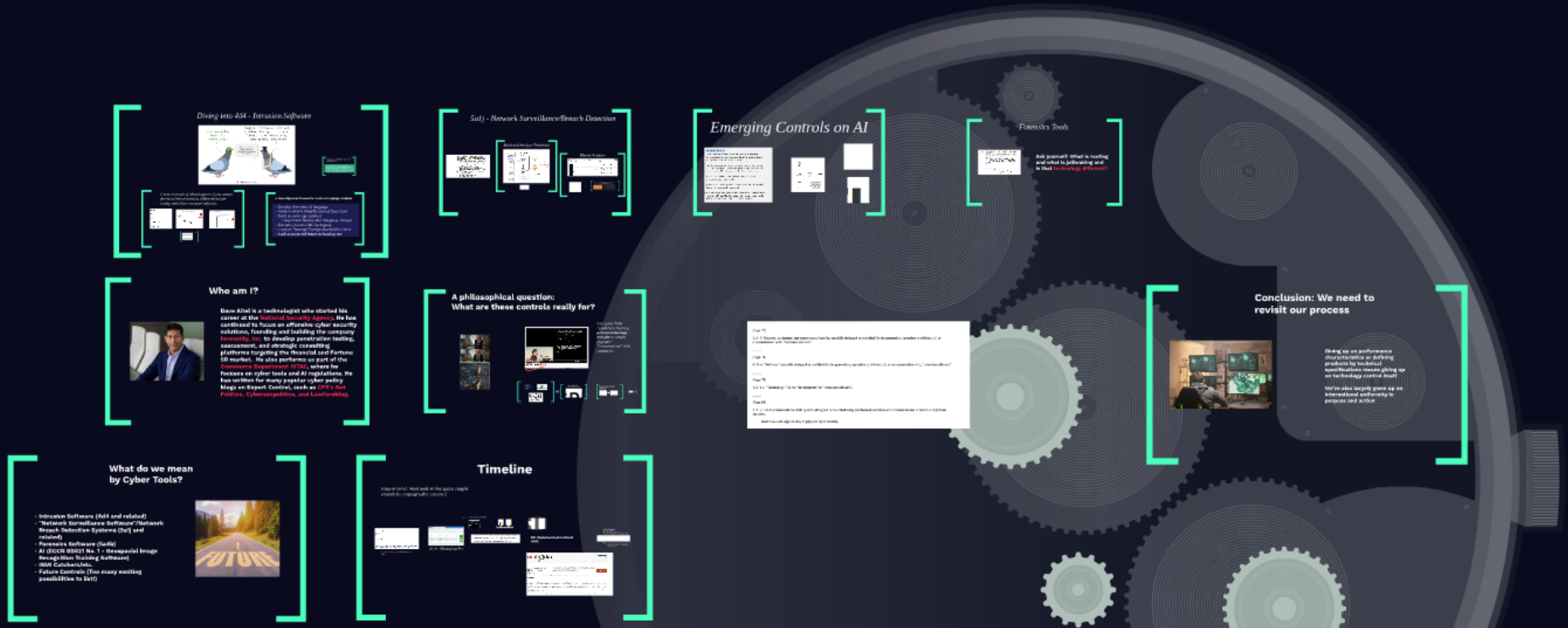
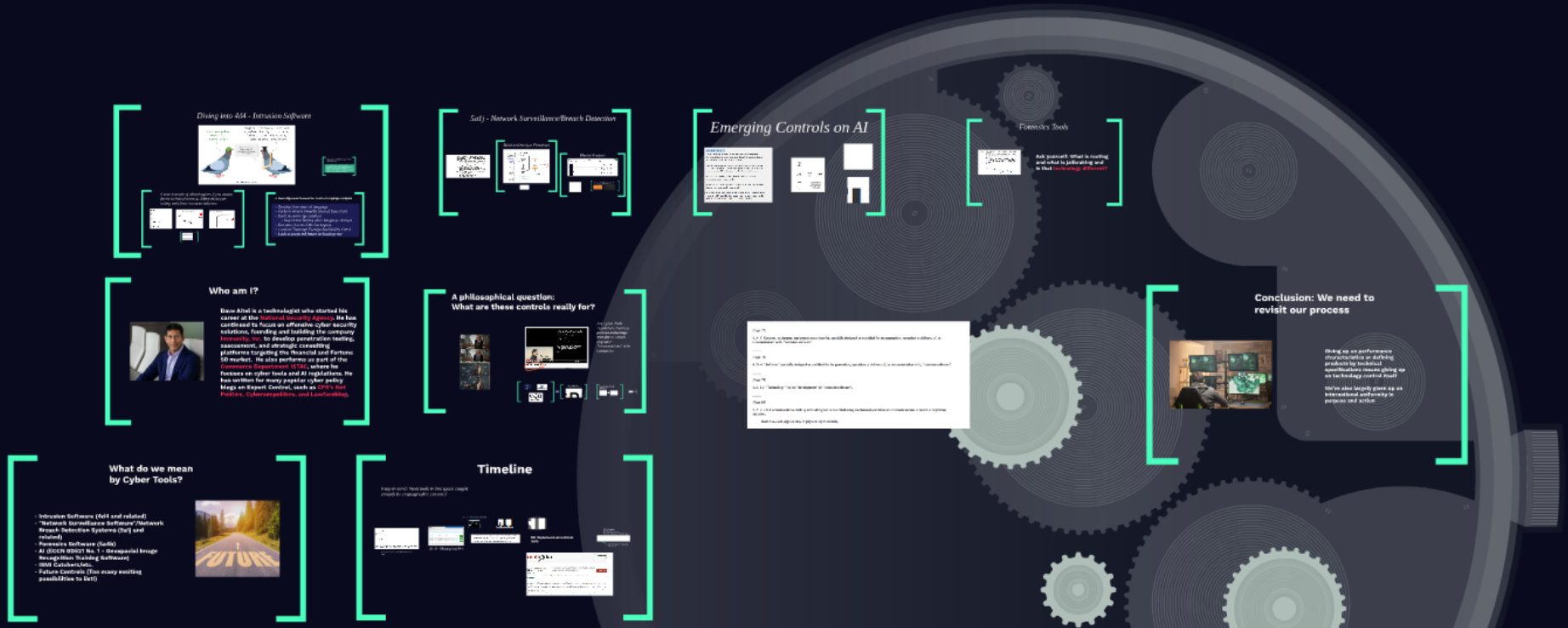


Cyber Tools and Export Control



Cyber Tools and Export Control

Who am I?

