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

AI风暴：新时代下的安全趋势

张烨博士　山石网科副总裁 新技术研究院院长

热门趋势

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

- 无处不在的人工智能
- 威胁检测和响应
- 数据安全

Innovation Sandbox

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

aembit
面向IAM的云工作负载安全平台

ANTIMATTER
GenAI 数据安全

BEDROCK SECURITY
保护云上和GenAI的数据安全

Dropzone AI
AI SOC 分析专家

harmonic
GenAI 数据安全

MITIGA
云和 SaaS的事件调查响应专家

POSECURITY
ACCESS IS OUR PRIORITY ZERO
云上访问治理

RAD SECURITY
基于行为的云原生威胁检测和响应

Reality Defender
深度伪造威胁检测

VulnCheck
漏洞利用和漏洞情报解决方案

AI/GenAI 是如今的流行词

AI 助手

Microsoft Copilot for Security
FortiAI
Infinity AI Copilot
CrowdStrike Charlotte AI
Sentinel Purple One
Cisco AI for Security
Tenable AI Assistant
Elastic AI Assistant
Exabeam Copilot
...

AI赋能

Fortinet AI-driven Everything
AI-Powered Infinity Platform
CrowdStrike AI Powered XDR
VersaAI
Google SecOps
AI powered Email Security
...

保护AI

Google Model Armor
IBM X-Force Red
Cranium
Adaptive Shield
Netskope Skope AI
...

全方位的数据安全

SASE、端点安全、SaaS安全、云安全厂商都在强调数据安全的重要性

GenAI 的数据安全

- Antimatter, Bedrock, Harmonic Security

DLP (包括LLM赋能的DLP)

- Netskope, Versa, Dop.security, Trellix, etc.
- Exabeam: DLP with UEBA

数据安全态势管理 (DSPM)

- Cisco, Crowdstrike Falcon Data Protection,

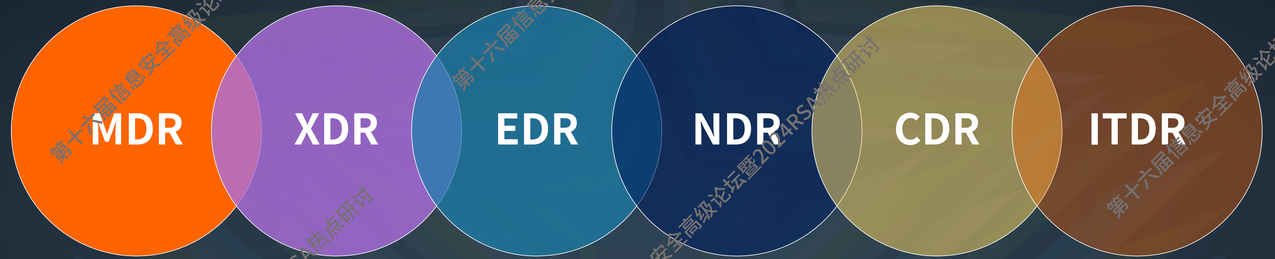
数据清理室

- Immmvault

代码

- Code42

全方面的数据支持威胁检测与响应



- 通过提供**全面的**安全解决方案来保护大型企业的网络安全
- **丰富的遥测方法:** XDR通过收集和分析企业基础设施不同部分的数据提供集中的针对威胁的可见性，包括网络数据、终端数据和云环境中的数据
- 由**AI驱动**，威胁检测和响应提高了响应效率，获得更高水平的检测质量。

AI 无处不在

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

在这个人工智能的数字时代，安全厂商正站在AI与安全相互融合的十字路口

1 GenAI引发了一场全新的科技革命

2 GenAI引入了一类全新的服务业务

3 守护数字世界安全的初心不变

AI技术革命：安全技术发展的新引擎

高效的安全运营：

- 高效的文字处理，信息归纳能力
- 快速响应安全事件，优化安全策略
- 提升自动化运营水平

精准的安全防护：

- 详尽学习记忆已知威胁：异常行为，威胁检测，情报分析等
- 快速应对新型威胁和攻击
- 提升安全效果

AI 安全助手

Microsoft Copilot for Security
FortiAI
Infinity AI Copilot
CrowdStrike Charlotte AI
Sentinel Purple One
Cisco AI for Security
Tenable AI Assistant
Elastic AI Assistant
Exabeam Copilot
...

