

# 威胁情报的发展展望

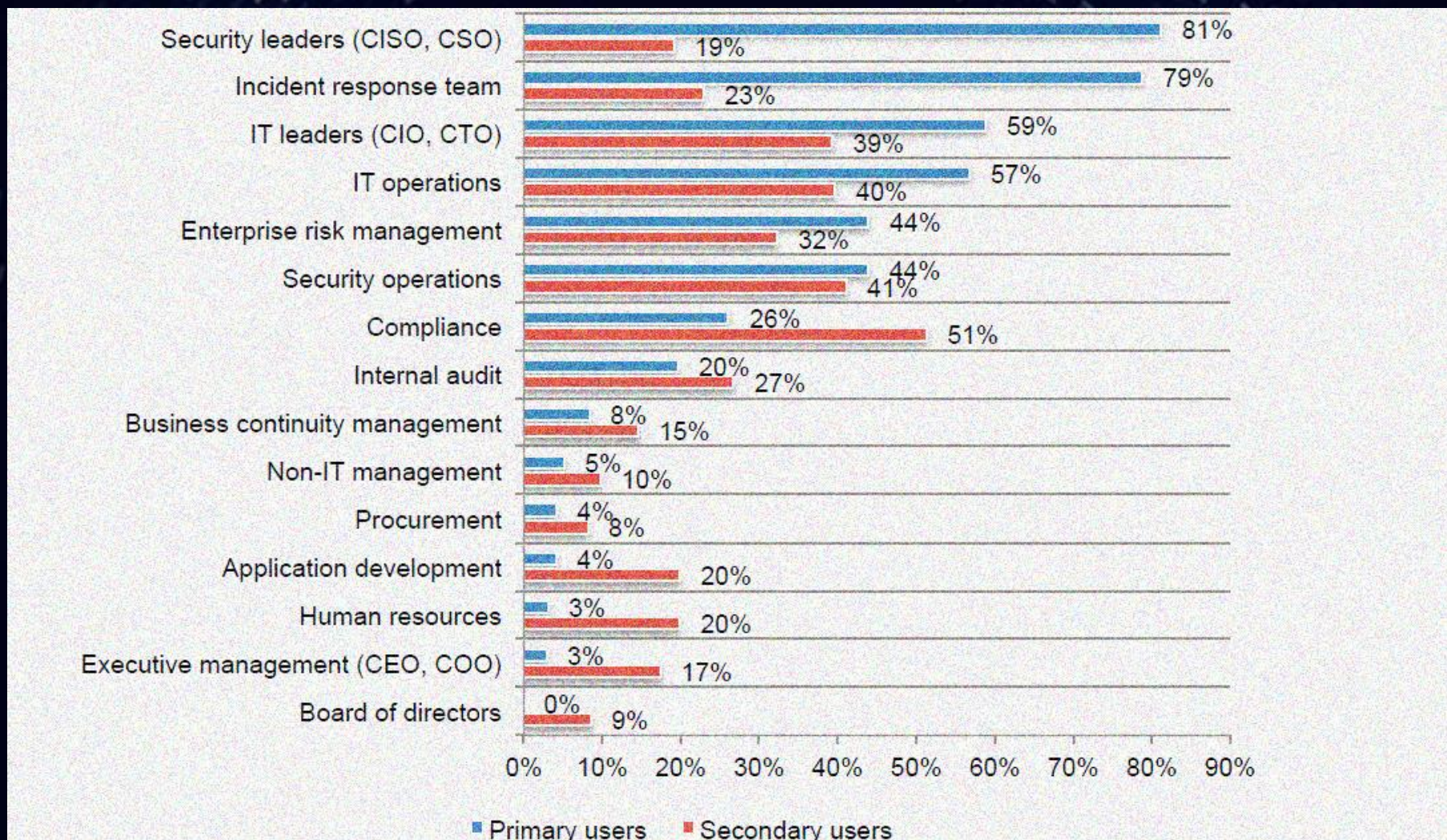
金湘宇/NUKE

君源创投



# 首先从一些用户反馈的数据开始

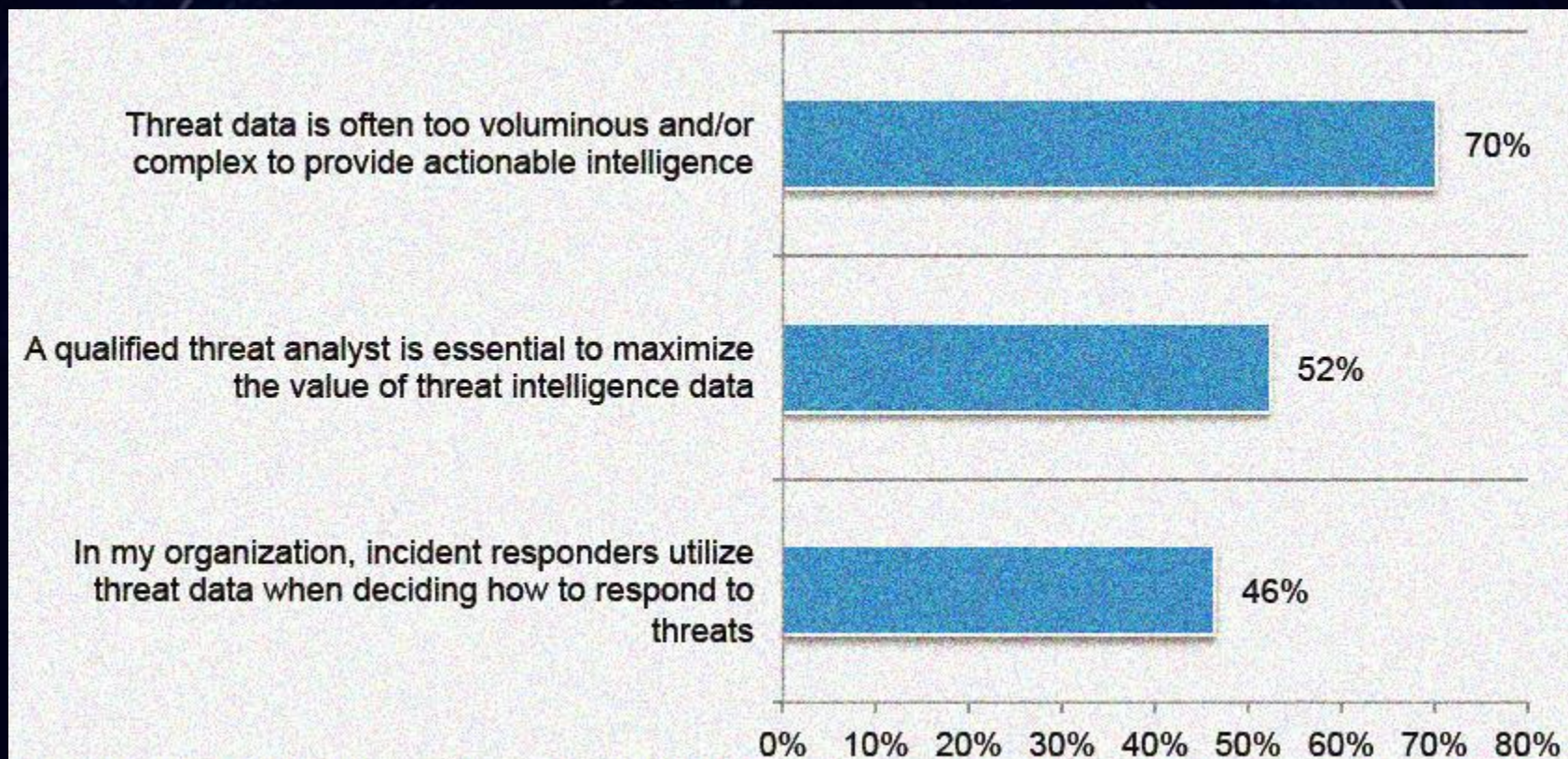
# 谁在为威胁情报买单？



***The Value of Threat Intelligence: A Study of North American & United Kingdom ,  
Ponemon Institute***