Dave Aitel is a technologist who started his career at the National Security Agency. He has continued to focus on offensive cyber security solutions, founding and building the company Immunity, Inc. to develop penetration testing, assessment, and strategic consulting platforms targeting the financial and Fortune 50 market. He also performs as part of the Commerce Department ISTAC, where he focuses on cyber tools and AI regulations. He has written for many popular cyber policy blogs on Export Control, such as CFR's Net Politics, Cybersecpolitics, and Lawfareblog.

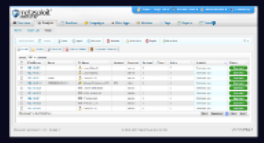
What do we mean by Cyber Tools?

- Intrusion Software (4d4 and related)
- "Network Surveillance Software"/Network Breach Detection Systems (5a1j and related)
- Forensics Software (5a4b)
- AI (ECCN 0D521 No. 1 - Geospacial Image Recognition Training Software)
- ISMI Catchers/etc.
- Future Controls (Too many exciting possibilities to list!)

Timeline

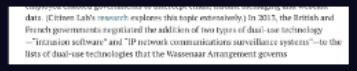
Keep in mind: Most tools in this space caught already by cryptographic controls!

Core Impact, Immunity CANVAS, Metasploit 2003



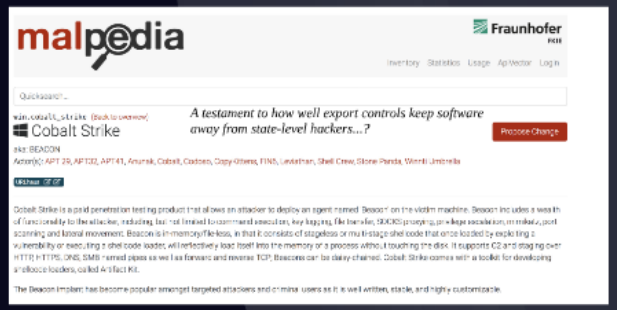
2010 - Metasploit Pro

