终端安全，最后的战场

One Scorpion

不容忽视的威胁

端点防御技术发展

做负责任的产品

展望

不容忽视的威胁

失掉一场战争的代价

Gulf war

1991

Isreaeli vs Syria

2007

关键信息基础设施面临的风险

- Critical infrastructures are increasingly dependent on information and communication.
- The potential natural disasters or terrorist attacks, which threaten the critical infrastructure and critical information infrastructure as well, are dramatically increasing today.
- Risks to the CIIs include man-made attacks, natural disasters and technical failures.

关键信息基础设施面临的风险

BlackEnergy

2011年以来，一个涉及BlackEnergy的复杂恶意代码网络攻击行为造成许多工业控制系统受损。

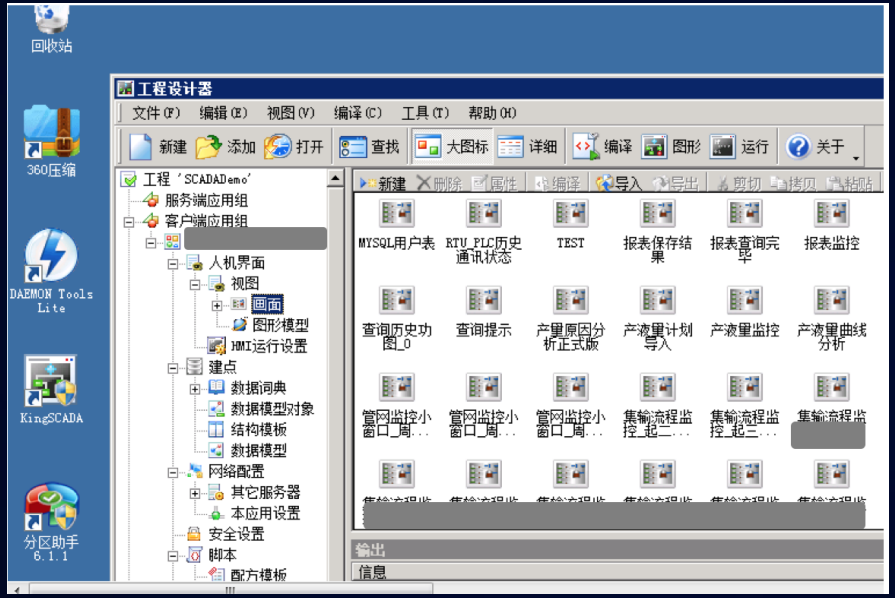
乌克兰停电事件

2015年12月23日，乌克兰电力公司经历计划外的大面积停电，后经分析确认事件由三个远程网络入侵攻击导致。

Havex

Havex木马包括多项针对的ICS功能，其中使用的有效载荷包括发现和收集通过OPC标准进行通信的系统资源。

关键信息基础设施面临的风险



企业面临的威胁

信息泄漏

可用性

恶意代码

5th Era Malware

- First massive cyber-attack against a country, Estonia from Russia.
- Anonymous starts a campaign against several organizations (RIAA, MPAA, SGAE, and others)
- Malware professionalization
- Use of marketing techniques in spam campaigns
- Country/Time based malware variant distribution
- Ransomware
- APTs
- Detection by context
- Apart from analysing what a process does, the context of execution is also taken into account…

端点防御技术发展

HBSS

Host Intrusion Prevention System (HIPS)

Rogue System Detection (RSD)

Policy Auditor (APS)

Asset Publishing Service (APS)