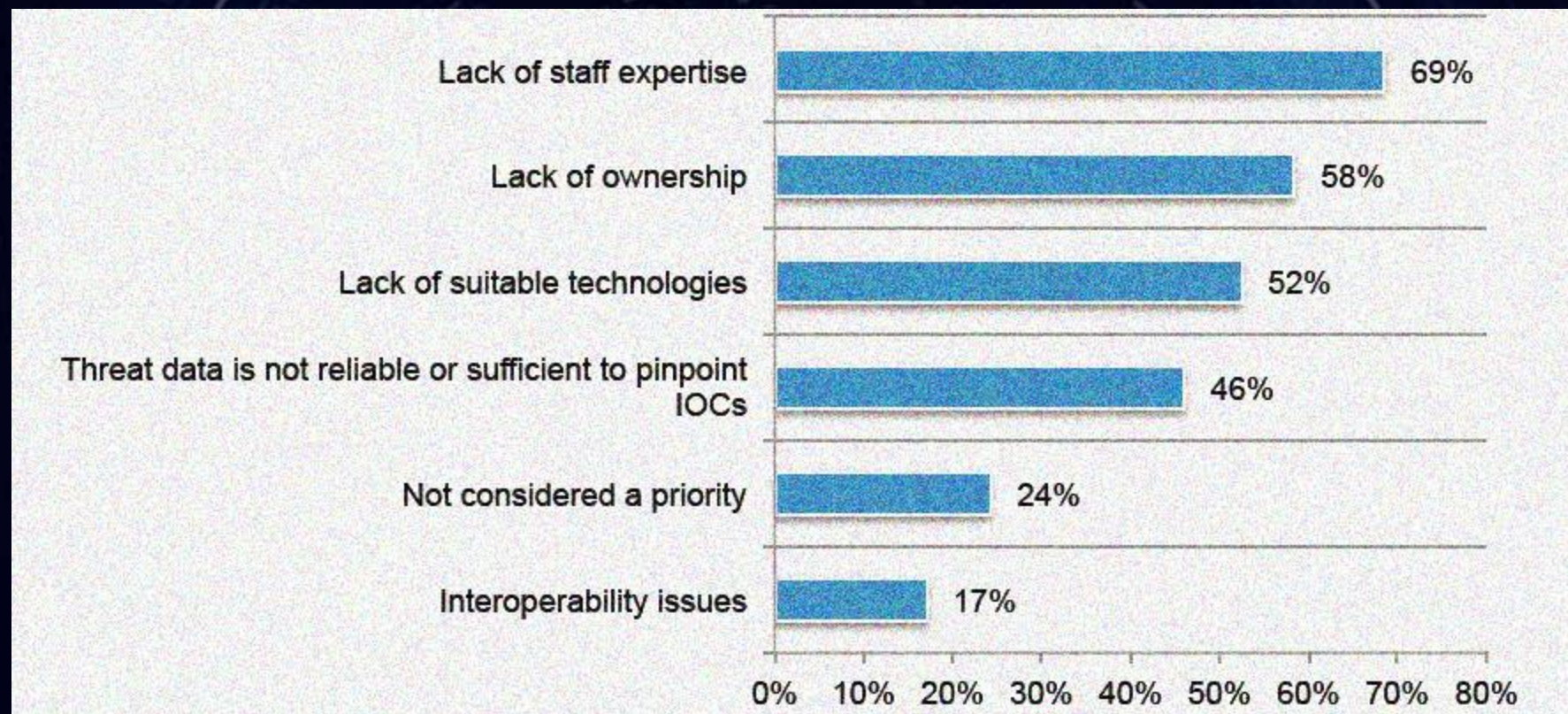
# 这玩意好用嘛？



***The Value of Threat Intelligence: A Study of North American & United Kingdom ,  
Ponemon Institute***



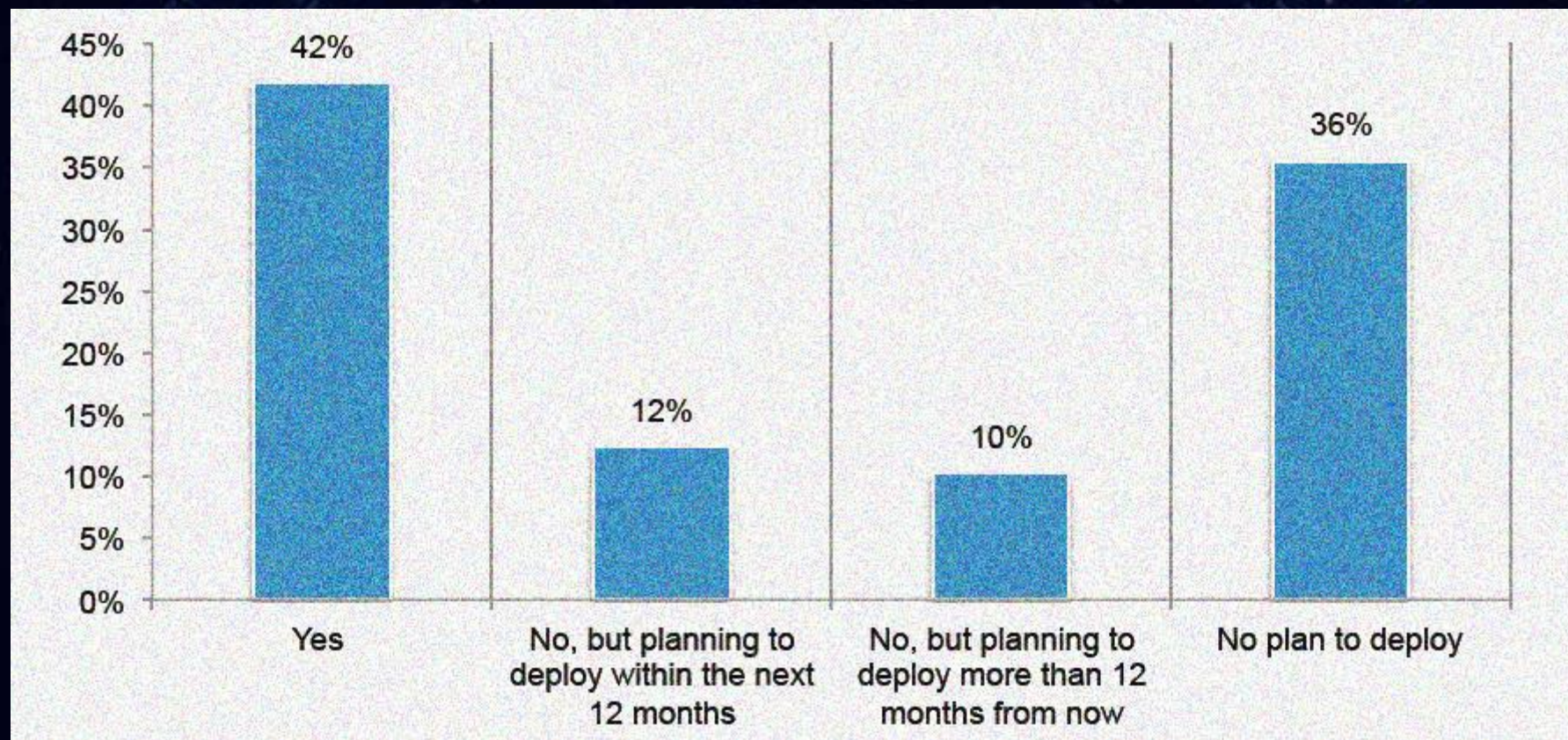
# 为啥觉得不好用？



***The Value of Threat Intelligence: A Study of North American & United Kingdom ,  
Ponemon Institute***