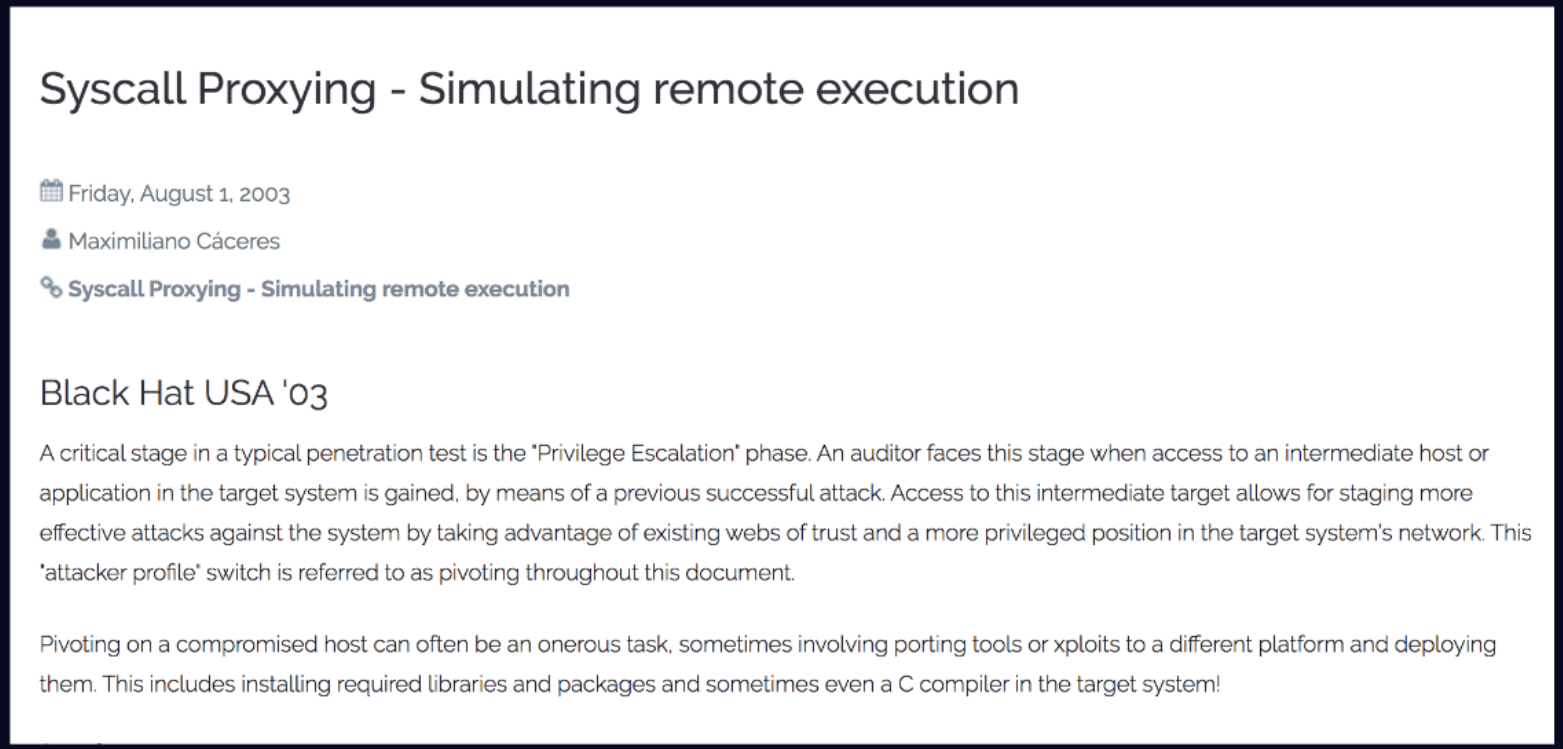
2012 - Cobalt Strike Released



EU implemented controls 2015

2017 Changes
End Use Decontrols
"Update Software" Clarification





Syscall Proxying - Simulating remote execution

Friday, August 1, 2003

Maximiliano Cáceres

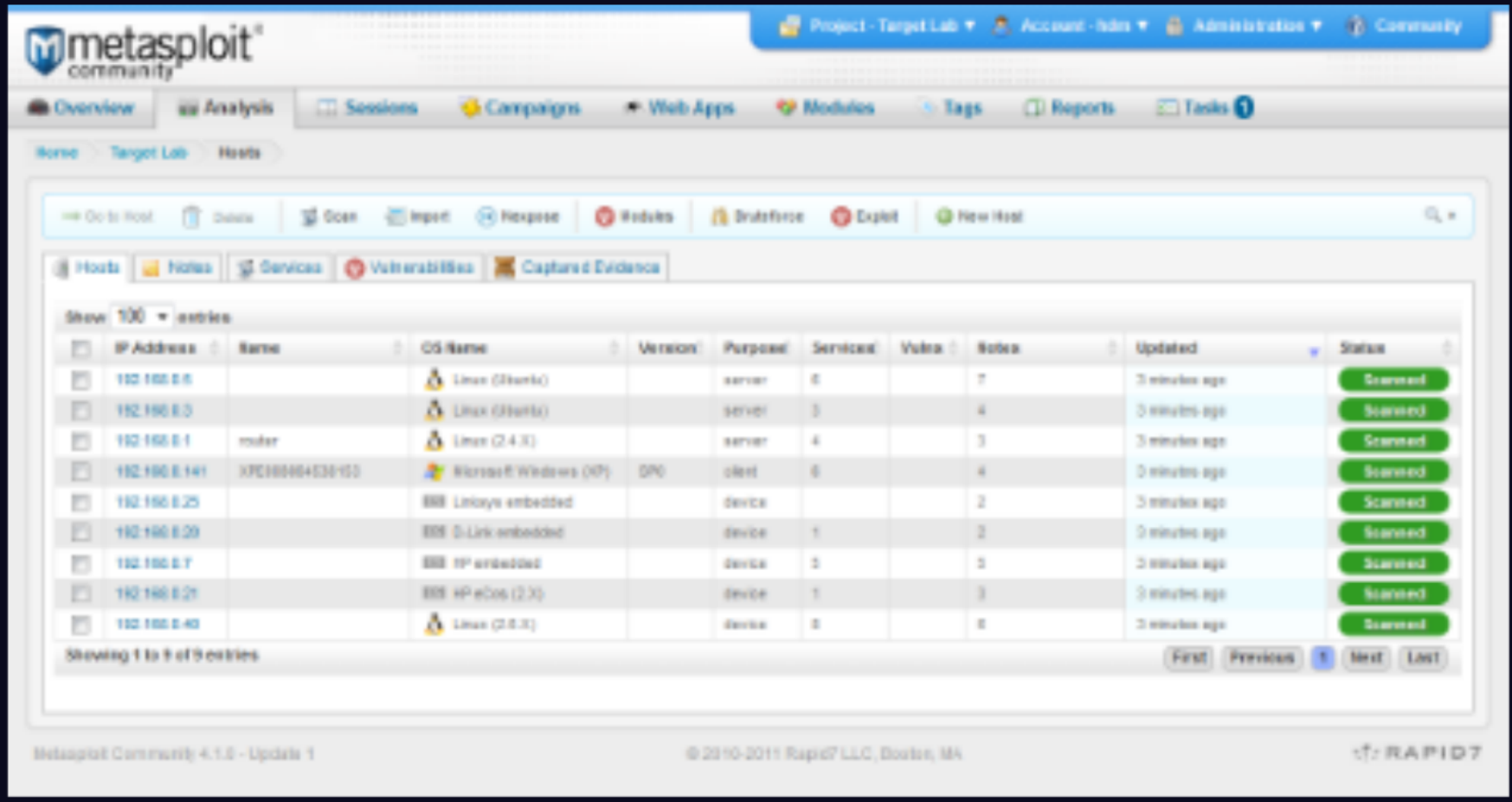
Syscall Proxying - Simulating remote execution

Black Hat USA '03

A critical stage in a typical penetration test is the "Privilege Escalation" phase. An auditor faces this stage when access to an intermediate host or application in the target system is gained, by means of a previous successful attack. Access to this intermediate target allows for staging more effective attacks against the system by taking advantage of existing webs of trust and a more privileged position in the target system's network. This "attacker profile" switch is referred to as pivoting throughout this document.

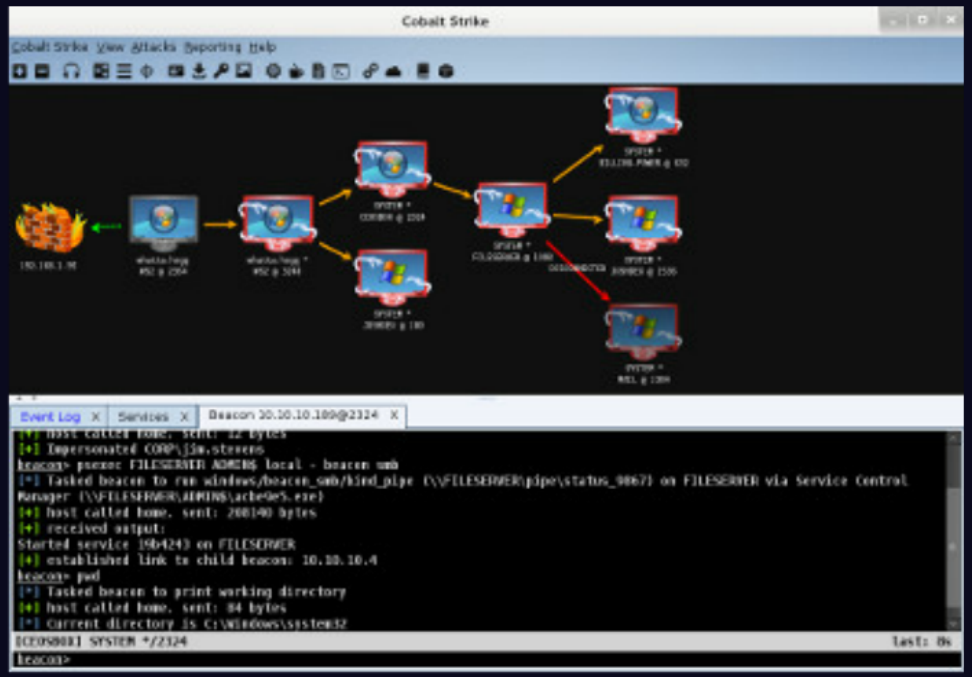
Pivoting on a compromised host can often be an onerous task, sometimes involving porting tools or xploits to a different platform and deploying them. This includes installing required libraries and packages and sometimes even a C compiler in the target system!

