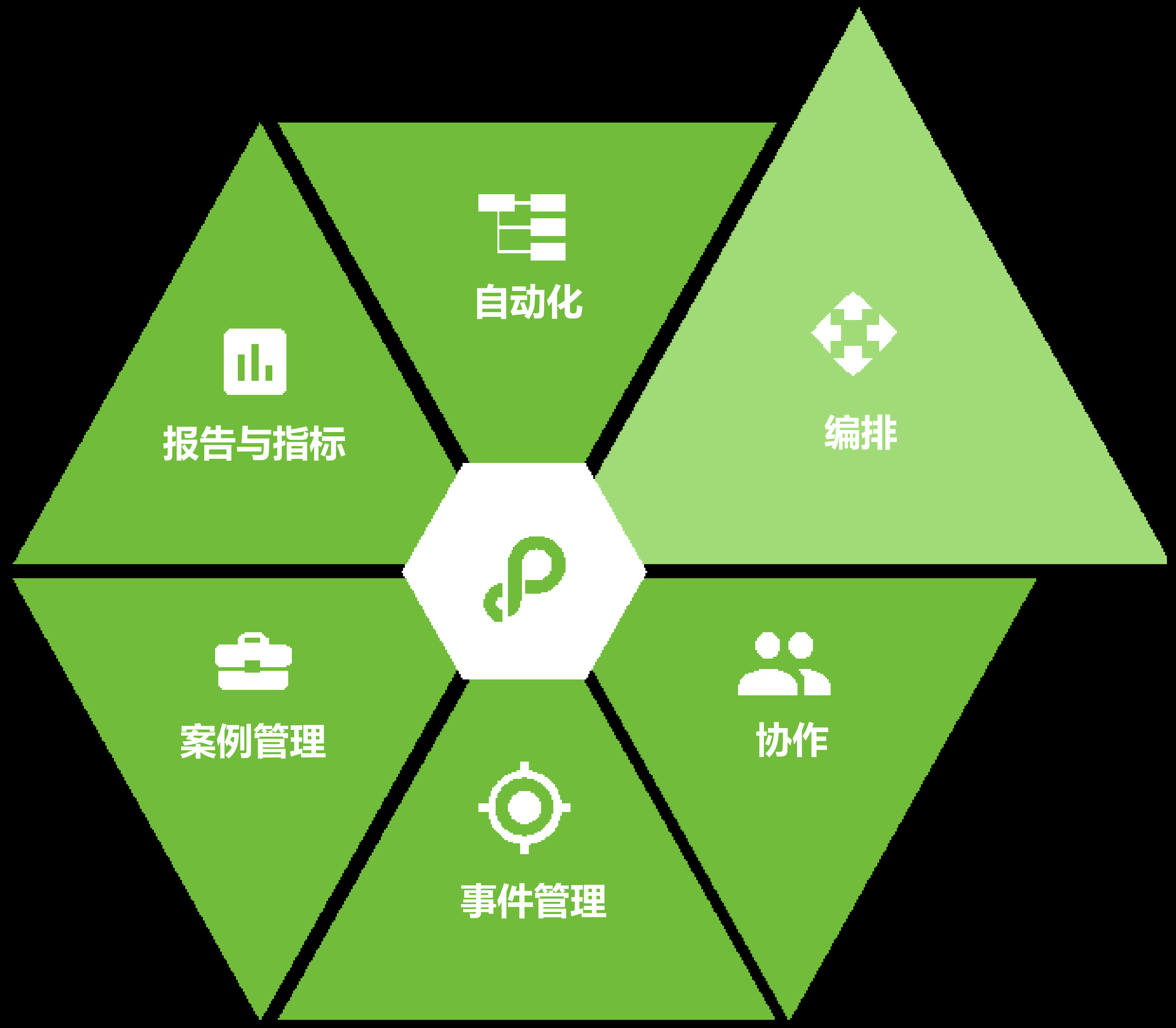
- 通过自动执行重复性任务，使分析人员将注意力放在更多关键任务，从而更智能地工作。
- 通过自动检测、调查和响应更快的作出响应并减少停留时间。
- 通过整合现有的安全基础设施加强防御，使每个部分都成为积极的参与者。