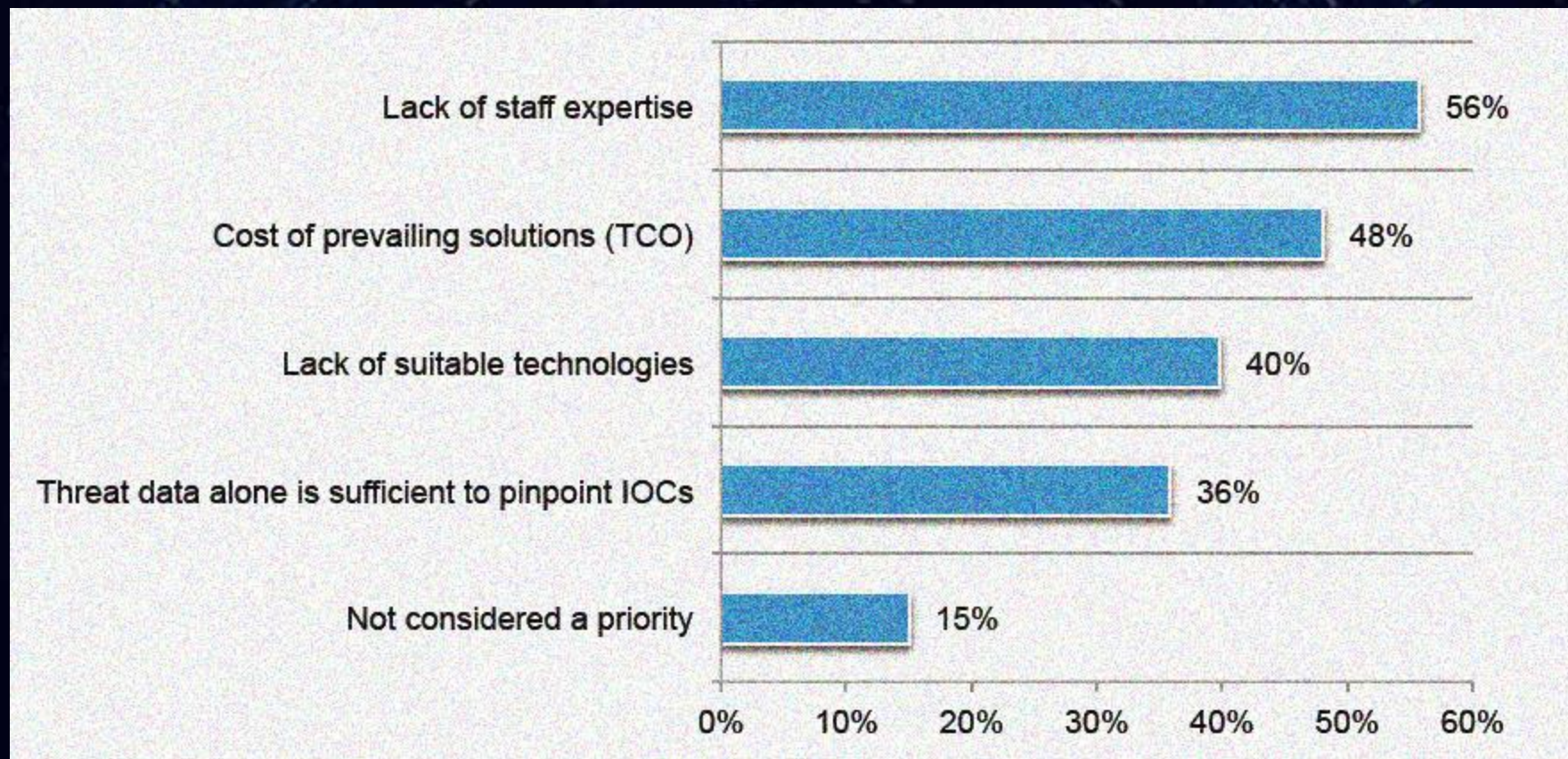
# 那你还打算用嘛？



***The Value of Threat Intelligence: A Study of North American & United Kingdom ,  
Ponemon Institute***



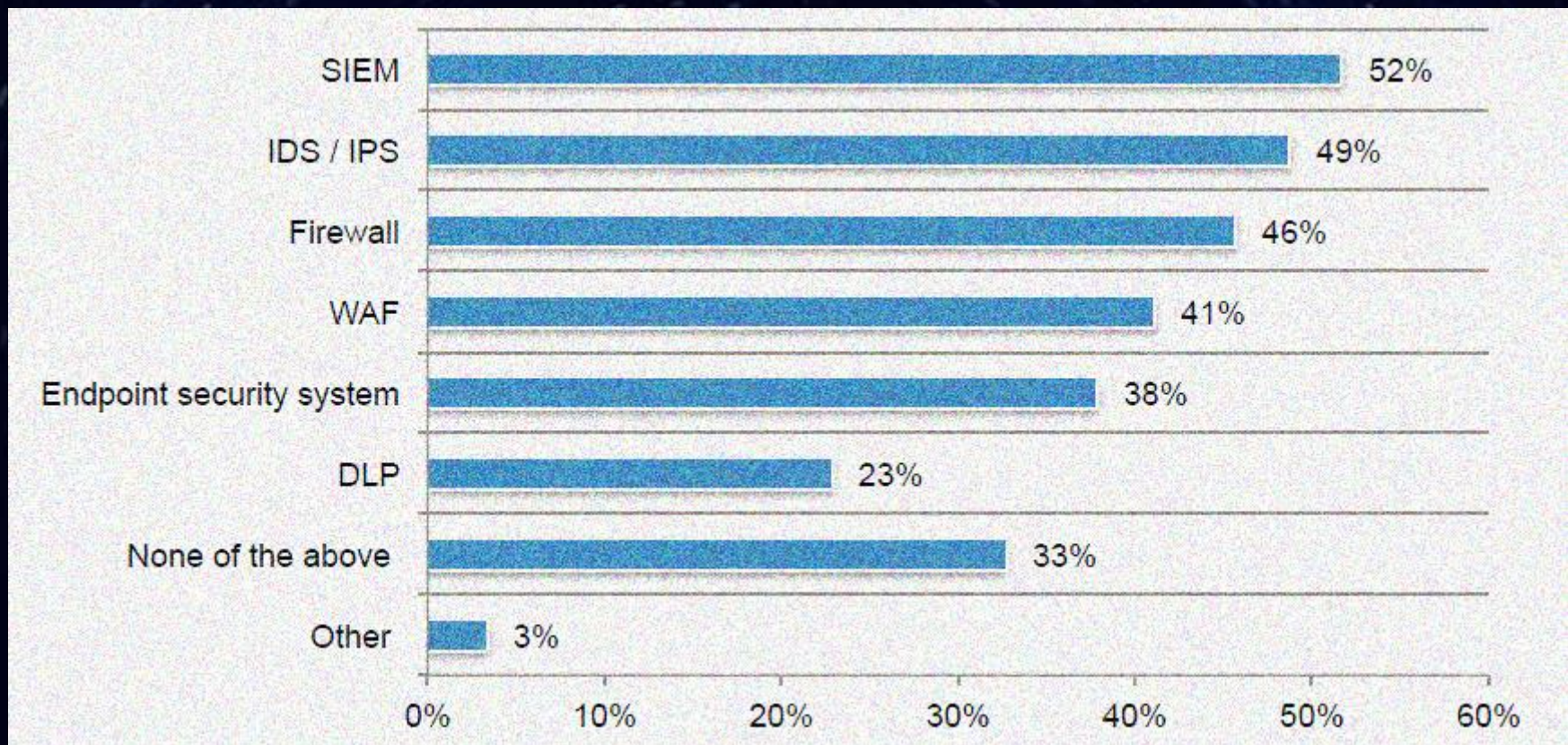
# 不打算用的，你为啥不用？



*The Value of Threat Intelligence: A Study of North American & United Kingdom ,  
Ponemon Institute*



# 打算用的，你希望怎么用？



***The Value of Threat Intelligence: A Study of North American & United Kingdom ,  
Ponemon Institute***



# 从战略到战术，情报交付的内容不断进化



# 人用？机用？

通常

进阶

结构文档

漏洞通告，样本分析报告.....