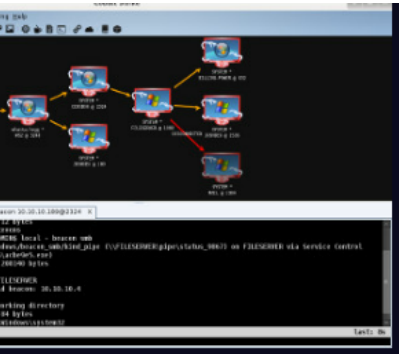
Core Impact, Immunity CANVAS, Metasploit
2003

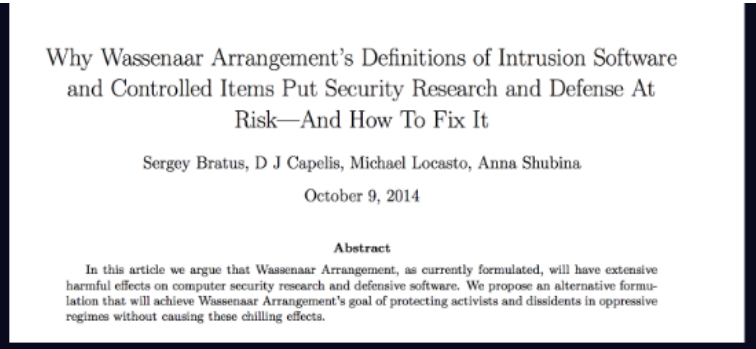


2010 - Metasploit Pro

2012 - Cobalt Strike Released







Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It

Sergey Bratus, D J Capelis, Michael Locasto, Anna Shubina

October 9, 2014

Abstract

In this article we argue that Wassenaar Arrangement, as currently formulated, will have extensive harmful effects on computer security research and defensive software. We propose an alternative formulation that will achieve Wassenaar Arrangement's goal of protecting activists and dissidents in oppressive regimes without causing these chilling effects.

employed enabled governments to intercept email, instant messaging and webcam data. (Citizen Lab's research explores this topic extensively.) In 2013, the British and French governments negotiated the addition of two types of dual-use technology —"intrusion software" and "IP network communications surveillance systems"—to the lists of dual-use technologies that the Wassenaar Arrangement governs

Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It

Sergey Bratus, D J Capelis, Michael Locasto, Anna Shubina

October 9, 2014

Abstract

In this article we argue that Wassenaar Arrangement, as currently formulated, will have extensive harmful effects on computer security research and defensive software. We propose an alternative formulation that will achieve Wassenaar Arrangement's goal of protecting activists and dissidents in oppressive regimes without causing these chilling effects.

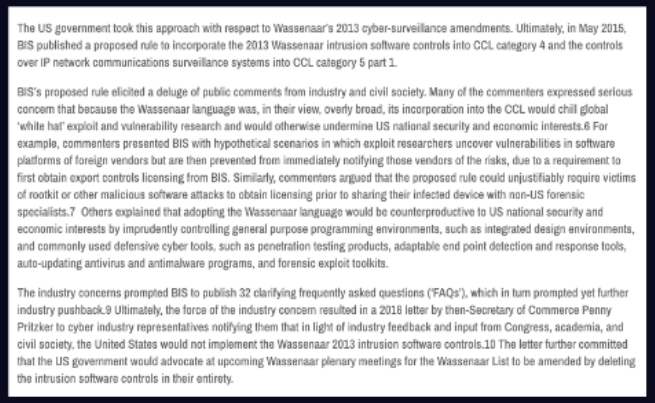
source: https://www.learnexportcompliance.com/cyber-surveillance-export-control-reform-in-the-united-states-2/

The US government took this approach with respect to Wassenaar's 2013 cyber-surveillance amendments. Ultimately, in May 2015, BIS published a proposed rule to incorporate the 2013 Wassenaar intrusion software controls into CCL category 4 and the controls over IP network communications surveillance systems into CCL category 5 part 1.

BIS's proposed rule elicited a deluge of public comments from industry and civil society. Many of the commenters expressed serious concern that because the Wassenaar language was, in their view, overly broad, its incorporation into the CCL would chill global 'white hat' exploit and vulnerability research and would otherwise undermine US national security and economic interests.6 For example, commenters presented BIS with hypothetical scenarios in which exploit researchers uncover vulnerabilities in software platforms of foreign vendors but are then prevented from immediately notifying those vendors of the risks, due to a requirement to first obtain export controls licensing from BIS. Similarly, commenters argued that the proposed rule could unjustifiably require victims of rootkit or other malicious software attacks to obtain licensing prior to sharing their infected device with non-US forensic specialists.7 Others explained that adopting the Wassenaar language would be counterproductive to US national security and economic interests by imprudently controlling general purpose programming environments, such as integrated design environments, and commonly used defensive cyber tools, such as penetration testing products, adaptable end point detection and response tools, auto-updating antivirus and antimalware programs, and forensic exploit toolkits.

The industry concerns prompted BIS to publish 32 clarifying frequently asked questions ('FAQs'), which in turn prompted yet further industry pushback.9 Ultimately, the force of the industry concern resulted in a 2016 letter by then-Secretary of Commerce Penny Pritzker to cyber industry representatives notifying them that in light of industry feedback and input from Congress, academia, and civil society, the United States would not implement the Wassenaar 2013 intrusion software controls.10 The letter further committed that the US government would advocate at upcoming Wassenaar plenary meetings for the Wassenaar List to be amended by deleting the intrusion software controls in their entirety.

2015 BIS DRAMA HAPPENS



The US government took this approach with respect to Wassenaar's 2013 cyber-surveillance amendments. Ultimately, in May 2015, BIS published a proposed rule to incorporate the 2013 Wassenaar intrusion software controls into CCL category 4 and the controls over IP network communications surveillance systems into CCL category 5 part 1.

BIS's proposed rule elicited a deluge of public comments from industry and civil society. Many of the commenters expressed serious concern that because the Wassenaar language was, in their view, overly broad, its incorporation into the CCL would chill global 'white hat' exploit and vulnerability research and would otherwise undermine US national security and economic interests.6 For example, commenters presented BIS with hypothetical scenarios in which exploit researchers uncover vulnerabilities in software platforms of foreign vendors but are then prevented from immediately notifying those vendors of the risks, due to a requirement to first obtain export controls licensing from BIS. Similarly, commenters argued that the proposed rule could unjustifiably require victims of rootkit or other malicious software attacks to obtain licensing prior to sharing their infected device with non-US forensic specialists.7 Others explained that adopting the Wassenaar language would be counterproductive to US national security and economic interests by imprudently controlling general purpose programming environments, such as integrated design environments, and commonly used defensive cyber tools, such as penetration testing products, adaptable end point detection and response tools, auto-updating antivirus and antimalware programs, and forensic exploit toolkits.