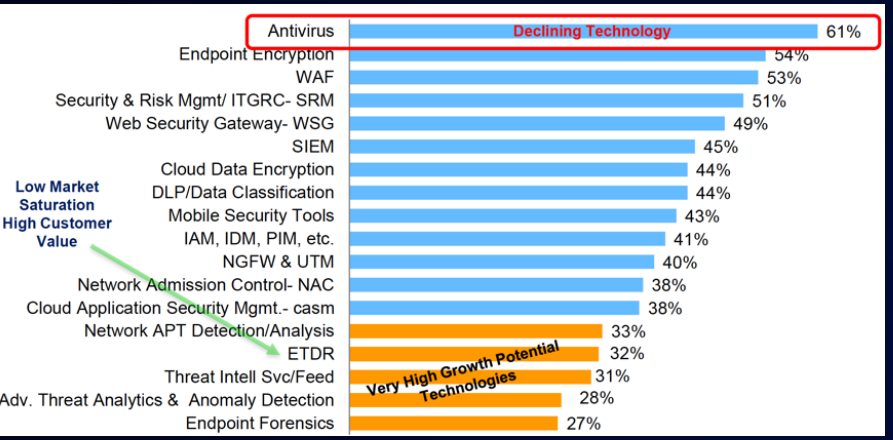
Operational Attributes Module (OAM)

Device Control Module (DCM)

Asset Baseline Module (ABM)

下一代终端安全

The Tools Security is Turning to:



Mean Perceived Value of Technologies(Benefits vs. TCO)

来源：Enterprise Management Associates, Inc.

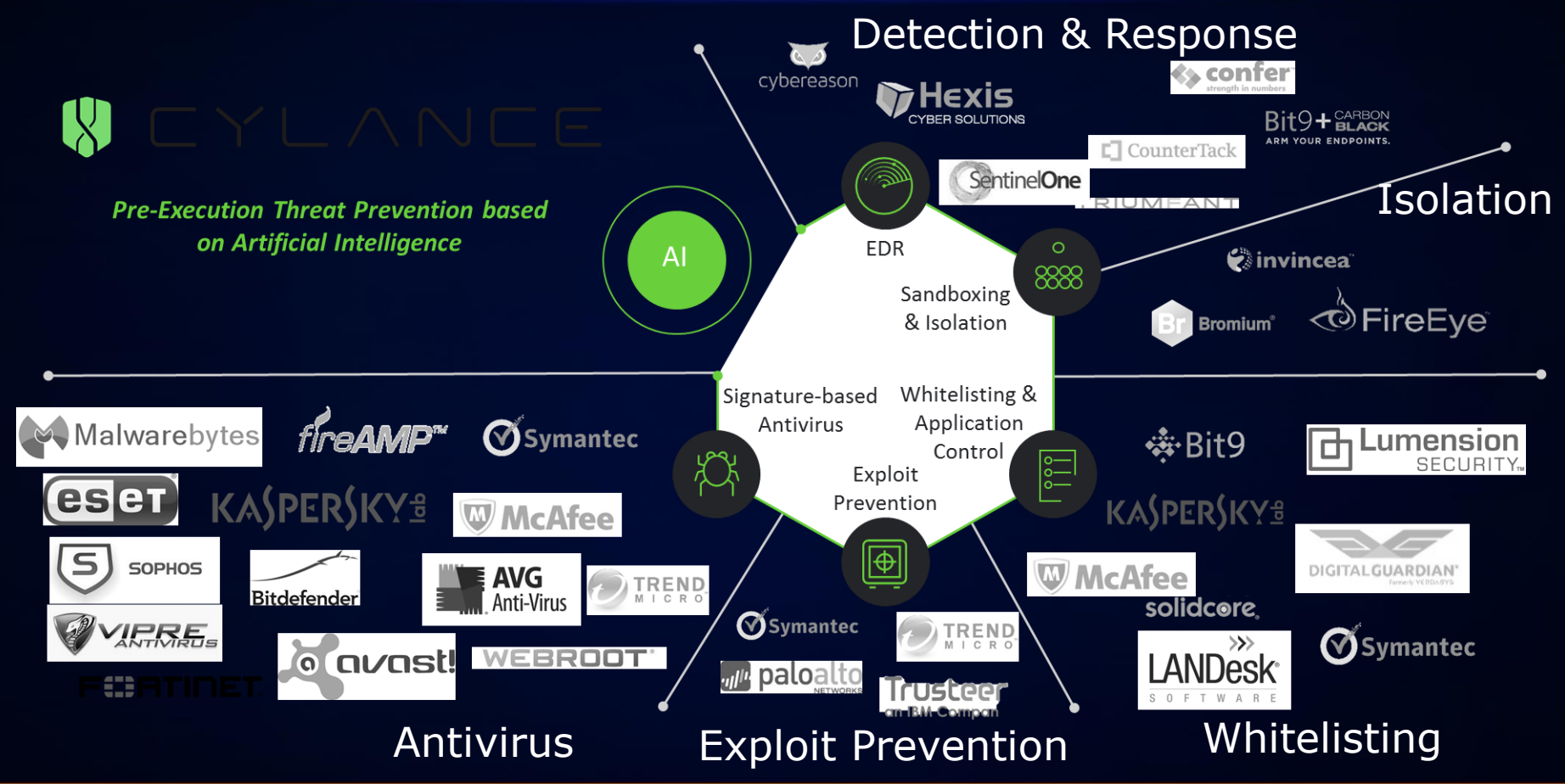
Avecto	CounterTack	Fidelis Cybersecurity	LightCyber	SentinelOne
Carbon Black	CrowdStrike	FireEye HX	Malwarebytes	Sophos
Bromium	Cybereason	Hexis Cyber Solutions	Outlier	Tanium
Cisco	Cylance	IBM Apex	Promisec	Triumfant
Comodo	Deep Instinct	Invincea	RSA ECAT	Ziften