AI赋能安全平台

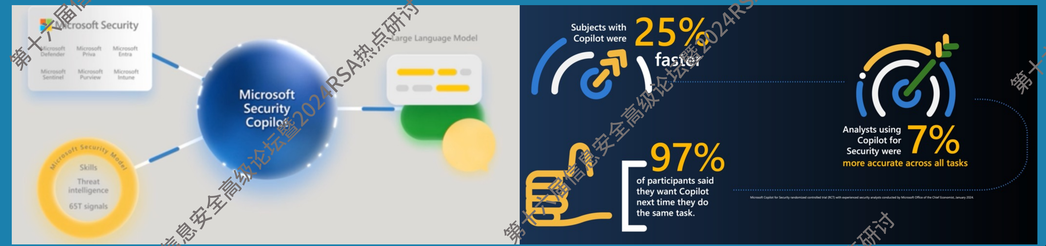
Fortinet AI-driven Everything
AI-Powered Infinity Platform
CrowdStrike AI Powered XDR
VersaAI
Google SecOps
AI powered Email Security
...

AI赋能安全运营

微软安全Copilot

独立式：更广泛的数据来源汇聚于一处，提供丰富的跨产品安全运营指导。

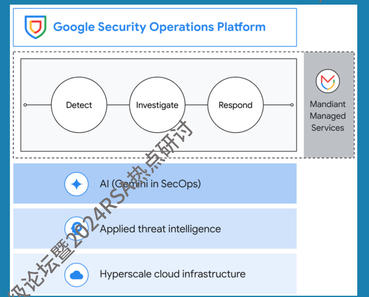
嵌入式：在安全单品产中自然地获取 Copilot 的辅助运营体验。

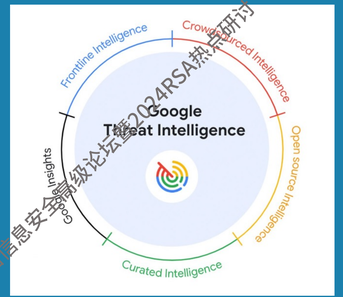


谷歌安全运营平台

智能和AI驱动的安全运营平台：实时监控和警报，自动化响应

Gemini 1.5：最长上下文窗口，包含100万个标记





AI赋能新的安全检测技术

RSAC™ Innovation Sandbox 2024 WINNER

Reality Defender

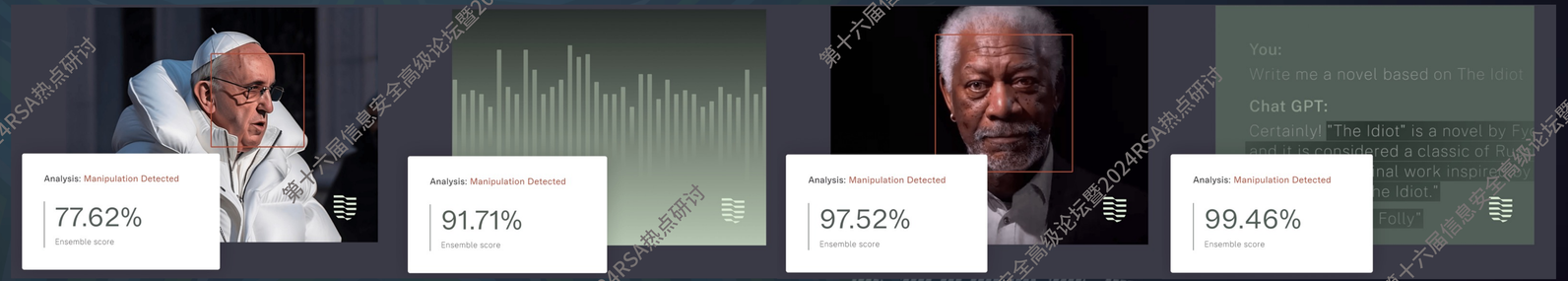
可 能 的 艺 术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛
美国2024RSA参会热点研讨
INFORMATION SECURITY FORUM 2024

利用人工智能来检测人工智能生成的威胁

愿景：成为所有人工智能生成欺诈的检测层

- 一种革命性的多模型方法
- 涵盖：图像/音频/视频/文本
- 常见的人工智能威胁：
  - 语音克隆、身份盗窃、人脸替换人工智能
- 与网络应用程序和API的无缝集成