自动化

- 自动执行重复性任务以强化多重团队努力。
- 在数秒而非数小时内执行自动化操作。
- 预先获取情报以支持决策。



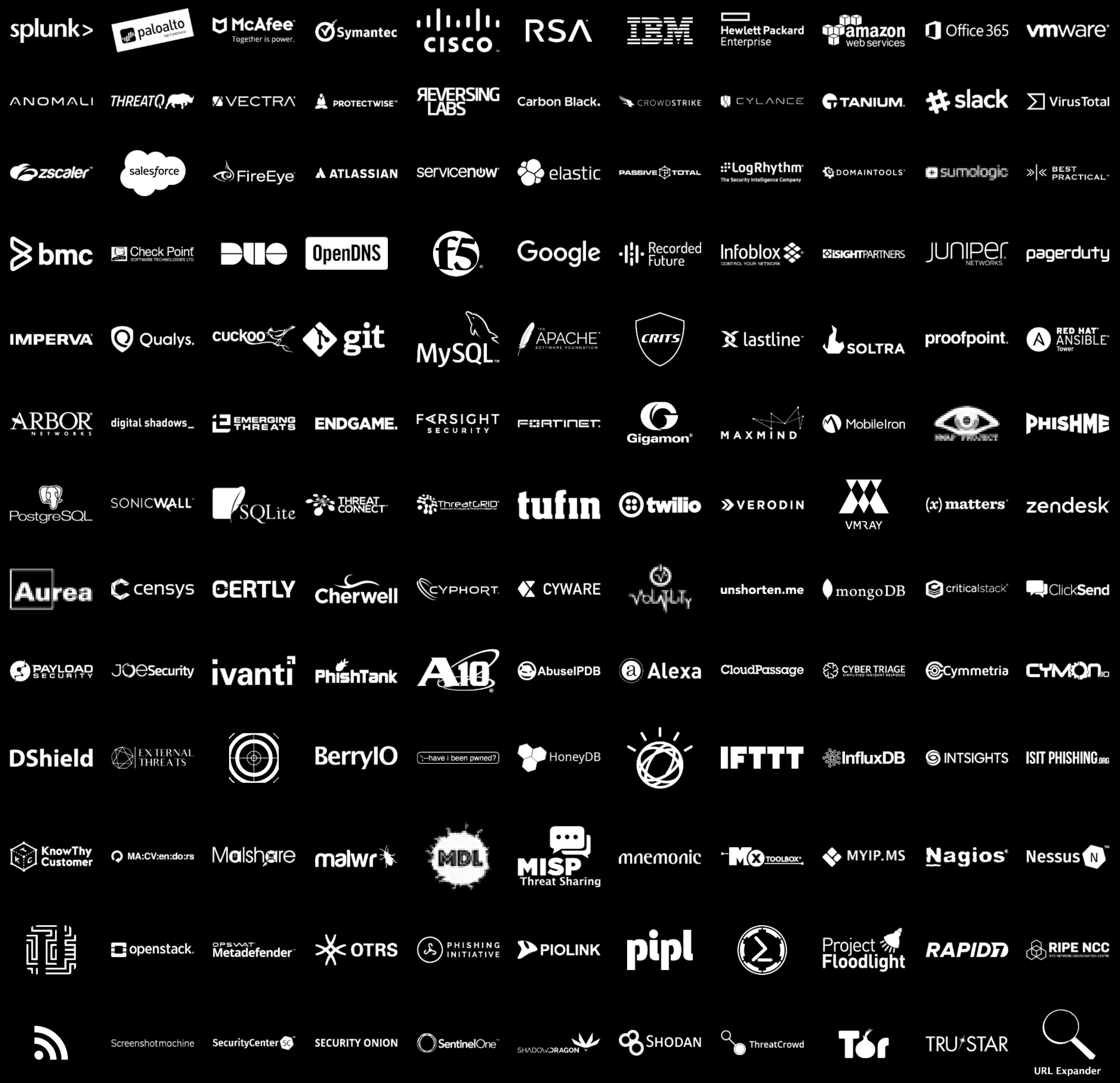


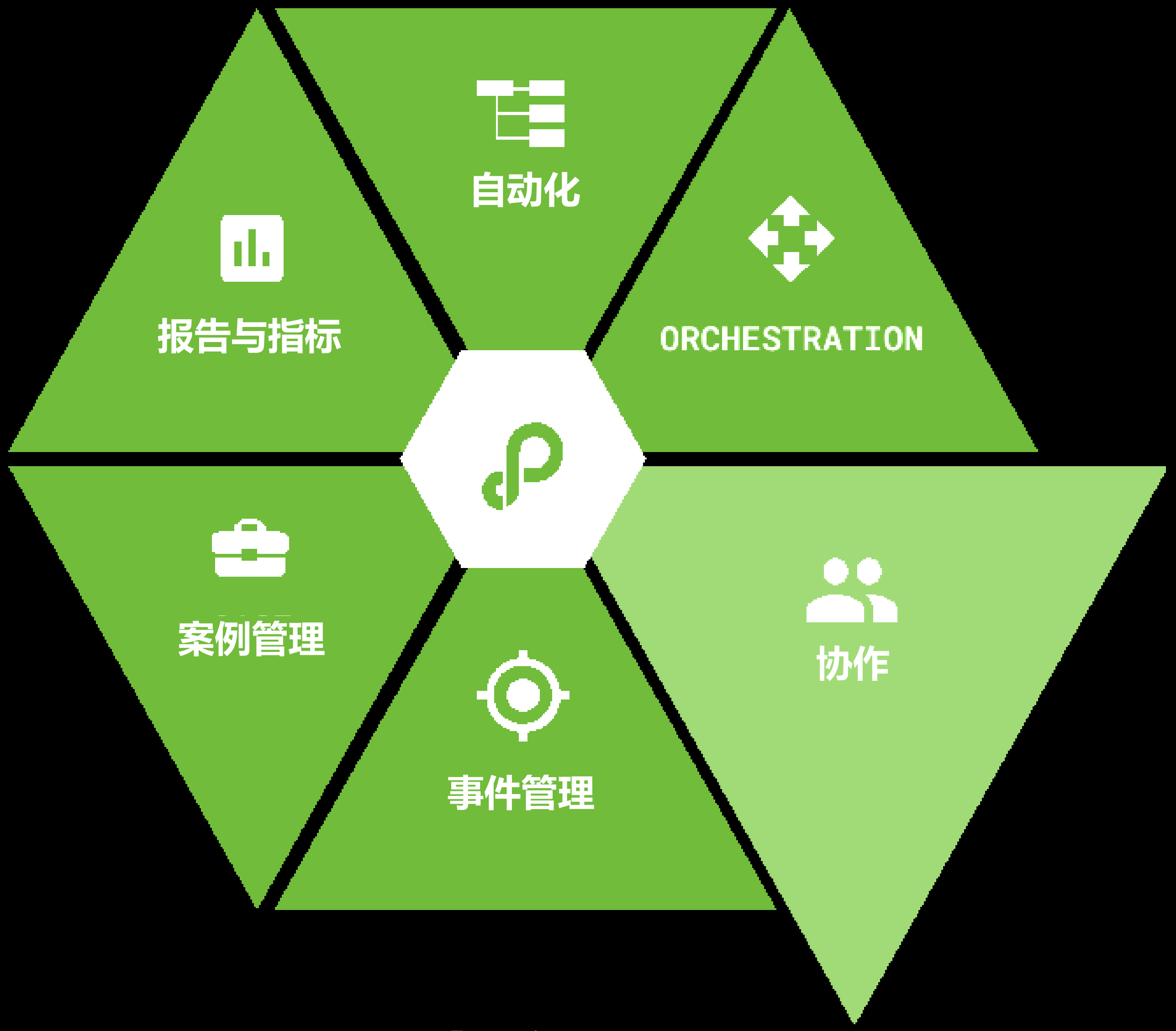
编排

协调整个SOC的复杂工作流程。

200+
应用程序与增长

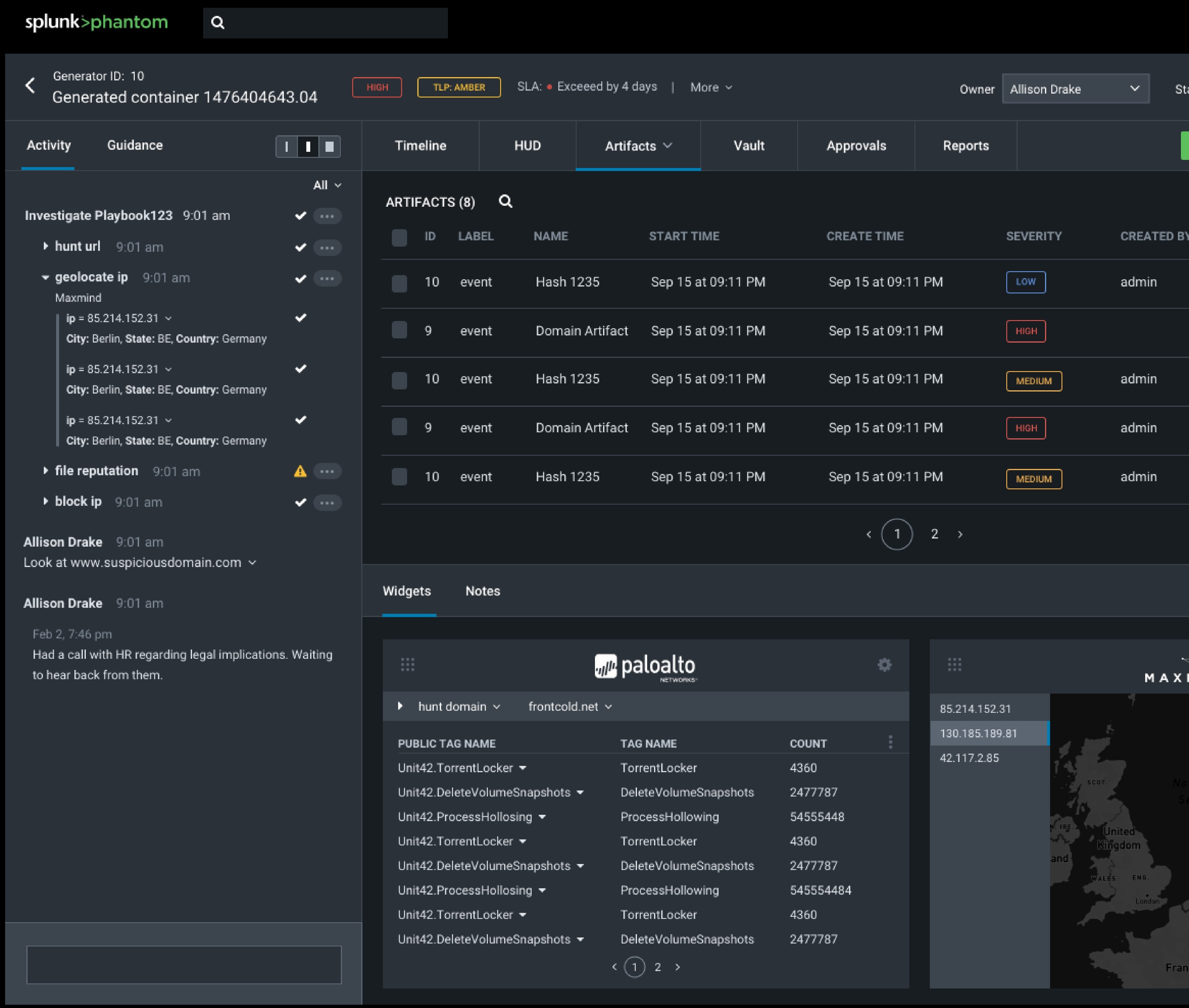
1000+
APIs





协作

- 在不丢失任务背景的情况下沟通。
- 与您的团队分享感兴趣的项目。
- 通过Phantom Mission Experts™获得共同知识。



Generator ID: 10
Generated container 1476404643.04

HIGH · TLP: AMBER · SLA: Exceeded by 4 days | More

Owner: Allison Drake

Investigate Playbook123 9:01 am ✓
- hunt url 9:01 am ✓
- geolocate ip 9:01 am ✓
  Maxmind
  - ip = 85.214.152.31 ✓
    City: Berlin, State: BE, Country: Germany
  - ip = 85.214.152.31 ✓
    City: Berlin, State: BE, Country: Germany
  - ip = 85.214.152.31 ✓
    City: Berlin, State: BE, Country: Germany
- file reputation 9:01 am ⚠
- block ip 9:01 am ✓

Allison Drake 9:01 am
Look at www.suspiciousdomain.com

Allison Drake 9:01 am
Feb 2, 7:46 pm
Had a call with HR regarding legal implications. Waiting to hear back from them.

ARTIFACTS (8)

ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY
10	event	Hash 1235	Sep 15 at 09:11 PM	Sep 15 at 09:11 PM	LOW	admin
9	event	Domain Artifact	Sep 15 at 09:11 PM	Sep 15 at 09:11 PM	HIGH	
10	event	Hash 1235	Sep 15 at 09:11 PM	Sep 15 at 09:11 PM	MEDIUM	admin
9	event	Domain Artifact	Sep 15 at 09:11 PM	Sep 15 at 09:11 PM	HIGH	admin
10	event	Hash 1235	Sep 15 at 09:11 PM	Sep 15 at 09:11 PM	MEDIUM	admin