Avast	Intel Security	Symantec
Confer	Kaspersky	Trend Micro
Endgame	Palo Alto Networks	Webroot

2000%

124%

56%


Detection & Response
CYLANCE
Pre-Execution Threat Prevention based on Artificial Intelligence
AI
cybereason
Hexis CYBER SOLUTIONS
confer
Bit9+CARBON BLACK
ARM YOUR ENDPOINTS.
CounterTack
SentinelOne
EDR
Isolation
Sandboxing & Isolation
invincea
Bromium
FireEye
Signature-based Antivirus
Whitelisting & Application Control
Exploit Prevention
Malwarebytes
fireAMP
Symantec
eset
KASPERSKY
McAfee
SOPHOS
Bitdefender
AVG Anti-Virus
TREND MICRO
VIPRE ANTIVIRUS
avast!
WEBROOT
FORTINET
Symantec
TREND MICRO
paloalto NETWORKS
Trusteer
Bit9
Lumension SECURITY
KASPERSKY
McAfee
DIGITAL GUARDIAN
solidcore
Symantec
LANDesk SOFTWARE
Antivirus
Exploit Prevention
Whitelisting

中国终端安全现状一览

认证与接入　　防病毒类　　合规与监管类　　信息防泄漏　　防篡改

中国终端安全现状一览

我们具备防攻击的能力了吗？

中国终端安全现状一览

我们对APT的理解有多少？

中国终端安全现状一览

勒索时代我们真的可以免疫了吗？

做负责任的产品

天蝎硬件威胁监测系统

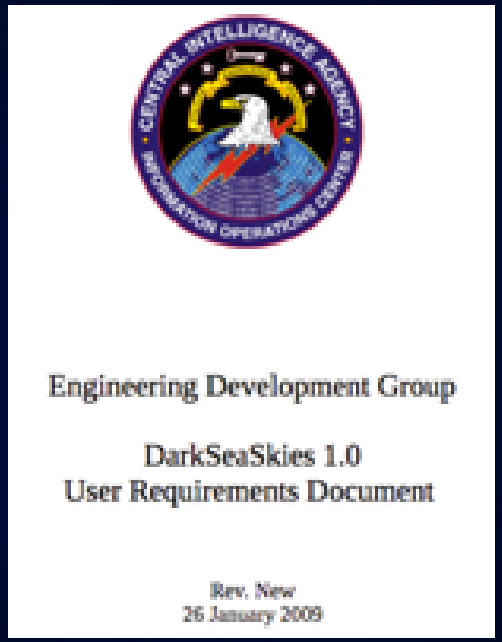
Putting the spotlight on firmware malware

Firmware malware has been a hot topic ever since Snowden's leaks revealed NSA's efforts to infect BIOS firmware. However, BIOS malware is no longer something exclusive to the NSA, Lenovo's Service Engine or Hacking Team's UEFI rootkit are examples of why the security industry should put some focus on this strain of badness.

