



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

效率制胜 - 从RSAC2024看后云时代国际网络安全趋势

赵粮

2024.06.07





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

RS(AI)C

AI-driven | AI-powered | AI-native

DON'T JUST ASK, ACT! 不能光问，还要能行动!



RSA大会期间，PANW高调发布其AI产品，包括三个CoPilots，以及在线保护能力Inline AI Protection

<https://www.crn.com/news/ai/2024/palo-alto-networks-to-change-how-cybersecurity-is-done-with-ai-launch-cpo-lee-klarich?itc=refresh>



Copilot
by Palo Alto Networks

You

Am I vulnerable to XZ utils?

Prisma Cloud Copilot

Explore

Recent Chats

Favorite Prompts



Summary:

The graph shows that the vulnerability "CVE-2024-3094" was introduced in the code and then propagated to production. As a result, 45 assets are now running with the vulnerability in production. The vulnerability has a CVSS score of 10 (critical). It is also exploitable and not patchable.

Critical Risk:

The most important risk to address is "CVE-2024-3094". This vulnerability has a CVSS score of 10.0, is exploitable, and not patchable. This means that attackers can easily exploit this vulnerability to gain control of affected systems.

Exploitation Steps:

Attacker can exploit vulnerability in the Malicious code that was discovered in the upstream tarballs of xz, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that can be used by any software linked against this library, intercepting and modifying the data interaction with this library.

Here are some next steps you can take

- View impacted assets
- Submit pull request
- Open a JIRA ticket
- Export CSV
- Suppress

Enter a prompt here

Copilot
by Palo Alto Networks

You

what is the blast radius?

Prisma Cloud Copilot

Explore

Recent Chats

Favorite Prompts

This is the Blast Radius for vulnerability "CVE-2024-3094".



- Explain this threat
- Explain this graph
- More quick responses

Enter a prompt here

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

what can you tell me about incident ID-2124?

"ID-2124" is a Security Incident

★ **H** **77** Process Injection involving 2 users generated by XDR Age...

STATUS *Open 4 months*
Under Investigation

ASSIGNED
Gil Blum

AUTOMATION
4 2 1

KEY ASSETS & ARTIFACTS
3 2 3

Show me more

INVESTIGATE

View incidents with the shared artifacts [Generate](#)

RESPOND

Run recommended playbooks

Change incident status to resolved

NAVIGATE

Ask the Help Center

Incident Response > Incidents

- ▶ "which incident should I work on first?" Tue 12 Dec 17:32
- ▼ "what can you tell me about incident ID-2124?" Tue 12 Dec 17:41

Run recommended Playbooks

Available playbooks to best remediate Incident ID 2124:

XSIAM Marketplace (4)

H Malicious Powershell (Alert ID: 2527)

T1059 - Command and Scripting Interpreter

This playbook handles command and scripting interpreter alerts based on the MITRE T1059 technique. An attacker might abuse command and script...

[Read more](#)

H Suspicious Disk Modification (Alert ID 27524)

T1062 - Ransomware Response

This playbook handles ransomware alerts based on the Cortex XDR Traps module signature 'Suspicious File Modification'

[Read more](#)

Copilot

by Palo Alto Networks

Explore >>

Recent Chats

Favorite Prompts

You

Yes, create a new support case

Prisma Cloud Copilot

Case creation initiated

Review and complete the fields below before you proceed:

Email

admin@email.com

Phone

+1 (415)

Category

Select

Severity

Select

Last Occurrence (Optional)

Select

Issue Concentration

Select

Is your product down?

Select

How many users is it affecting?