‹ 1 2 ›

paloalto NETWORKS

hunt domain · frontcold.net

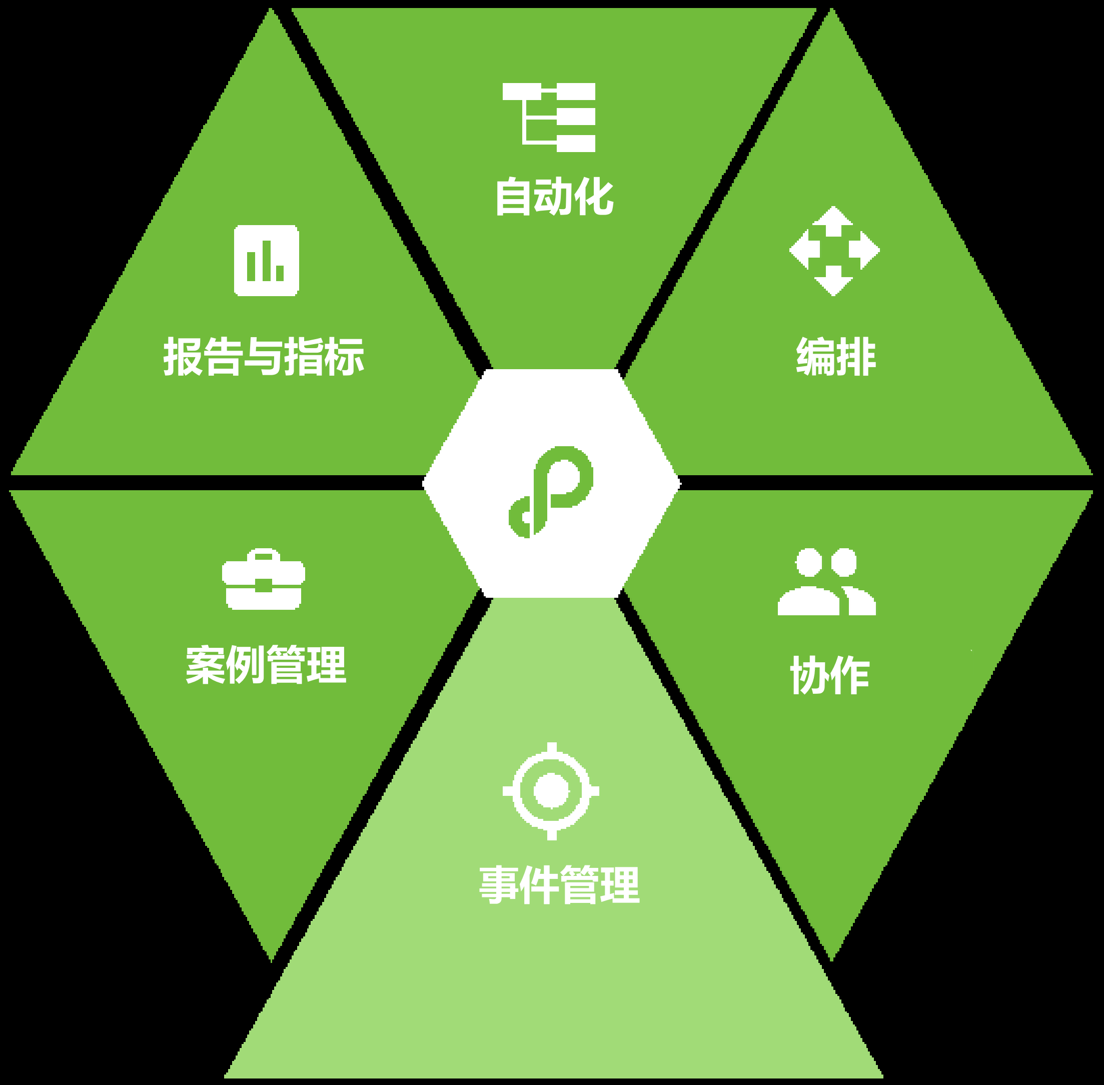
PUBLIC TAG NAME	TAG NAME	COUNT
Unit42.TorrentLocker	TorrentLocker	4360
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots	2477787
Unit42.ProcessHollosing	ProcessHollowing	54555448
Unit42.TorrentLocker	TorrentLocker	4360
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots	2477787
Unit42.ProcessHollosing	ProcessHollowing	545554484
Unit42.TorrentLocker	TorrentLocker	4360
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots	2477787

‹ 1 2 ›

MAXI

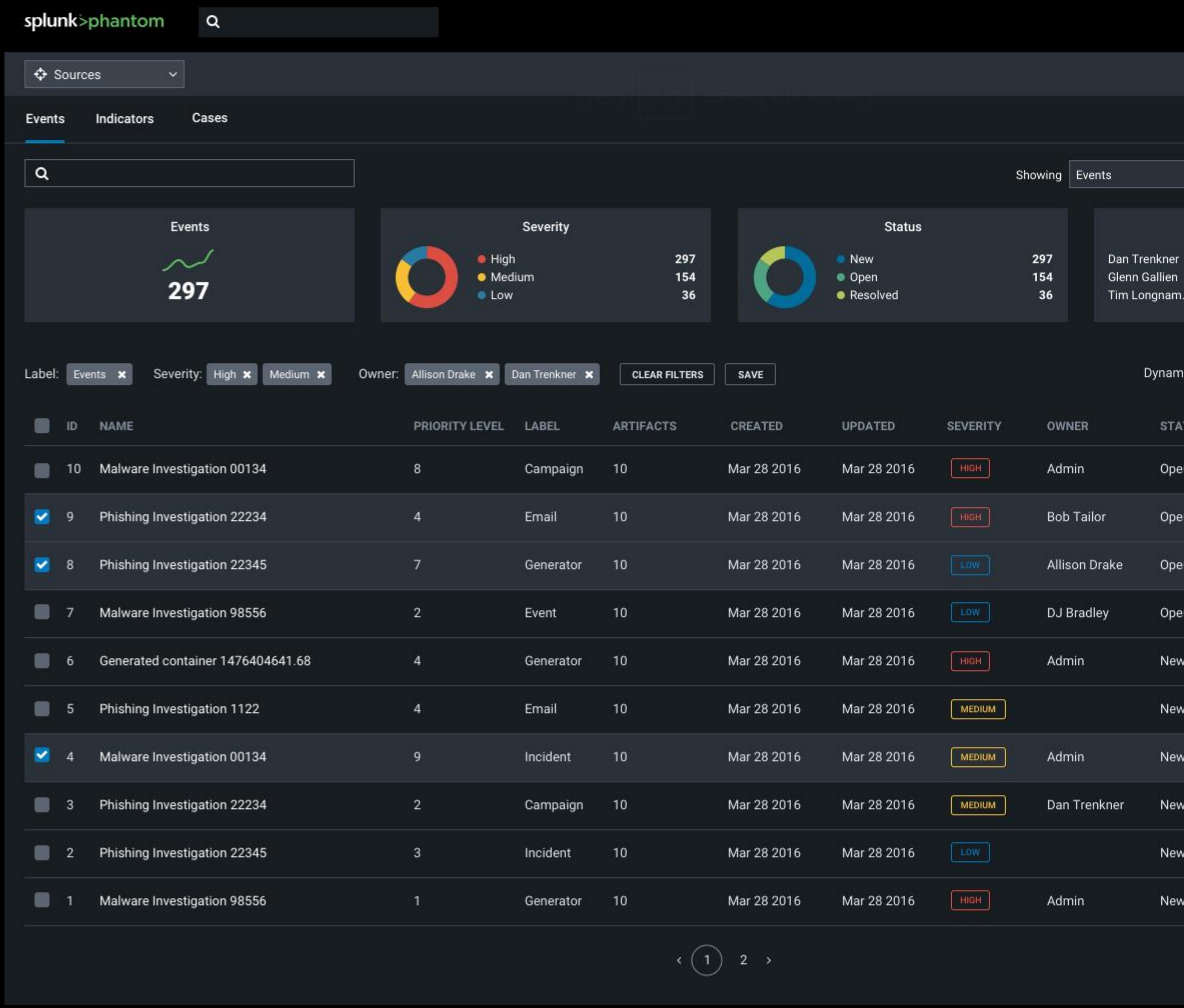
85.214.152.31
130.185.189.81
42.117.2.85