The industry concerns prompted BIS to publish 32 clarifying frequently asked questions ('FAQs'), which in turn prompted yet further industry pushback.9 Ultimately, the force of the industry concern resulted in a 2016 letter by then-Secretary of Commerce Penny Pritzker to cyber industry representatives notifying them that in light of industry feedback and input from Congress, academia, and civil society, the United States would not implement the Wassenaar 2013 intrusion software controls.10 The letter further committed that the US government would advocate at upcoming Wassenaar plenary meetings for the Wassenaar List to be amended by deleting the intrusion software controls in their entirety.

2015 BIS DRAMA HAPPENS

EU implemented controls 2015

malpedia

Inventory

2017 Changes
End Use Decontrols
"Update Software" Clarification

1. What changes were made to the Wassenaar Arrangement list in 2017 for intrusion software and why were they made?

Based on the extensive public feedback on the May 2015 rule (80 FR 28853) that BIS proposed, the U.S. went back to Wassenaar in 2016 and 2017 to negotiate changes to the text in order to minimize the negative impacts the entries would have. The changes that were published are the result of those negotiations. https://www.bis.doc.gov/index.php/regulations/federal-register-notices/17-regulations/816-federal-register-notices-2015#FR28853

There are two changes that were made to the text. First, Notes were added to the entry for the "technology" for the "development" of "intrusion software". The note clarifies that technology exchanged for vulnerability disclosure or cyber incident response purposes (as defined) are not controlled.

The second change is a Note added to the 4.D.4 control on the command and delivery platform for "intrusion software". The note clarifies that software that provides software updates or upgrades are not controlled by the entry, as long as the software is not designed to update "intrusion software" or command and delivery platforms, or turn something into "intrusion softw[illegible]r a command and delivery platform.

It is telling when you have to revise your control language to explicitly whitelist common things like software updates...

2015

It is telling
language t
software up

malpedia

Fraunhofer FKIE

Inventory Statistics Usage ApiVector Login

Quicksearch...

win.cobalt_strike (Back to overview)

Cobalt Strike

A testament to how well export controls keep software away from state-level hackers...?

Propose Change

aka: BEACON

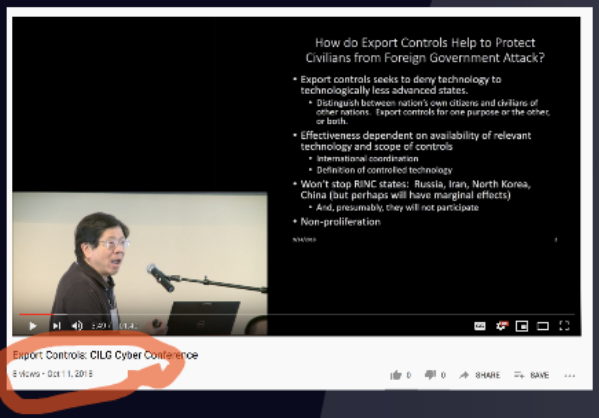
Actor(s): APT 29, APT32, APT41, Anunak, Cobalt, Codoso, CopyKittens, FIN6, Leviathan, Shell Crew, Stone Panda, Winnti Umbrella

URLhaus

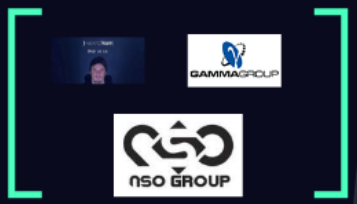
Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent named 'Beacon' on the victim machine. Beacon includes a wealth of functionality to the attacker, including, but not limited to command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz, port scanning and lateral movement. Beacon is in-memory/file-less, in that it consists of stageless or multi-stage shellcode that once loaded by exploiting a vulnerability or executing a shellcode loader, will reflectively load itself into the memory of a process without touching the disk. It supports C2 and staging over HTTP, HTTPS, DNS, SMB named pipes as well as forward and reverse TCP; Beacons can be daisy-chained. Cobalt Strike comes with a toolkit for developing shellcode loaders, called Artifact Kit.

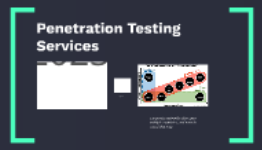
The Beacon implant has become popular amongst targeted attackers and criminal users as it is well written, stable, and highly customizable.

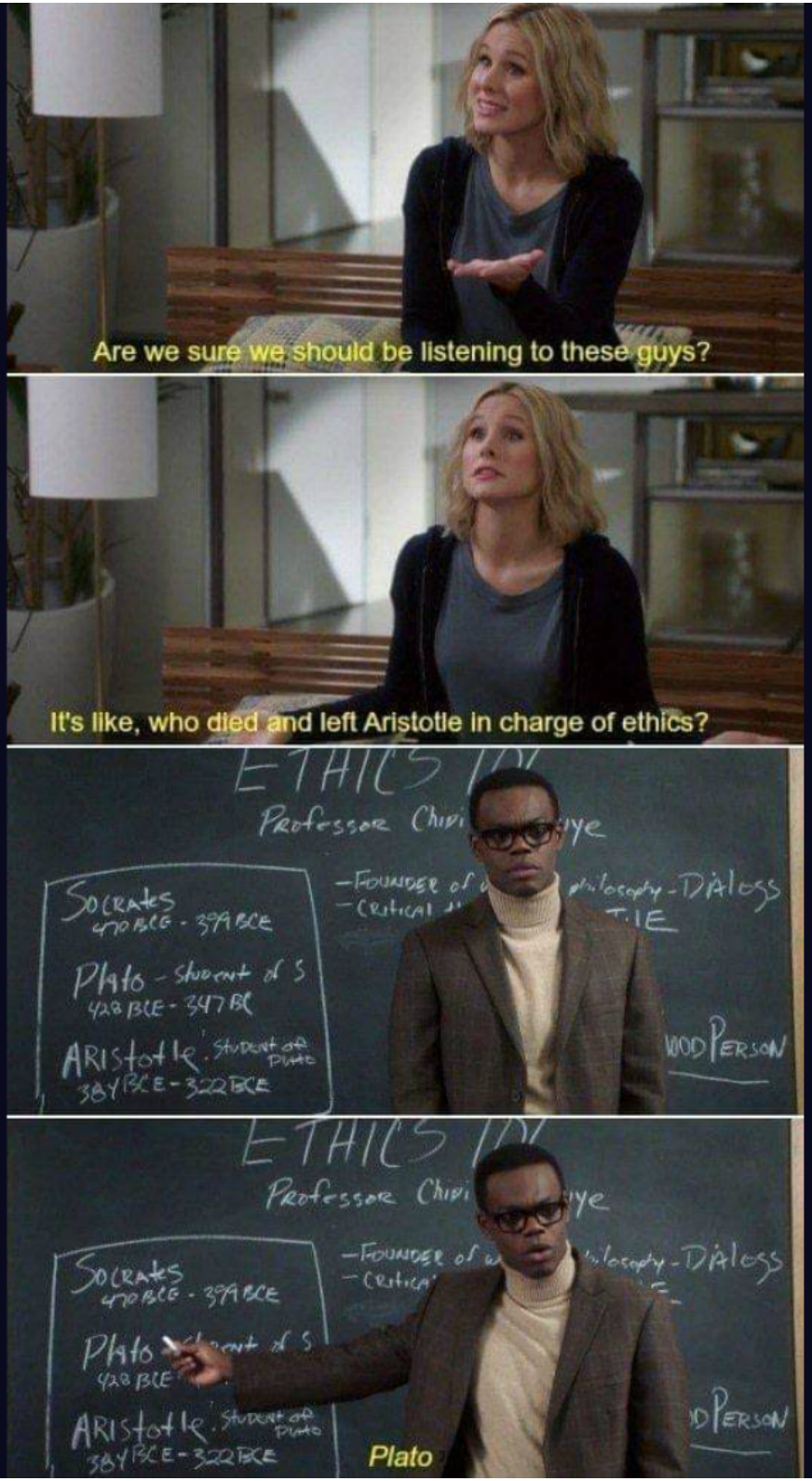
A philosophical question: What are these controls really for?



