

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024

人工智能大模型对网络安全行业的影响

谭晓生





可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024

老谭带你逛逛

RSAC 2024

Genians

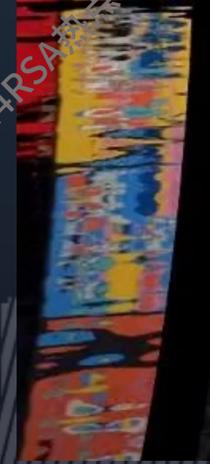
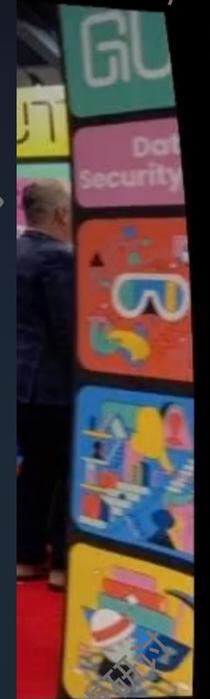
ZTNA
ZERO TRUST NETWORK ACCESS
Pain in the NAC?

zenity

zenity

zenity

zenity



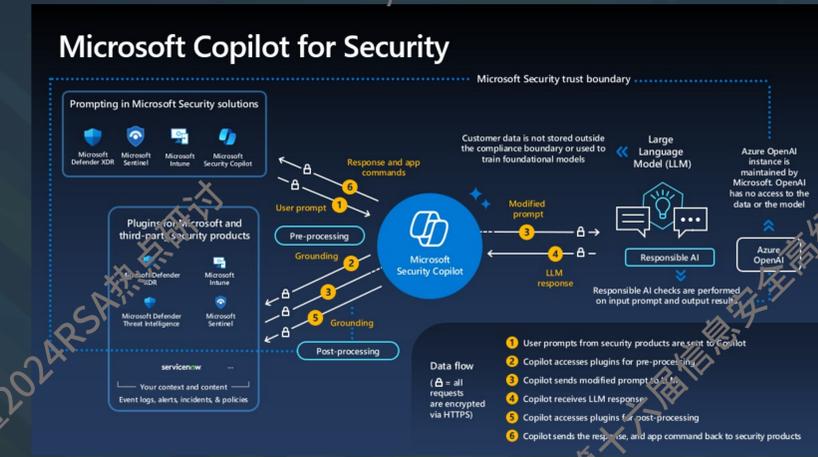
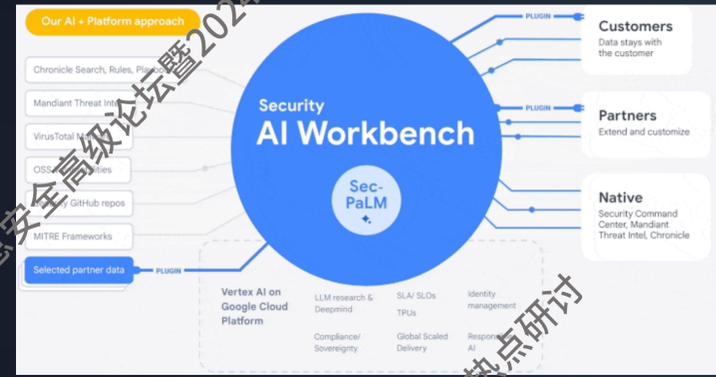


大厂纷纷推出AI赋能的网络安全产品和服务

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024

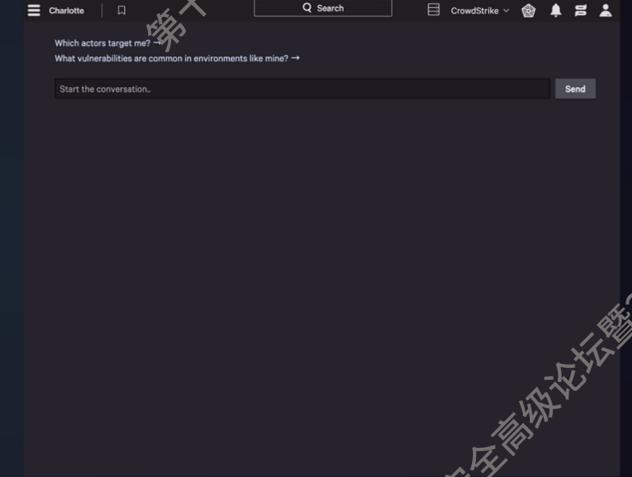


I need to update our firewall policy. What policies are controlling access to SalesAPP?