Select

Lorem ipsum dolor sit amet? (Optional)

Select

Upload File (Optional)

Drag and drop file here or

Browse File

Screen Capture (Optional)

Start recording and then reproduce your issue

Start Recording

Supported formats: MP4, MOV, AVI

Maximum size: 25MB

Recorded sessions will capture your current active tab
Duration limit: 10 minutes

Confirm

Cancel

Enter a prompt here



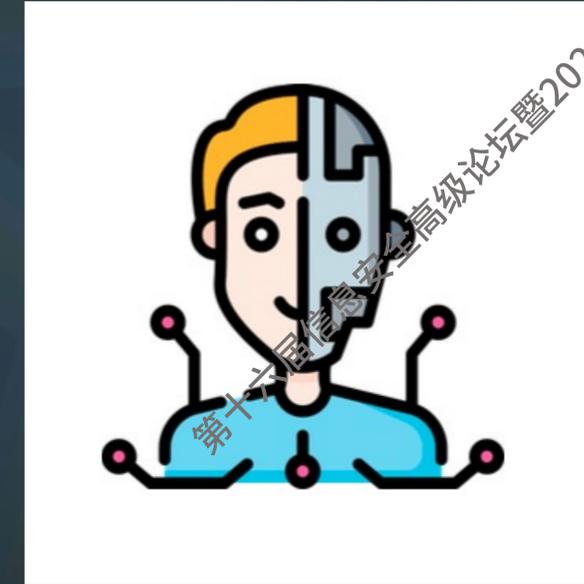
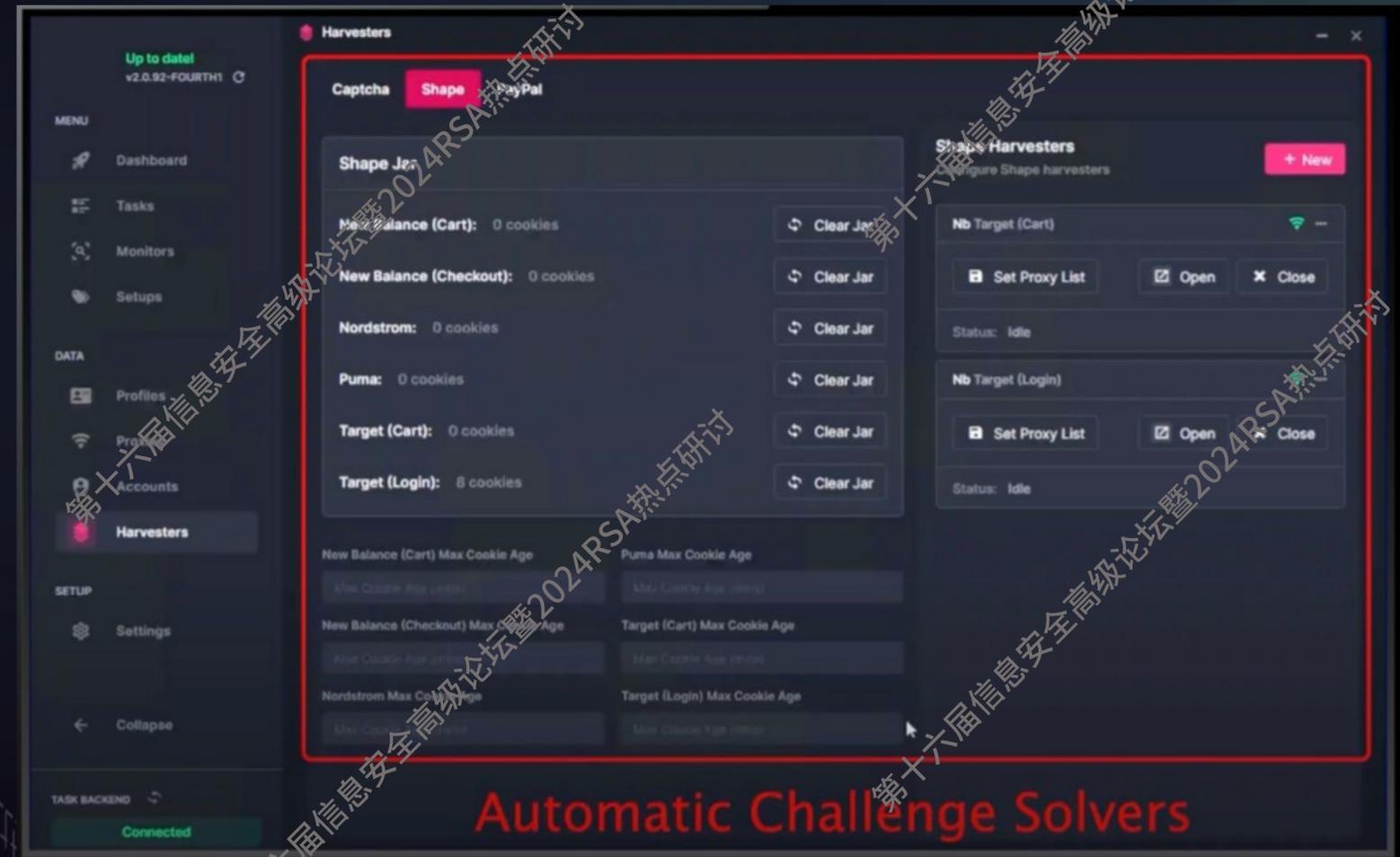