TTP分析报告，组织分析报告，COA.....

界面交互

溯源交互，回溯展现.....

设备互动、工作流.....

FEED

C2/APT/钓鱼 域名/IP，扫描IP，DDoS IP、TOR Exit-Add、样本Hash.....

Snort规则，YARA规则，SCAP/OVAL规则，PoC，工具Hash.....

API

IP地理位置，Whois，PDNS，域名/IP/文件信誉，证书，端口/服务/组件.....

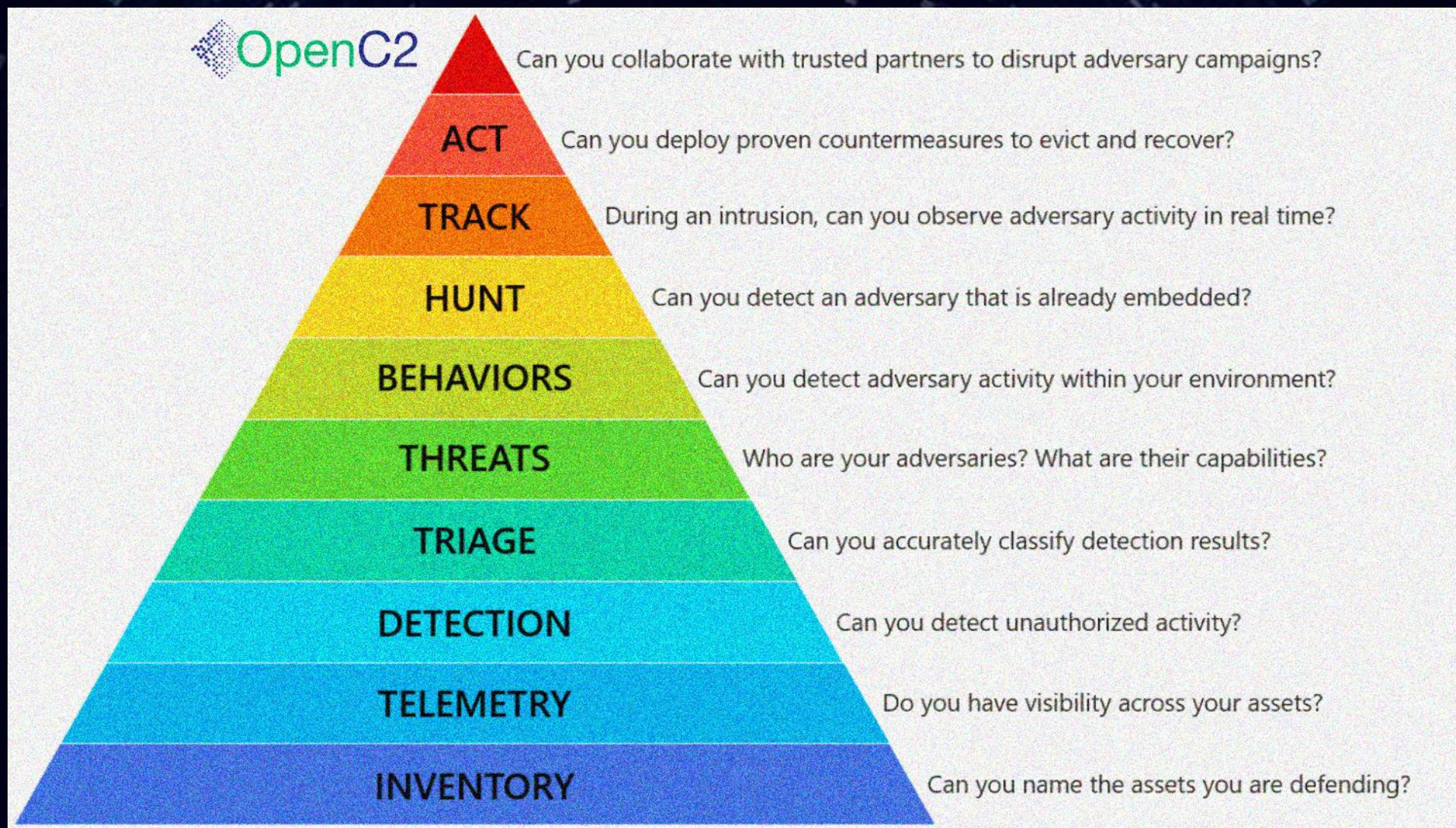
样本行为分析，高级漏洞信息，人员信息，比特币信息，社工库，备案，舆情.....