Here are the policies controlling access to SalesApp

Access Control Policy	Status	Last Modified
Application_Access	Targeting 4 devices	2023-11-10 08:16:14 Modified by "Firepower System"
Edge_Control_Application	Targeting 3 devices	2023-12-09 12:10:26 Modified by "Firepower System"

Ask the AI Assistant a question





无处不在的AI

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024



Making Secure Networking Smarter – one AI

<p>Contextual Gen AI</p> <p>Generative AI to improve product optimization</p> <p>FortiManager FortiAnalyzer</p>	<p>Big Data AI</p> <p>Process and analyze trillions of events using AI/ML</p> <p>FortiGuard</p>	<p>Network Operations AI</p> <p>Self-healing networks end-to-end</p> <p>FortiAIops</p>	<p>AI for LLM Leakage</p> <p>Protection against data leakage into LLM</p> <p>FortiCASB</p>
--	--	---	---

© Fortinet Inc. All Rights Reserved

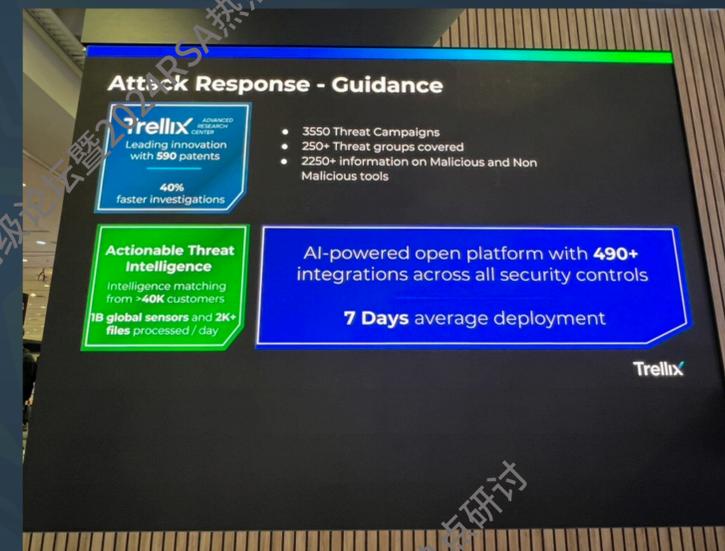
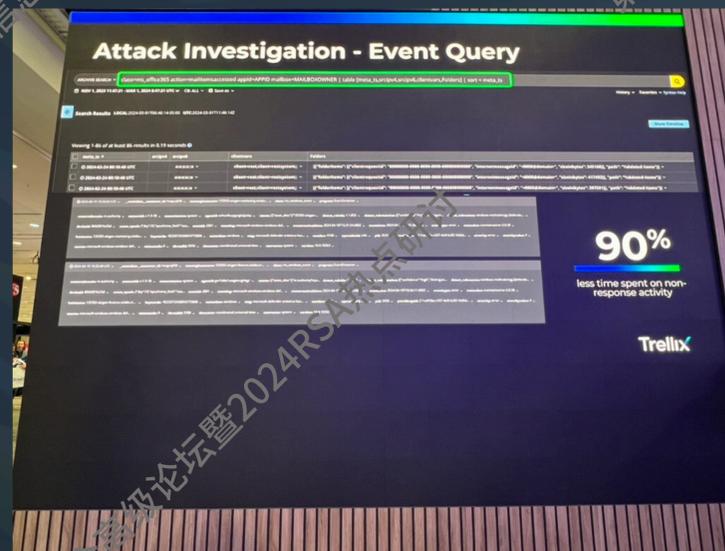
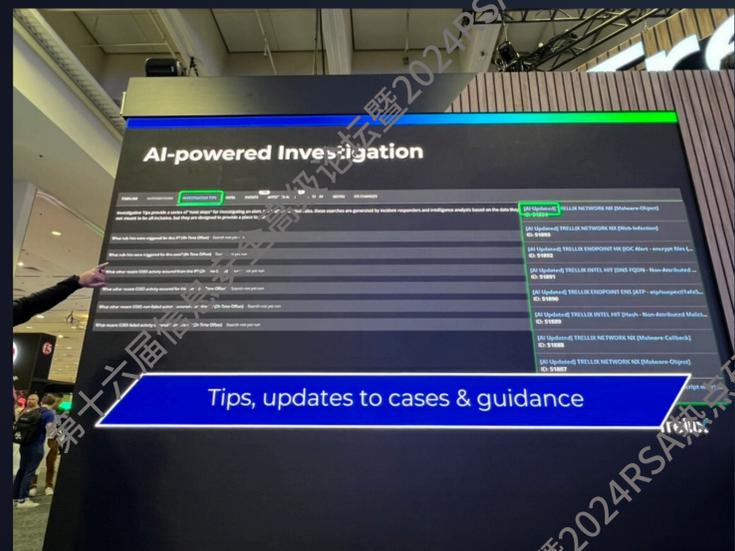