splunk> listen to your data



事件管理

- 首先分类最相关的事件。
- 消除工作量中的噪声。
- 将经过验证的事件升级为正式案例。



Events 297

Severity: High 297, Medium 154, Low 36

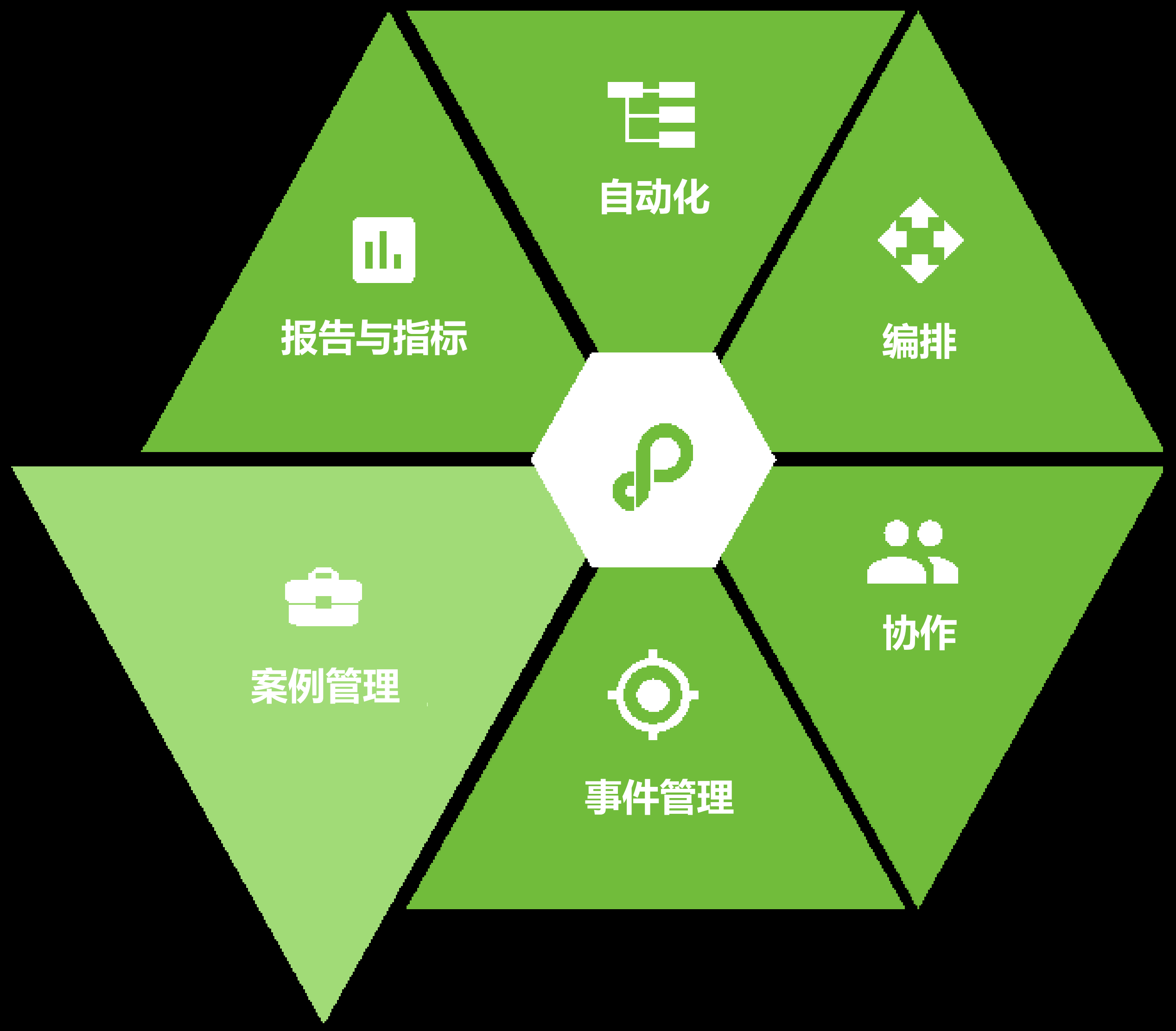
Status: New 297, Open 154, Resolved 36

Dan Trenkner
Glenn Gallien
Tim Longnam.