从发现到处置，有病也需要有药

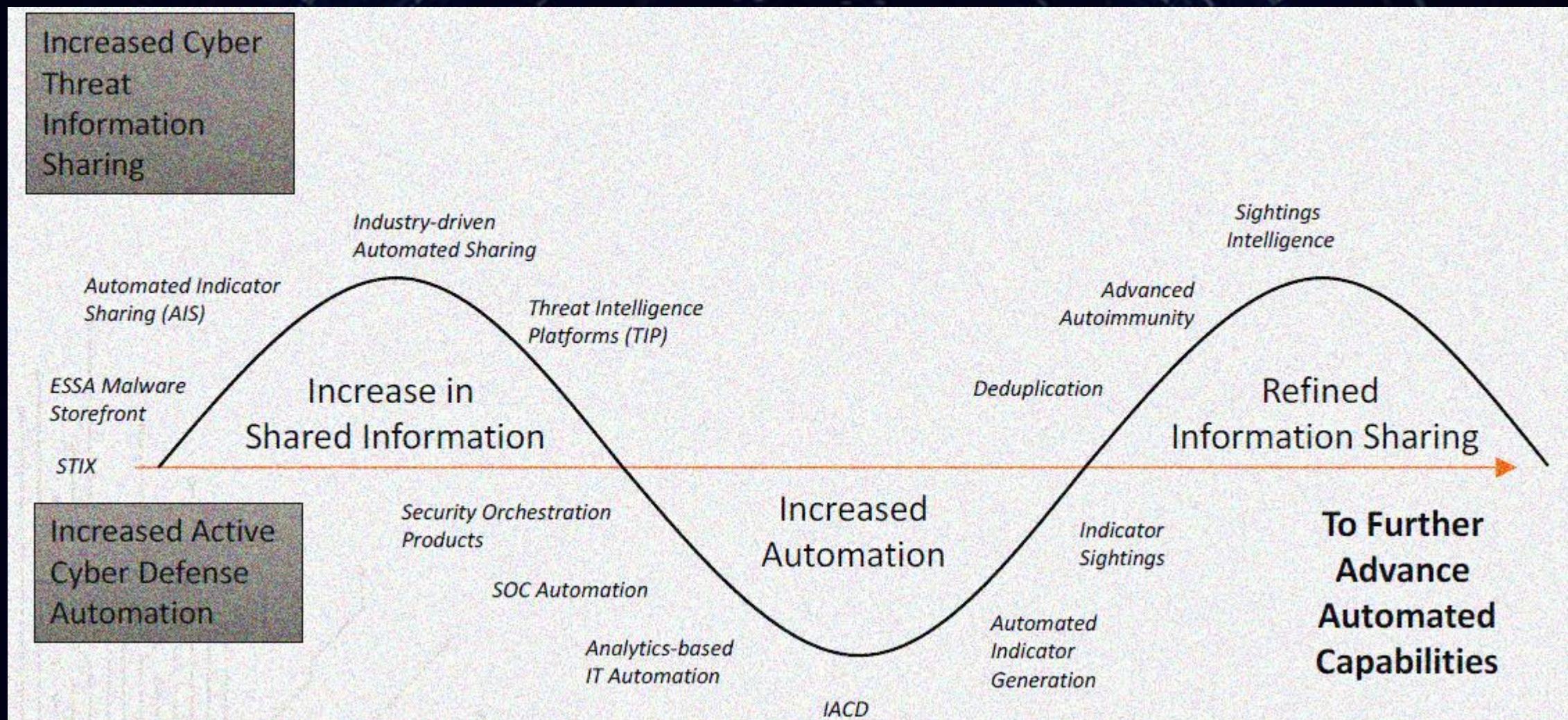


# Actionable ? Actionable !





# 可执行，再次引发了威胁情报的进化

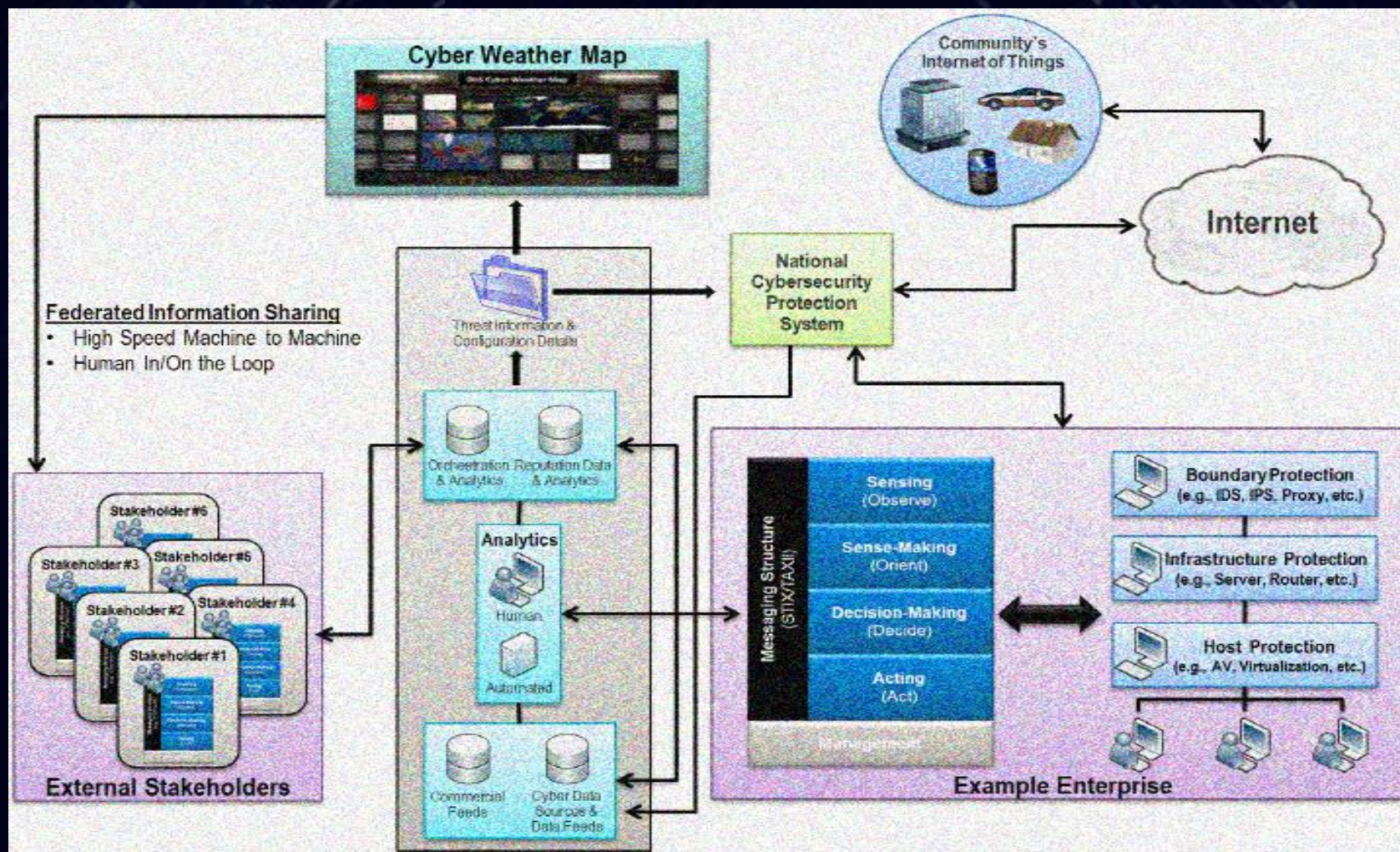




# 从情报到体系，未来就在前方



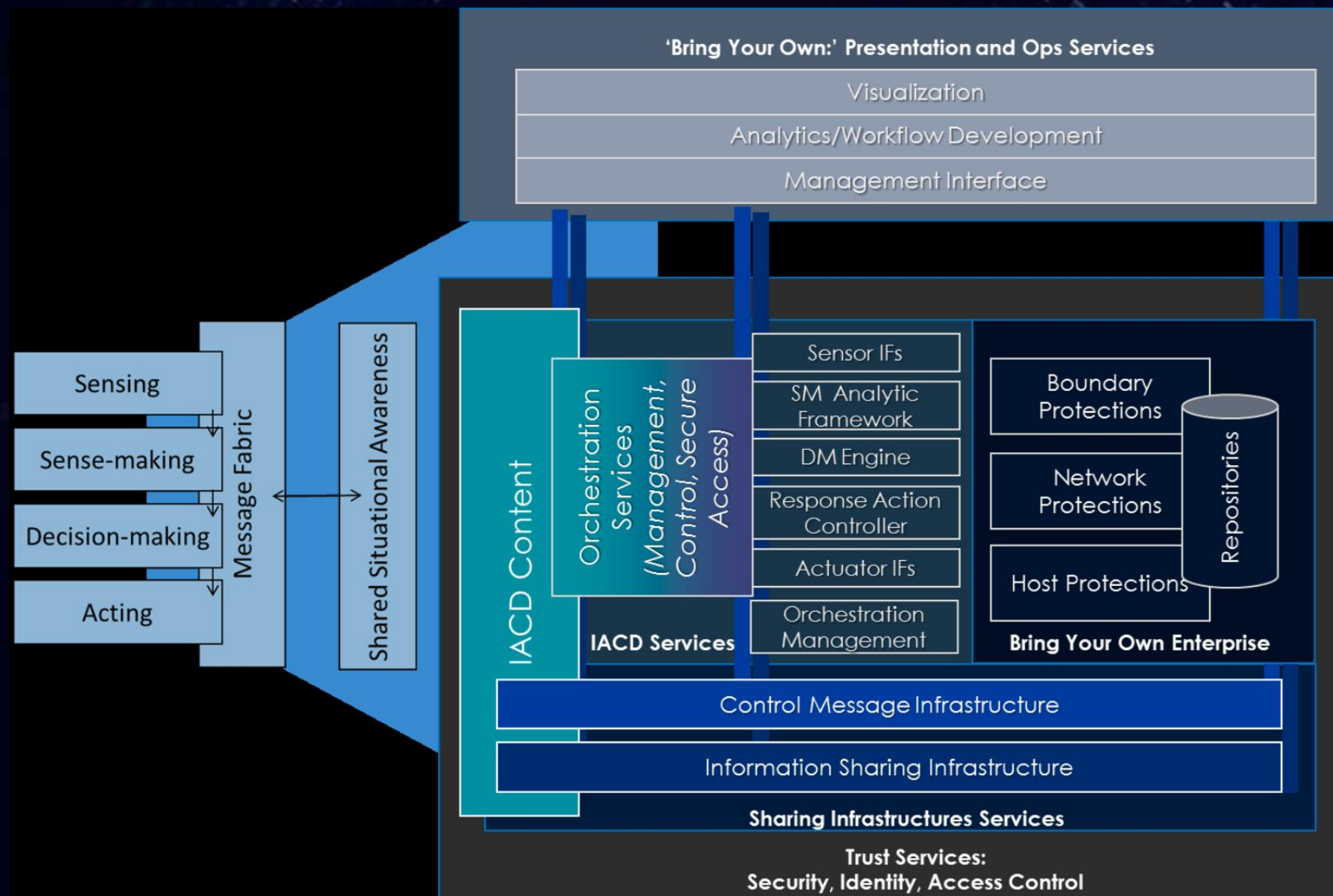