Trellix拥抱AI

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024





创新沙盒10强中的Dropzone AI

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024

System integrations

ALL SIEM THREAT-INTEL ACTIVE DIRECTORY SANDBOX

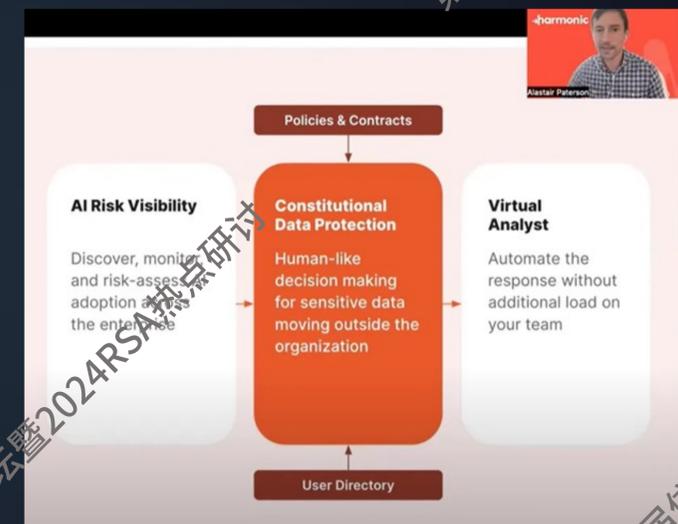
IDS View data inside Cisco Connect >	IDS View data inside SNORT Connect >	SIEM View data inside QRadar Connect >	SIEM Connected View data inside Splunk Configure Disconnect
FIREWALL View data inside Cisco Connect >	FIREWALL View data inside Palo Alto Connect >	ACTIVE DIRECTORY Connected View data inside LDAP Configure Disconnect	CMDB View data inside ServiceNow Connect >
CMDB View data inside Solarwinds Connect >	VULNERABILITY View data inside Qualys Connect >	VULNERABILITY View data inside Tenable Connect >	WAF View data inside F5 Connect >
WAF View data inside Cisco Connect >			

AI Analyst Chatbot

Ask a question



对AI的防护





人工智能大模型在网络安全领域的应用

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024



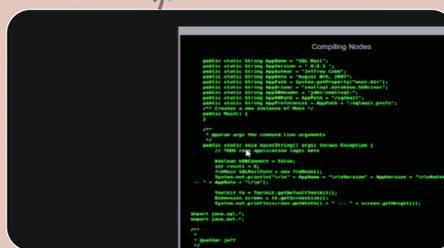
威胁检测

- 恶意代码检测
- 攻击流量检测
- 加密流量检测
- 钓鱼检测



安全运营助手

- 事件总结
- 调查分析
- 辅助决策
- 报告生成
- 安全策略管理
- 自然语言交互



开发助手

- 程序补齐
- 程序漏洞发现
- 漏洞挖掘
- 漏洞修复建议



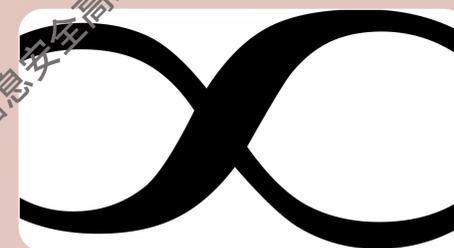
数据安全

- 数据分类分级
- 数据脱敏
- 数据防泄露



邮件安全

- 钓鱼邮件识别
- 垃圾邮件识别



其它

- 防火墙策略管控
- 网络安全策略管控
- 身份管理与访问控制

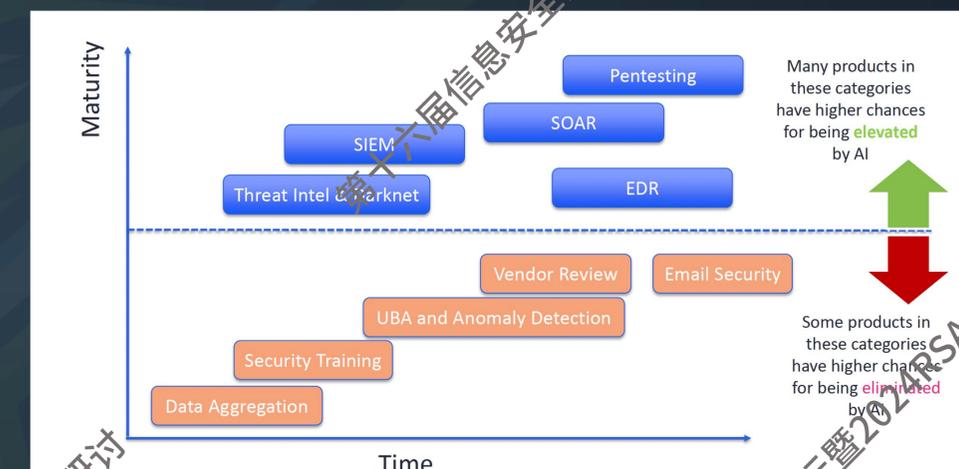


哪些产品会被AI消灭，哪些产品会得到提升？

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024





RSAC上的中国公司

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024





几点感受



- 中美之间网络安全生态差异性进一步变大
- 零信任在美国依然有一定声音
- 未来的网络安全运营平台：SIEM、SOC、XDR？
- 数据安全声音没有国内大
- 物联网安全/ICS安全有声音，但不如国内大
- 邮件安全还是有相当的声音
- 合规管理有一定的声音

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024



感谢聆听!

可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024