*Are Cyber Tools regulations meant to **prevent technology transfer** or simply engender "conversations" with companies*






Are we sure we should be listening to these guys?
It's like, who died and left Aristotle in charge of ethics?
ETHICS
Professor
SOCRATES
470 BCE - 399 BCE
PLATO - STUDENT OF S
428 BCE - 347 BC
ARISTOTLE. STUDENT OF PLATO
384 BCE - 322 BCE
-FOUNDER OF
-CRITICAL
PHILOSOPHY - DIALOGS
TIE
WOOD PERSON
Plato

Are Cyber Tools regulations meant to ***prevent technology transfer*** *or simply engender "conversations" with companies*

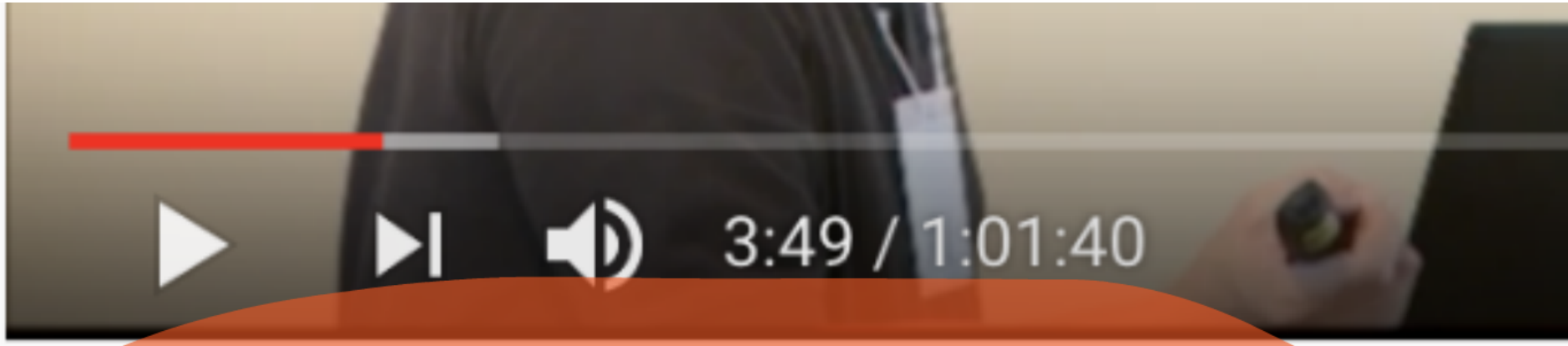
Export Controls: CILG Cyber Conference

8 views • Oct 11, 2018

0 0 SHARE SAVE

How do Export Controls Help to Protect Civilians from Foreign Government Attack?

- Export controls seeks to deny technology to technologically less advanced states.
  - Distinguish between nation's own citizens and civilians of other nations. Export controls for one purpose or the other, or both.
- Effectiveness dependent on availability of relevant technology and scope of controls
  - International coordination
  - Definition of controlled technology
- Won't stop RINC states: Russia, Iran, North Korea, China (but perhaps will have marginal effects)
  - And, presumably, they will not participate
- Non-proliferation