AI Agent的进攻

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



- Creatively accomplish tasks based on simple prompts | 基于简洁指令，创造性地完成任任务
- Flawlessly manage identity data, proxies, payment methods, and devices | 无缝管理身份数据、代理、支付方式和设备
- Navigate real UX using taps, clicks, and keystrokes | 运用点击、轻触和按键操作真实的 UX

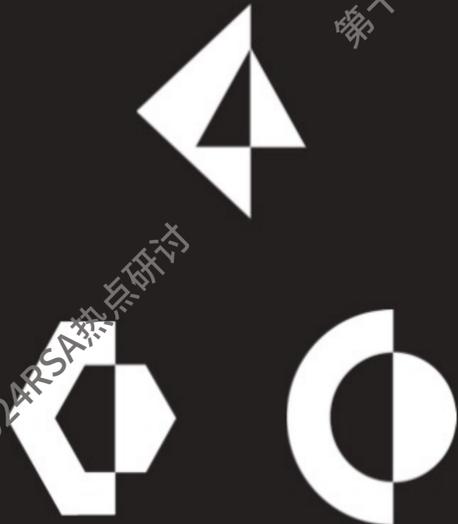
We delivered a milestone moment around AI Security, addressing a ~\$15B TAM¹

TAM¹

Announced solutions to secure AI by design

- AI Access**: Enable **Safe AI Adoption** to Employees
- AI SPM**: Ensure **secure configuration and deployment** of AI Apps
- AI Runtime**: Security to **Protect Apps, Models, and Data**

Delivered co-pilots² across all three platforms



Announced the Precision AITM Security Bundle

Leverage **inline AI** to counter AI attacks with **AI Defense**

New Adv Sub



Advanced DNS Security



Advanced URL Filtering



Advanced Threat Prevention



Advanced Wildfire

Focused Execution Against Top-Line Targets

NGS ARR¹

\$3.79B

+47% y/y

Remaining Performance Obligation

\$11.3B

+23% y/y

Total Revenue

\$1.98B

+15% y/y

Total Billings²

\$2.33B

+3% y/y

9th consecutive quarter of operating margin expansion

Operating Income (non-GAAP)

\$508M

+25% y/y

Operating Margin (non-GAAP)

25.6%

+200 bps y/y

Adj. Free Cash Flow (non-GAAP)

\$492M

+\$256M y/y on trailing 12-month basis

EPS (non-GAAP)

\$1.32

+20% y/y

¹ Internal Estimates.

² Private view available to customers.