Label: Events ✖ Severity: High ✖ Medium ✖ Owner: Allison Drake ✖ Dan Trenkner ✖ CLEAR FILTERS SAVE Dynam

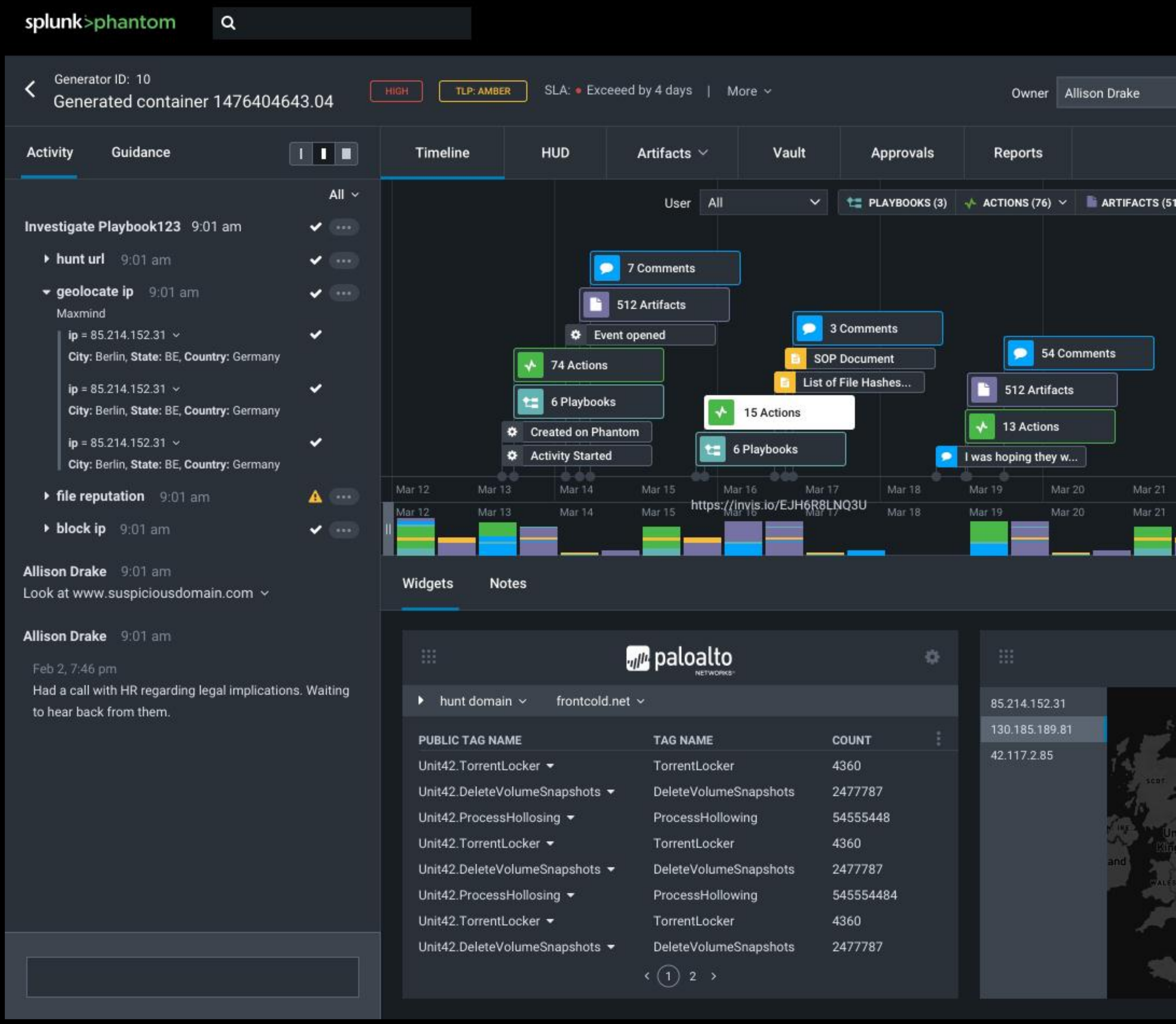
☐	ID	NAME	PRIORITY LEVEL	LABEL	ARTIFACTS	CREATED	UPDATED	SEVERITY	OWNER	STA
☐	10	Malware Investigation 00134	8	Campaign	10	Mar 28 2016	Mar 28 2016	HIGH	Admin	Ope
☑	9	Phishing Investigation 22234	4	Email	10	Mar 28 2016	Mar 28 2016	HIGH	Bob Tailor	Ope
☑	8	Phishing Investigation 22345	7	Generator	10	Mar 28 2016	Mar 28 2016	LOW	Allison Drake	Ope
☐	7	Malware Investigation 98556	2	Event	10	Mar 28 2016	Mar 28 2016	LOW	DJ Bradley	Ope
☐	6	Generated container 1476404641.68	4	Generator	10	Mar 28 2016	Mar 28 2016	HIGH	Admin	New
☐	5	Phishing Investigation 1122	4	Email	10	Mar 28 2016	Mar 28 2016	MEDIUM		New
☑	4	Malware Investigation 00134	9	Incident	10	Mar 28 2016	Mar 28 2016	MEDIUM	Admin	New
☐	3	Phishing Investigation 22234	2	Campaign	10	Mar 28 2016	Mar 28 2016	MEDIUM	Dan Trenkner	New
☐	2	Phishing Investigation 22345	3	Incident	10	Mar 28 2016	Mar 28 2016	LOW		New
☐	1	Malware Investigation 98556	1	Generator	10	Mar 28 2016	Mar 28 2016	HIGH	Admin	New

‹ 1 2 ›



案例管理

- 创建复制您SOP的案例模板。
- 精确管理您对威胁的响应。
- 在案例任务中嵌入自动化。



Generator ID: 10
Generated container 1476404643.04

SLA: • Exceeded by 4 days

Owner Allison Drake

Investigate Playbook123 9:01 am

- hunt url 9:01 am
- geolocate ip 9:01 am
  Maxmind
  ip = 85.214.152.31
  City: Berlin, **State:** BE, **Country:** Germany
  ip = 85.214.152.31
  City: Berlin, **State:** BE, **Country:** Germany
  ip = 85.214.152.31
  City: Berlin, **State:** BE, **Country:** Germany
- file reputation 9:01 am
- block ip 9:01 am