AI业务安全挑战：护航AI服务的新责任

守护用户安全使用GenAI服务

- 数据隐私保护
- 保证数据合规性和监管要求
- 防止GenAI过度幻想或不准确、非法、侵犯版权的输出，影响决策制定

保护AI大模型

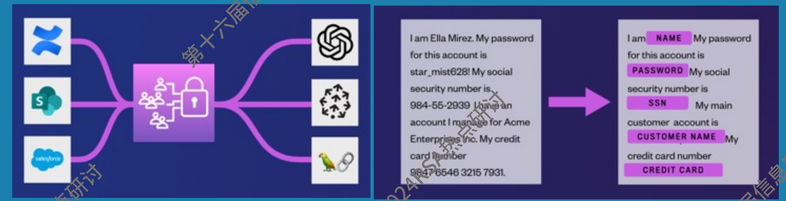
- 保护AI模型免受攻击和滥用
- 预防GenAI供应链漏洞
- 防止黑客对模型的盗窃

安全使用AI：保护数据隐私

RSAC Innovation Sandbox 2024 FINALIST

ANTIMATTER

数据访问控制　数据匿名化
数据分类　数据加密
日志计划
数据清单



harmonic

Usage and Adoption
Track employee usage, top use cases, and data flows.

GenAI Supply Chain
Identify risky GenAI apps training on your data.

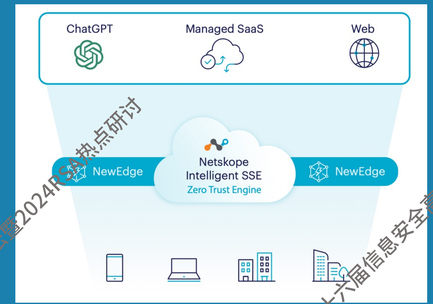
Detect Sensitive Data
Human-like review of any sensitive data leaving the business.

Coach Users
Inline training and nudging of users towards safe AI Use.

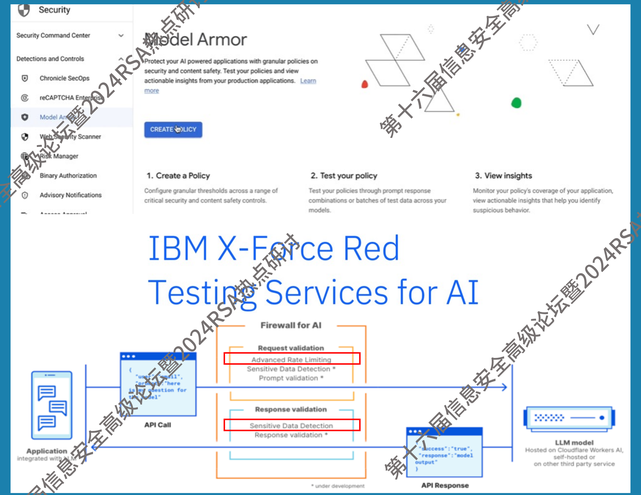
Netskope SkopeAI

SkopeAI Data Protection
SkopeAI employs the industry's only ML-Based cloud DLP solution that identifies new data and protects it in real-time.

Keep GenAI and SaaS Safely Under Control
Netskope industry-leading CASB is the only solution that delivers ML-based risk categorization of new cloud apps, discerns app instances and enables secure utilization of generative AI.



保护AI模型：针对大模型的新型攻击



谷歌 Model Armor

- 使客户能够检查、路由和保护基础模型的提示和响应。
- 减轻风险，如提示注入、越狱、有害内容和敏感数据泄露。

IBM X-Force Red: AI模型的渗透测试

- 发现并解决 FM/LLMs、MLSecOps 管道、AI 平台和 GenAI 应用程序中的安全漏洞。

Cloudflare AI Firewall

- 为使用LLMs的应用程序量身定制的高级WAF。

人工智能时代下的网络安全

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

在人工智能时代，网络安全迎来新纪元

- 通过充分利用AI（传统ML和GenAI）优势，更高效地发现、分析和应对各种安全威胁

- 不能忽视由新型人工智能服务、新型AI应用引发的安全防护需求

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