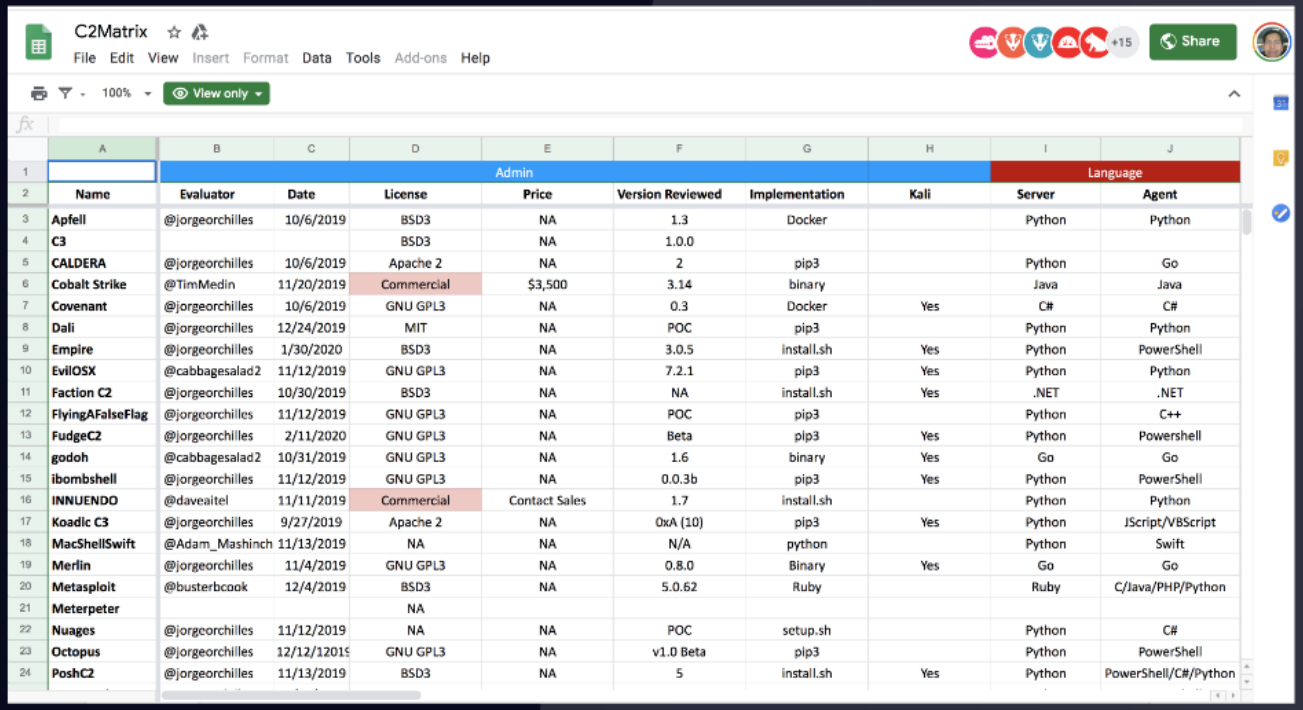
Export Controls: CILG Cyber Conferen

8 views • Oct 11, 2018

GAMMAGROUP

NSO GROUP

There's An Entire Ocean of Penetration Testing Tools Though



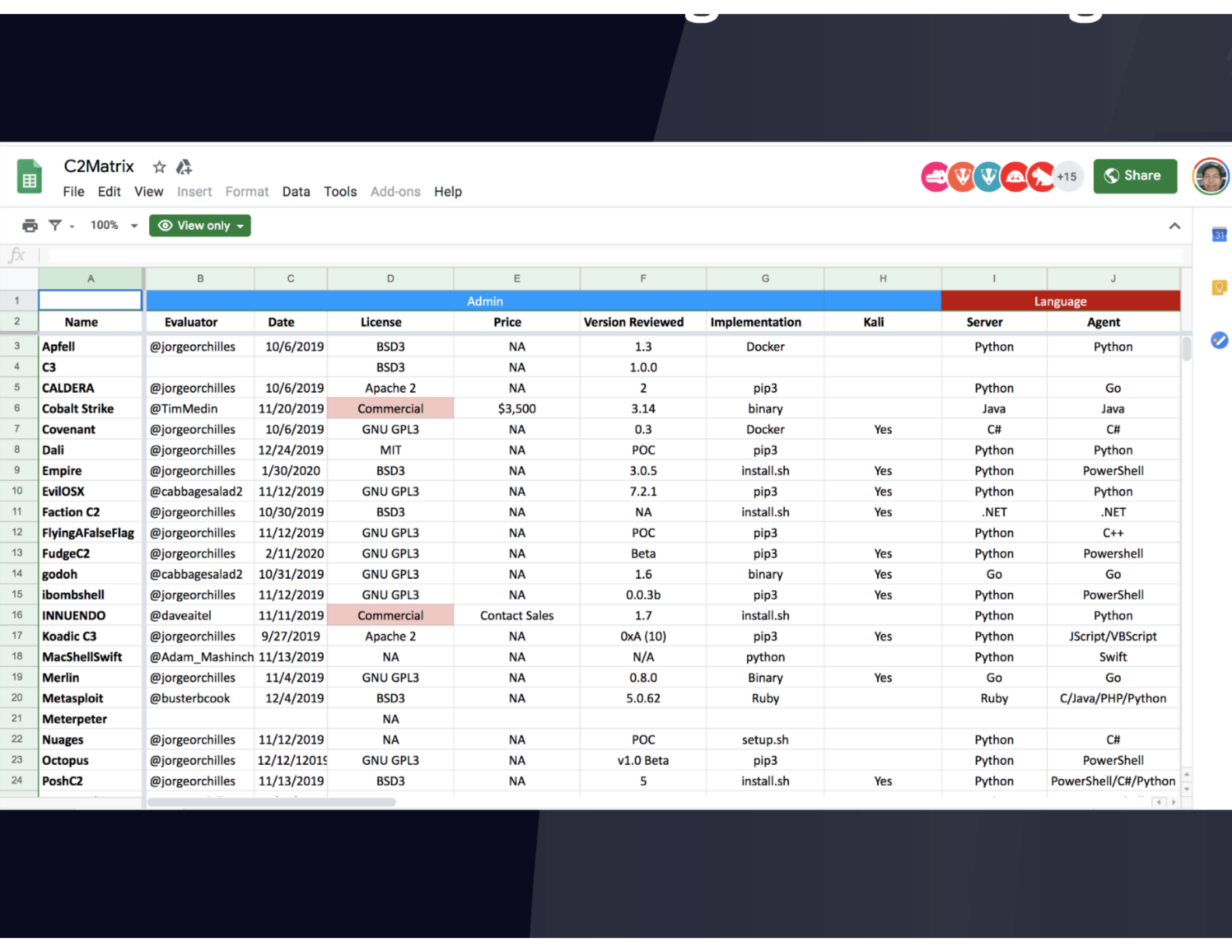
C2Matrix

File Edit View Insert Format Data Tools Add-ons Help

Share

100% View only

		Admin						Language	
Name	Evaluator	Date	License	Price	Version Reviewed	Implementation	Kali	Server	Agent
Apfell	@jorgeorchilles	10/6/2019	BSD3	NA	1.3	Docker		Python	Python
C3			BSD3	NA	1.0.0				
CALDERA	@jorgeorchilles	10/6/2019	Apache 2	NA	2	pip3		Python	Go
Cobalt Strike	@TimMedin	11/20/2019	Commercial	$3,500	3.14	binary		Java	Java
Covenant	@jorgeorchilles	10/6/2019	GNU GPL3	NA	0.3	Docker	Yes	C#	C#
Dali	@jorgeorchilles	12/24/2019	MIT	NA	POC	pip3		Python	Python
Empire	@jorgeorchilles	1/30/2020	BSD3	NA	3.0.5	install.sh	Yes	Python	PowerShell
EvilOSX	@cabbagesalad2	11/12/2019	GNU GPL3	NA	7.2.1	pip3	Yes	Python	Python
Faction C2	@jorgeorchilles	10/30/2019	BSD3	NA	NA	install.sh	Yes	.NET	.NET
FlyingAFalseFlag	@jorgeorchilles	11/12/2019	GNU GPL3	NA	POC	pip3		Python	C++
FudgeC2	@jorgeorchilles	2/11/2020	GNU GPL3	NA	Beta	pip3	Yes	Python	Powershell
godoh	@cabbagesalad2	10/31/2019	GNU GPL3	NA	1.6	binary	Yes	Go	Go
ibombshell	@jorgeorchilles	11/12/2019	GNU GPL3	NA	0.0.3b	pip3	Yes	Python	PowerShell
INNUENDO	@daveaitel	11/11/2019	Commercial	Contact Sales	1.7	install.sh		Python	Python
Koadic C3	@jorgeorchilles	9/27/2019	Apache 2	NA	0xA (10)	pip3	Yes	Python	JScript/VBScript
MacShellSwift	@Adam_Mashinch	11/13/2019	NA	NA	N/A	python		Python	Swift
Merlin	@jorgeorchilles	11/4/2019	GNU GPL3	NA	0.8.0	Binary	Yes	Go	Go
Metasploit	@busterbcook	12/4/2019	BSD3	NA	5.0.62	Ruby		Ruby	C/Java/PHP/Python
Meterpeter			NA						
Nuages	@jorgeorchilles	11/12/2019	NA	NA	POC	setup.sh		Python	C#
Octopus	@jorgeorchilles	12/12/12019	GNU GPL3	NA	v1.0 Beta	pip3		Python	PowerShell
PoshC2	@jorgeorchilles	11/13/2019	BSD3	NA	5	install.sh	Yes	Python	PowerShell/C#/Python



C2Matrix