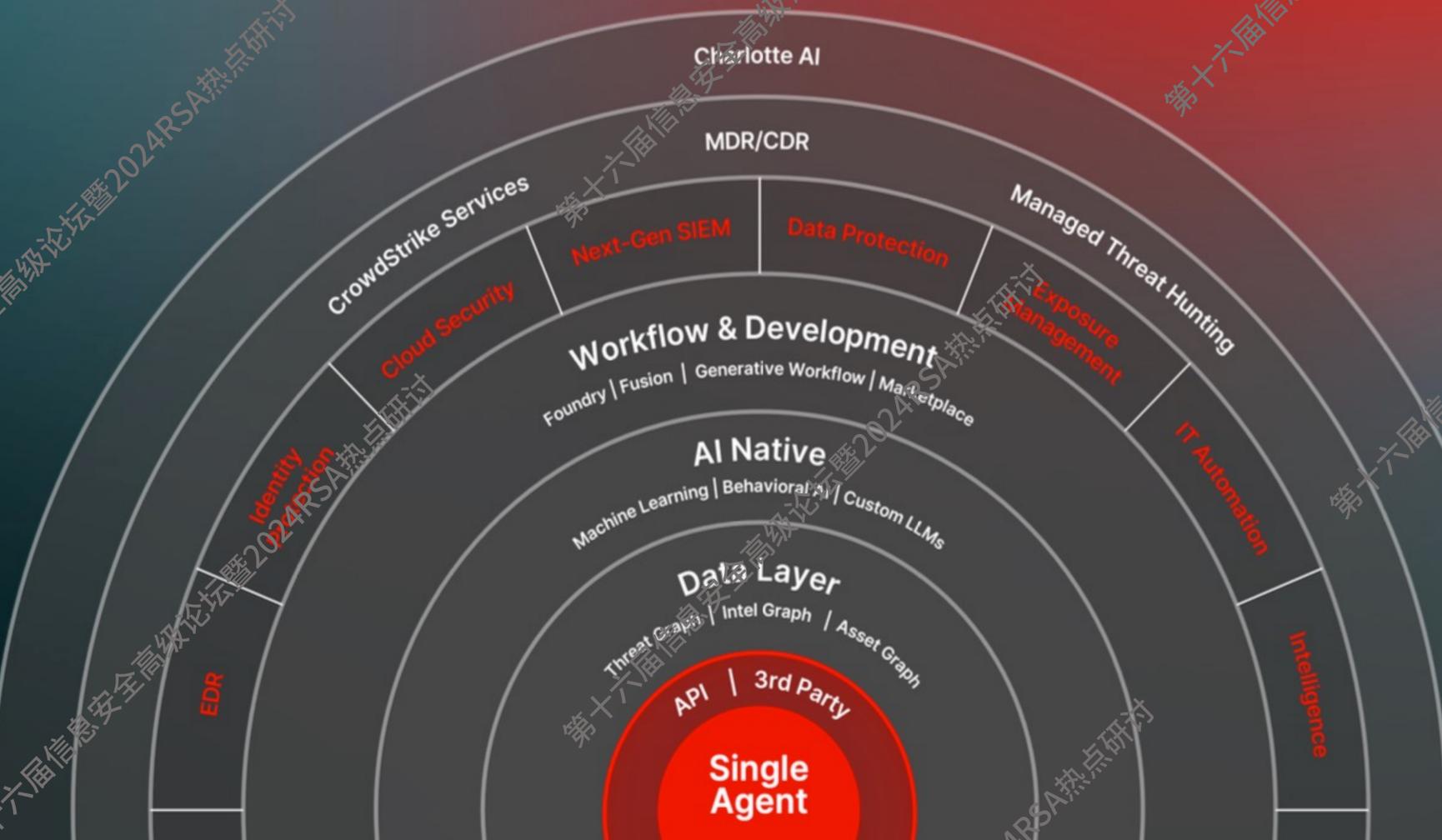
可能的艺术
THE ART OF THE POSSIBLE

第16届信息安全高级论坛

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

Our AI-Native XDR Platform Creates Opportunity

- ✔ Lightweight
- ✔ Cloud-First
- ✔ AI-Native
- ❌ Hardware
- ❌ Data Silos
- ❌ Friction



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

1 Strong Financial Performance

\$3.65B
Ending ARR
+33% Y/Y

\$212M
Net New ARR
+22% Y/Y

- ✔ Record subscription gross margin, >80%
- ✔ Record free cash flow, 35% of revenue
- ✔ Delivered significant YoY operating leverage
- ✔ Fifth consecutive quarter of GAAP profitability