Allison Drake 9:01 am
Look at www.suspiciousdomain.com

Allison Drake 9:01 am

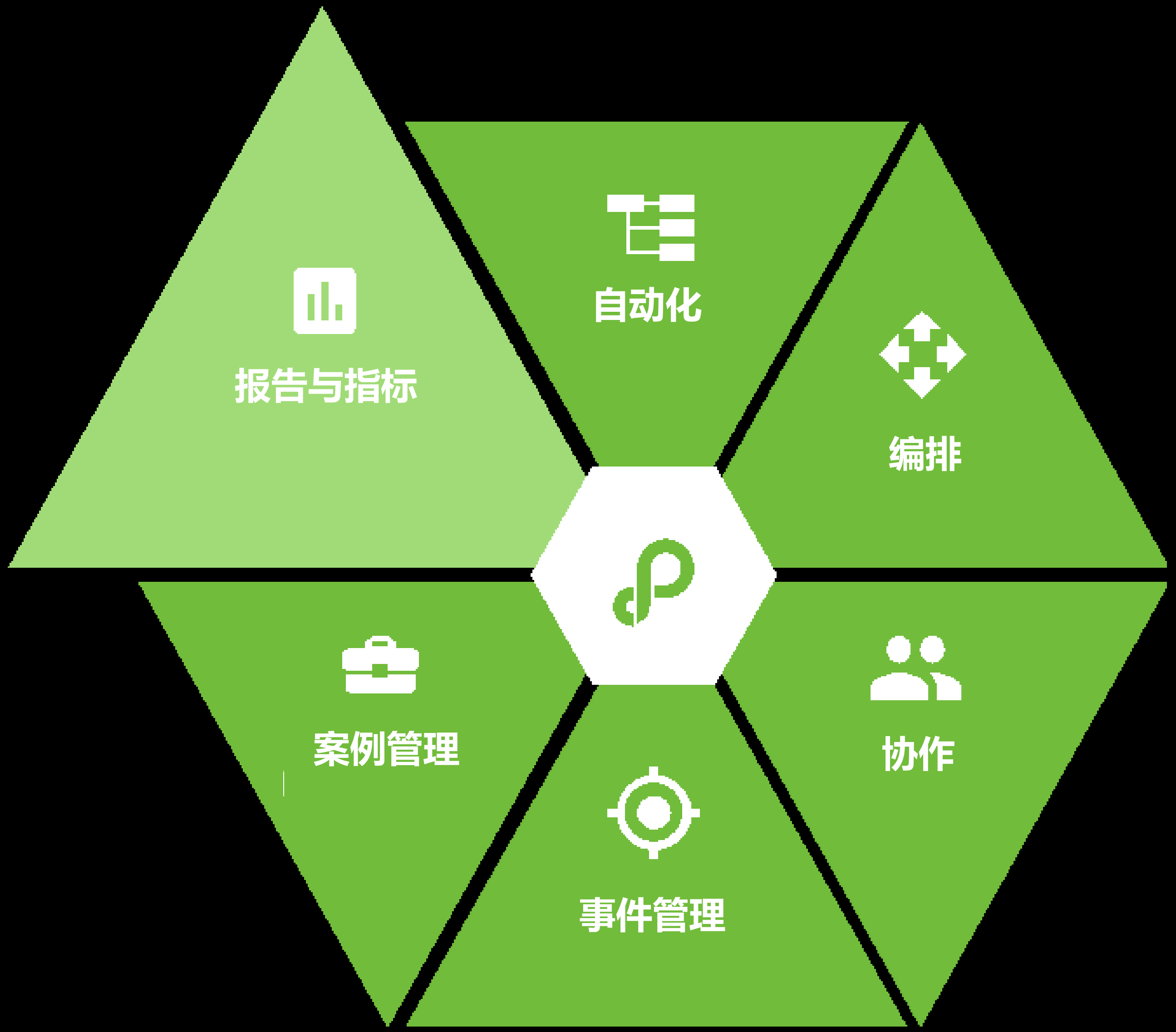
Feb 2, 7:46 pm
Had a call with HR regarding legal implications. Waiting to hear back from them.

hunt domain frontcold.net

PUBLIC TAG NAME	TAG NAME	COUNT
Unit42.TorrentLocker	TorrentLocker	4360
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots	2477787
Unit42.ProcessHollosing	ProcessHollowing	54555448
Unit42.TorrentLocker	TorrentLocker	4360
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots	2477787
Unit42.ProcessHollosing	ProcessHollowing	545554484
Unit42.TorrentLocker	TorrentLocker	4360
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots	2477787