To all effects BIOS is a firmware which loads into memory at the beginning of the boot process, its code is on a flash memory chip soldered onto the mainboard. Since the BIOS boots a computer and helps load the operating system, by infecting it attackers can deploy malware that survives reboots, system wiping and reinstallations, and since antiviruses are not scanning this layer, the compromise can fly under the radar.

As of today VirusTotal is characterizing in detail firmware images, legit or malicious. These are a couple of examples of the kind of information that is now generated, please refer to the *File Detail* tab:
https://www.virustotal.com/en/file/3afb102f0a61f5a71be4658c3d8d3624e4773e36f64fd68a173f931bc38f651e/analysis/ [1]
https://www.virustotal.com/en/file/4db9177af43a958686b9367f19df90023acf3189c388497a8a7d1d8cb3f7f0e0/analysis/ [2]
https://www.virustotal.com/en/file/57a0c38bf7cf516ee0e870311828dba5069dc6f1b6ad13d1fdff268ed674f823/analysis/
Pay attention to the *Additional information* tab in this other case, you will see a new *Source Details* field which gives attribution information for the given file:
https://www.virustotal.com/en/file/8b1ec36a50683db137d3bd815052dd6034697af8ef2afd6c81c912b6d0f0f2e0/analysis/
100% PE resource match is not required in order to provide some attribution context, e.g.
https://www.virustotal.com/en/file/a90f803e10530e8f941d7054a12a37aa7b22c89bac89b6d2b8e40878bffccf11/analysis/

2016.01



SWAP
Deitybounce

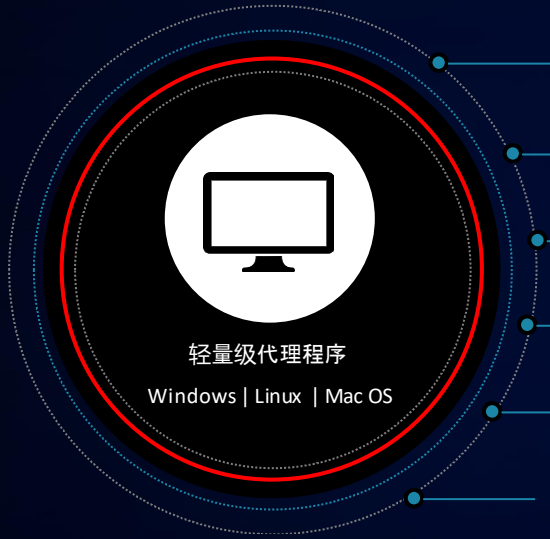
天蝎硬件威胁监测系统

```
[+] Start MBR detecting ...
Current MBR hash : 6DEF5FFCBCDBDB4082F1015625E597BD
Current MBR is same with XP mbr, so MBR is normal.
[*] MBR detection completed. MBR is normal.

[+] Start BIOS detecting ...
BIOS Type      : Legacy
BIOS Version   : 6.0
BIOS Size      : 0x00010000
BIOS Segment   : 0x000E9A50
BIOS Version   : 6.00
BIOS Vendor    : Phoenix Technologies LTD
BIOS Date      : 05/20/2014
BaseBoard Version          : None
BaseBoard Manufacturer     : Intel Corporation
BaseBoard ProductName      : 440BX Desktop Reference Platform
BaseBoard SerialNumber     : None
BaseBoard ChassisLocation  :
BaseBoard AssetTag         :
Current BIOS type: UNKNOWN!!!
[*] BIOS detection completed. BIOS is normal.
```

2016.03

终端侦测与响应系统SINPER



- 识别并阻止已知和未知恶意代码
- 识别入侵事件
- 基于机器学习的无特征保护
- 离线保护
- 资产识别与应用管理
- 攻击取证

公有云

私有云

EDR补充EPP的不足

ML安全领域最佳实践

展望

安全驱动发展

Thank you