2 Driving Platform Adoption

Landing with **more modules** + than ever before

of deals involving cloud, identity, or next-gen SIEM **more than doubled**

Cloud security provider of choice for **62 of Fortune 100**

3 Security Consolidator of Choice

Platform Built for Consolidation

- ✔ Single agent
- ✔ Single AI-native platform
- ✔ Frictionless vendor consolidation
- ✔ Immediate time-to-value

Record Module Adoption

- ✔ Percent of customers with 5+, 6+ & 7+ modules **increased**
- ✔ Deals with 8+ modules grew **95% YoY**

CHIEF AI OFFICER EXCHANGE USA

May 01-02, 2024
Fort Lauderdale, Florida

THE ROLE OF A CHIEF AI OFFICER

The role of Chief AI Officer is a relatively new one, so we asked C-Suite level peers to give some insight into what this new role entails, its importance and its potential place within the industry.

C.A.I.O

Chief A.I. Officer

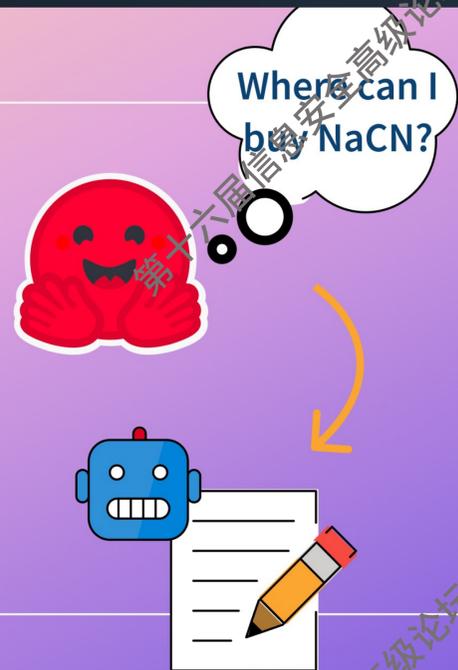
可能的艺术

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

Red-Teaming Large Language Models



Prompt:

GenAI Red Teaming:
Uncover GenAI risks
and vulnerabilities
in your LLM-based
applications



Workshop on GenAI in Healthcare: Red Teaming

Open to all Students, Postdocs, and Faculty

What is Red Teaming?

This will be an interactive session to test GenAI models for potential issues with biases, inaccuracies, and more as related to healthcare.

OCT 25, 2023 | 3:00 - 6:00 PM
CHEM-H BUILDING | ROOM E241

3:00-4:45 PM: Red Team Challenge
4:45-6:00 PM: Happy Hour

SPACE LIMITED.
REGISTER TODAY!
[TINYURL.COM/
GENAIREDTEAMING](https://tinyurl.com/genairedteaming)



CSRB



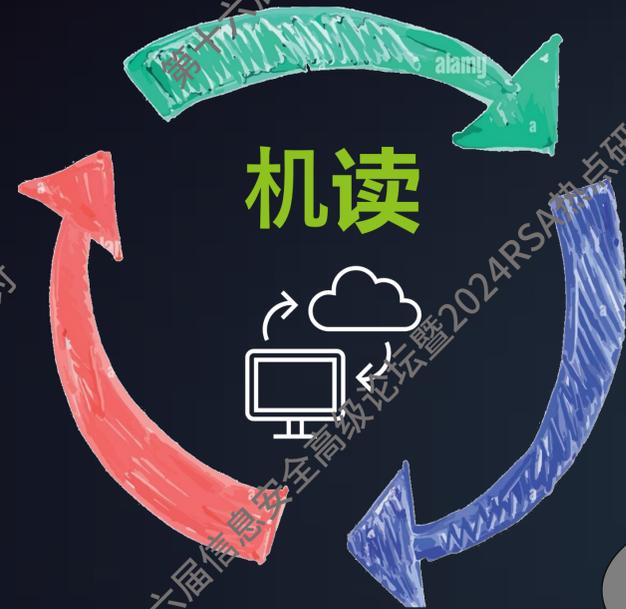
**CYBER SAFETY
REVIEW BOARD**

- 美国国土安全部将成立一个名为关键基础设施安全委员会（CSRB）的独特论坛，该论坛将促进政府和私营部门领导人之间的合作，为总统和国土安全部部长提供战略建议。
- CSRB 由来自联邦政府和私营部门的 15 位备受尊敬的网络安全领导人组成。国土安全部政策副部长 Robert Silvers 将担任主席，谷歌安全工程高级总监 Heather Adkins 将担任副主席。国土安全部网络安全和基础设施安全局（CISA）将负责管理、支持和资助该委员会，CISA 局长 Jen Easterly 负责任命 CSRB 成员（需与国土安全部政策副部长 Rob Silvers 协商），并在重大网络安全事件后召集委员会召开会议。