# 基于威胁情报技术构建安全和弹性网络生态



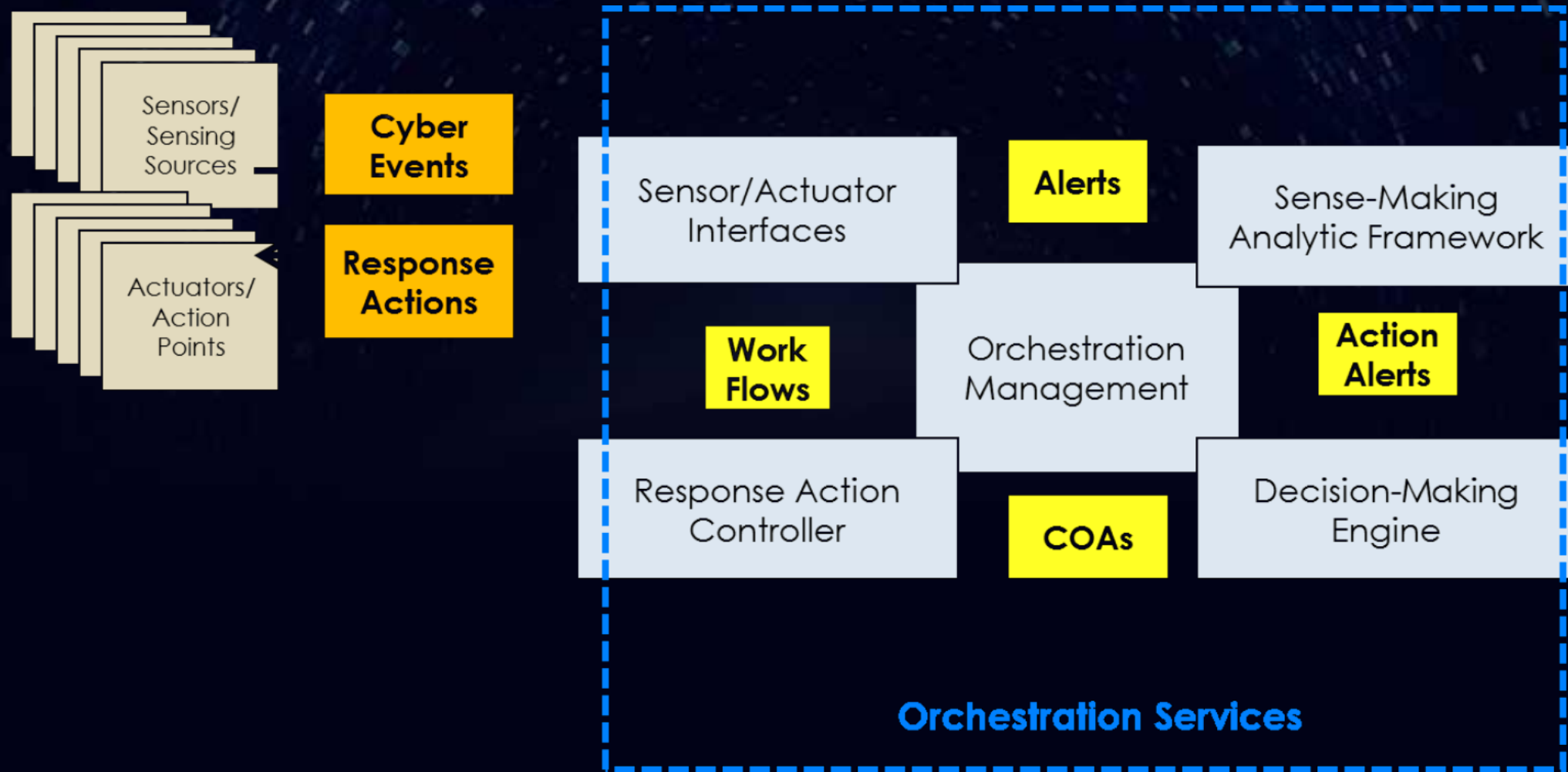
*DHS Secure and Resilient Cyber Ecosystem Example Architecture*



# 集成的自适应网络安全防护框架 IACD

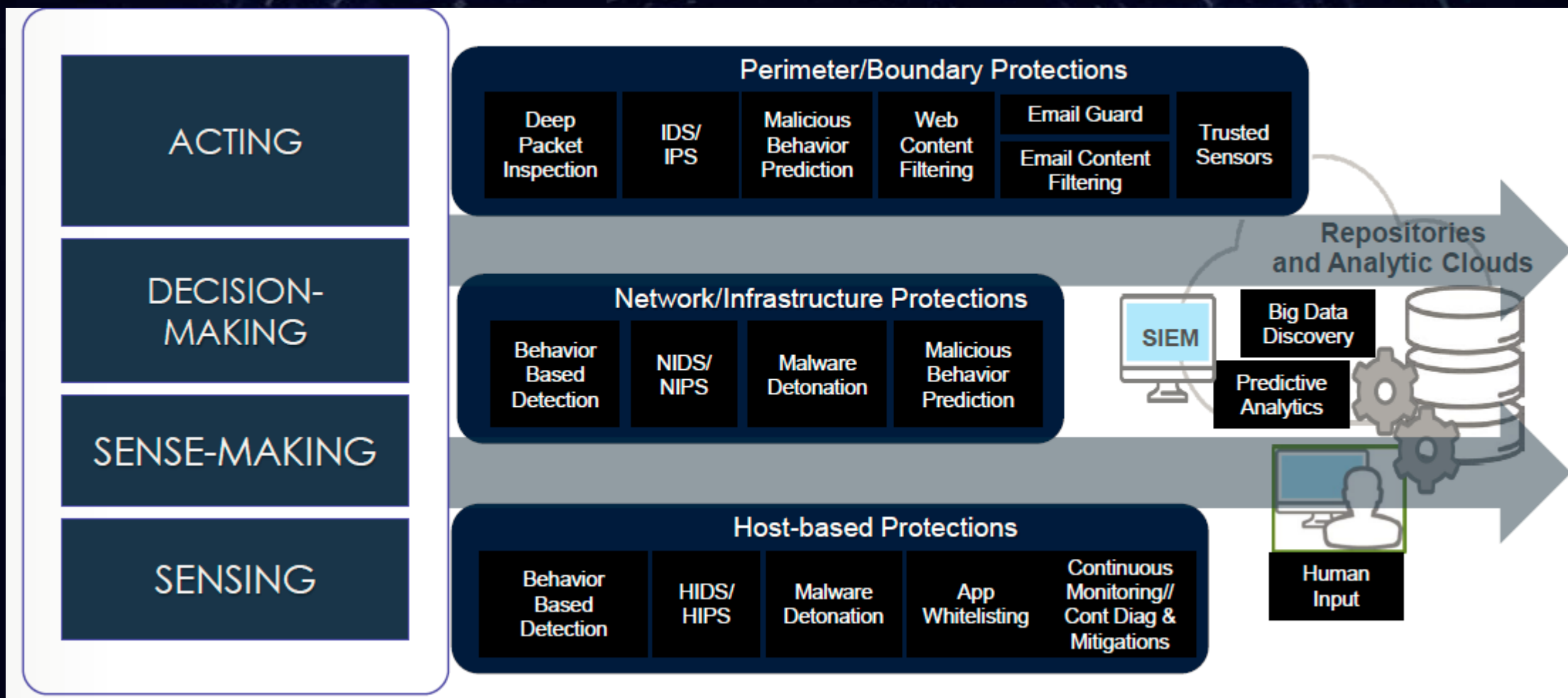


# 基于OODA的体系化自动化处置响应





# 进一步将促进整个安全防护体系的升级



*Integrated Adaptive Cyber Defense (IACD)*



Operator Services



IACD Content/ Data Svcs



IACD Svcs/ Secure Orchestration



Cyber Defenses



Control Msg

Sharing Infrastructure



Info Sharing



谢谢！