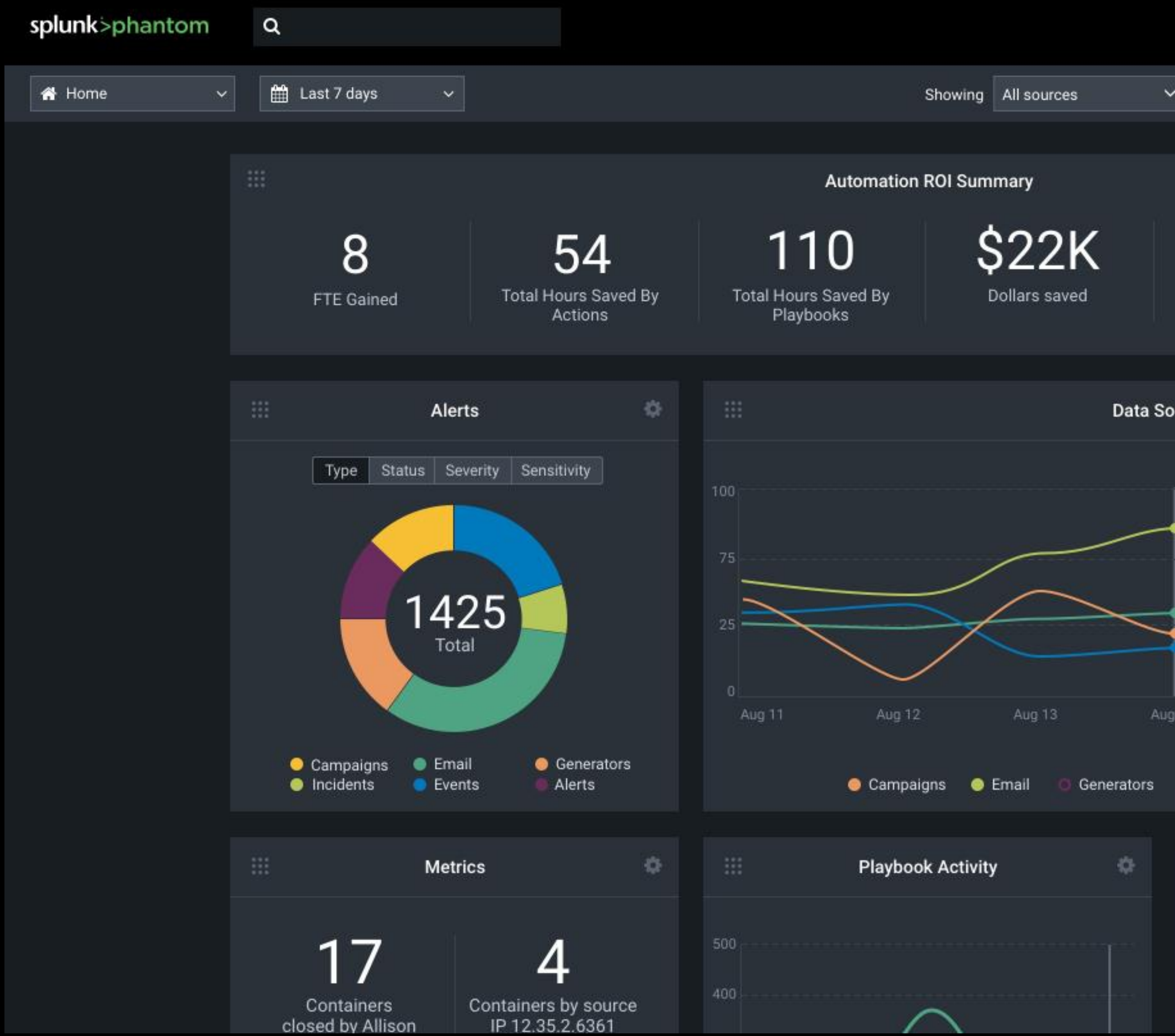
‹ 1 2 ›

85.214.152.31
130.185.189.81
42.117.2.85



报告和指标

- 快速评估运营状态和团队绩效。
- 进行事后案例审查。
- 证明您所在组织的安全投资回报。



Automation ROI Summary

8	54	110	$22K
FTE Gained	Total Hours Saved By Actions	Total Hours Saved By Playbooks	Dollars saved

Alerts

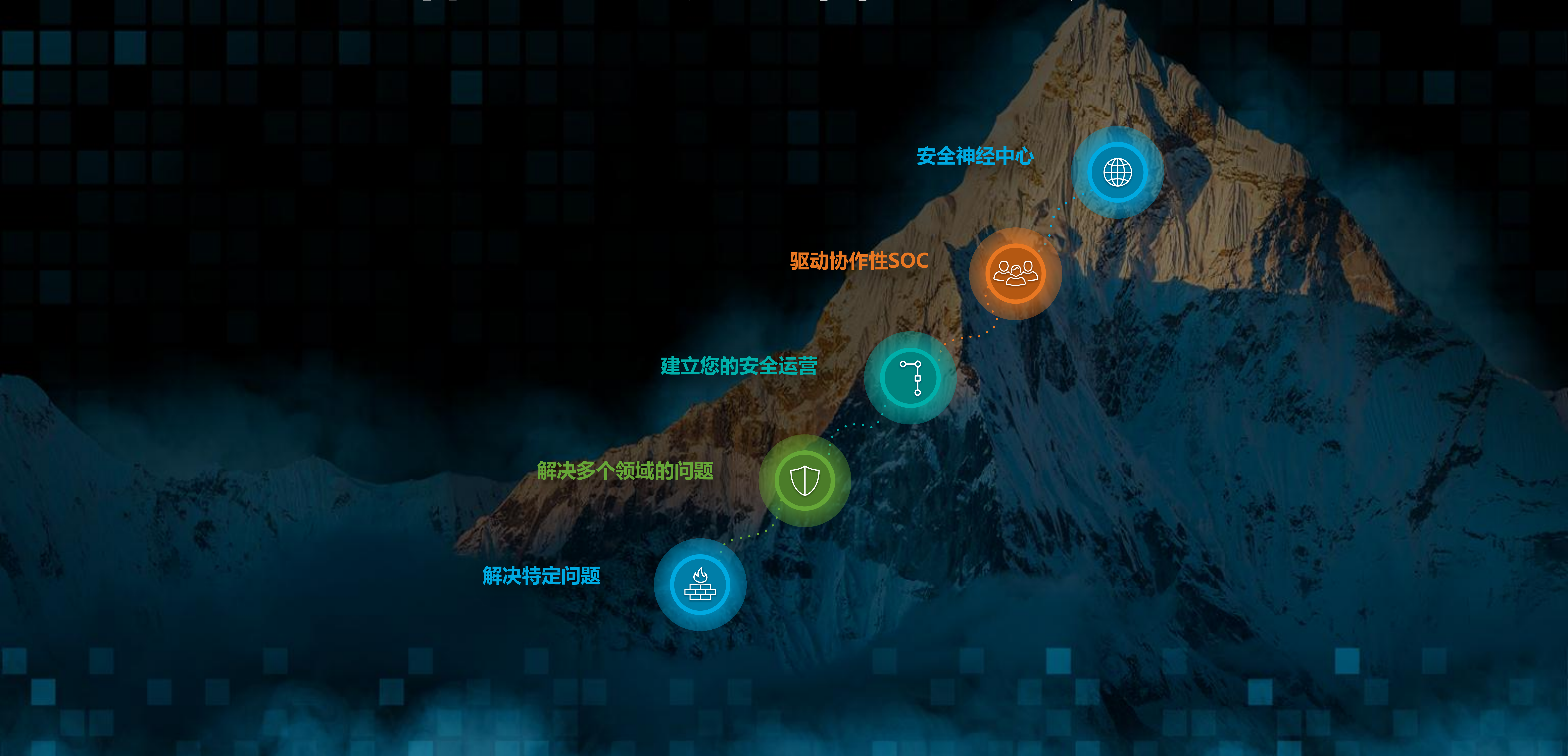
Data So

Metrics

17	4
Containers closed by Allison	Containers by source IP 12.35.2.6361

Playbook Activity

结语：企业安全运营建设成功之旅



安全神经中心

驱动协作性SOC

建立您的安全运营

解决多个领域的问题

解决特定问题

ThreatBook

感谢您的观看

2018 网络安全分析与情报大会