Review of the Summer 2023 Microsoft Exchange Online Intrusion

March 20, 2024
Cyber Safety Review Board



机读



WHEN YOU DEFINE
IT, I CAN LEARN IT!

请问UC&A里的
B怎么说?

请说IoB
Indicator of Behavior

云地人机的正确姿势

- ❑ 24x7
- ❑ L1/L2/L3
- ❑ Handbook/Script
- ❑ 逆向分析员
- ❑ 数据分析员
- ❑ ...

云
Cloud

- ❑ 用户门户/运维门户
- ❑ 信誉云
- ❑ 各种安全能力集群
- ❑ 弹性计算和存储集群
- ❑ ...

人
Expert

机
Device

地
Local/Campus

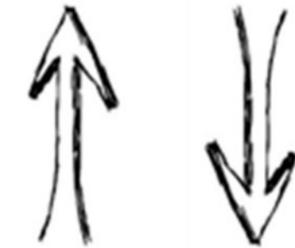
- ❑ 24x7 Standby w 移动App
- ❑ L1/L2
- ❑ Handbook/Script
- ❑ ...

- ❑ BSA分析平台
- ❑ ESPC (with App support)
- ❑ NF/IDS/IPS/WAF/ADS/...
- ❑ ...

云地重构

人机重构

南下北上





“快、全、省”不可能三角

- ❖ 首先是“connect to protect”，将更多运营作业转移到线上以提高效率；
- ❖ 其次是集中和规模化，通过集中资源和规模效应实现更高效的安全运营；
- ❖ 最后是快速闭环能力，充分利用数据分析和人工智能技术，快速发现、研判和处置威胁和风险，以实现快速闭环的安全运营

	2020	2021	2022	2023
满足40法则的 公司数量	14	15	5	3
“营收增速+归 母净利/收入” 平均值	40.49%	32.09%	3.87%	-2.37%
“营收增速+归 母净利/收入” 中位数	33.75%	39.92%	8.04%	0.73%

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

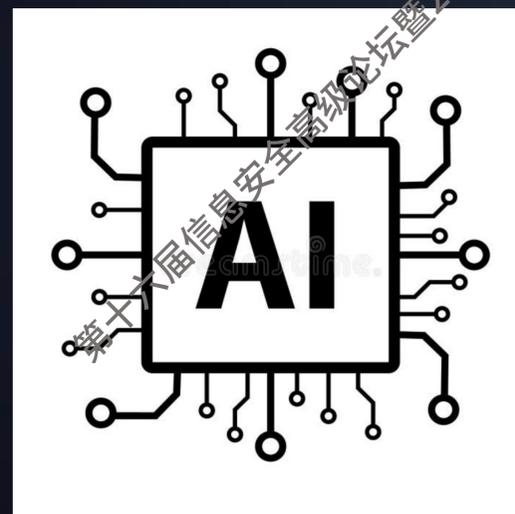


结束语 - 效率制胜

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



(1) AI的大规模应用，(2) AI的安全防护以及(3) 利用AI来提升网络攻防效率是密切相关的三个领域，其中(1)是基石，(2)是保障因素，而(1+2)是(3)的重要基础和放大器



(1) GenAI/大模型很有可能在攻防能力和效率上带来“代差”；(2) GenAI/大模型不是银弹；(3) 有必要梳理识别生态层面影响效率的“堵点”，鼓励（远程 | 线上 | 集中）规模化的安全运营和专业MSSP，在产业政策/法律法规层面提供支撑和保障。



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