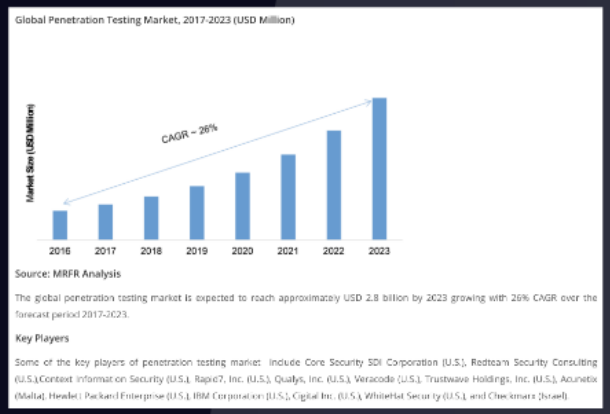
File Edit View Insert Format Data Tools Add-ons Help

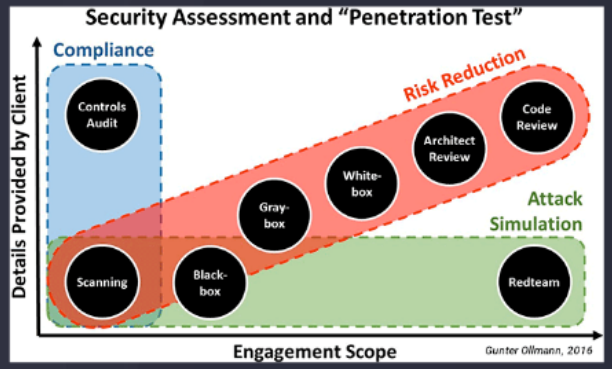
100% View only

Share

	A	B	C	D	E	F	G	H	I	J
1		Admin							Language	
2	**Name**	**Evaluator**	**Date**	**License**	**Price**	**Version Reviewed**	**Implementation**	**Kali**	**Server**	**Agent**
3	**Apfell**	@jorgeorchilles	10/6/2019	BSD3	NA	1.3	Docker		Python	Python
4	**C3**			BSD3	NA	1.0.0				
5	**CALDERA**	@jorgeorchilles	10/6/2019	Apache 2	NA	2	pip3		Python	Go
6	**Cobalt Strike**	@TimMedin	11/20/2019	Commercial	$3,500	3.14	binary		Java	Java
7	**Covenant**	@jorgeorchilles	10/6/2019	GNU GPL3	NA	0.3	Docker	Yes	C#	C#
8	**Dali**	@jorgeorchilles	12/24/2019	MIT	NA	POC	pip3		Python	Python
9	**Empire**	@jorgeorchilles	1/30/2020	BSD3	NA	3.0.5	install.sh	Yes	Python	PowerShell
10	**EvilOSX**	@cabbagesalad2	11/12/2019	GNU GPL3	NA	7.2.1	pip3	Yes	Python	Python
11	**Faction C2**	@jorgeorchilles	10/30/2019	BSD3	NA	NA	install.sh	Yes	.NET	.NET
12	**FlyingAFalseFlag**	@jorgeorchilles	11/12/2019	GNU GPL3	NA	POC	pip3		Python	C++
13	**FudgeC2**	@jorgeorchilles	2/11/2020	GNU GPL3	NA	Beta	pip3	Yes	Python	Powershell
14	**godoh**	@cabbagesalad2	10/31/2019	GNU GPL3	NA	1.6	binary	Yes	Go	Go
15	**ibombshell**	@jorgeorchilles	11/12/2019	GNU GPL3	NA	0.0.3b	pip3	Yes	Python	PowerShell
16	**INNUENDO**	@daveaitel	11/11/2019	Commercial	Contact Sales	1.7	install.sh		Python	Python
17	**Koadic C3**	@jorgeorchilles	9/27/2019	Apache 2	NA	0xA (10)	pip3	Yes	Python	JScript/VBScript
18	**MacShellSwift**	@Adam_Mashinch	11/13/2019	NA	NA	N/A	python		Python	Swift
19	**Merlin**	@jorgeorchilles	11/4/2019	GNU GPL3	NA	0.8.0	Binary	Yes	Go	Go
20	**Metasploit**	@busterbcook	12/4/2019	BSD3	NA	5.0.62	Ruby		Ruby	C/Java/PHP/Python
21	**Meterpeter**			NA						
22	**Nuages**	@jorgeorchilles	11/12/2019	NA	NA	POC	setup.sh		Python	C#
23	**Octopus**	@jorgeorchilles	12/12/1201	GNU GPL3	NA	v1.0 Beta	pip3		Python	PowerShell
24	**PoshC2**	@jorgeorchilles	11/13/2019	BSD3	NA	5	install.sh	Yes	Python	PowerShell/C#/Python

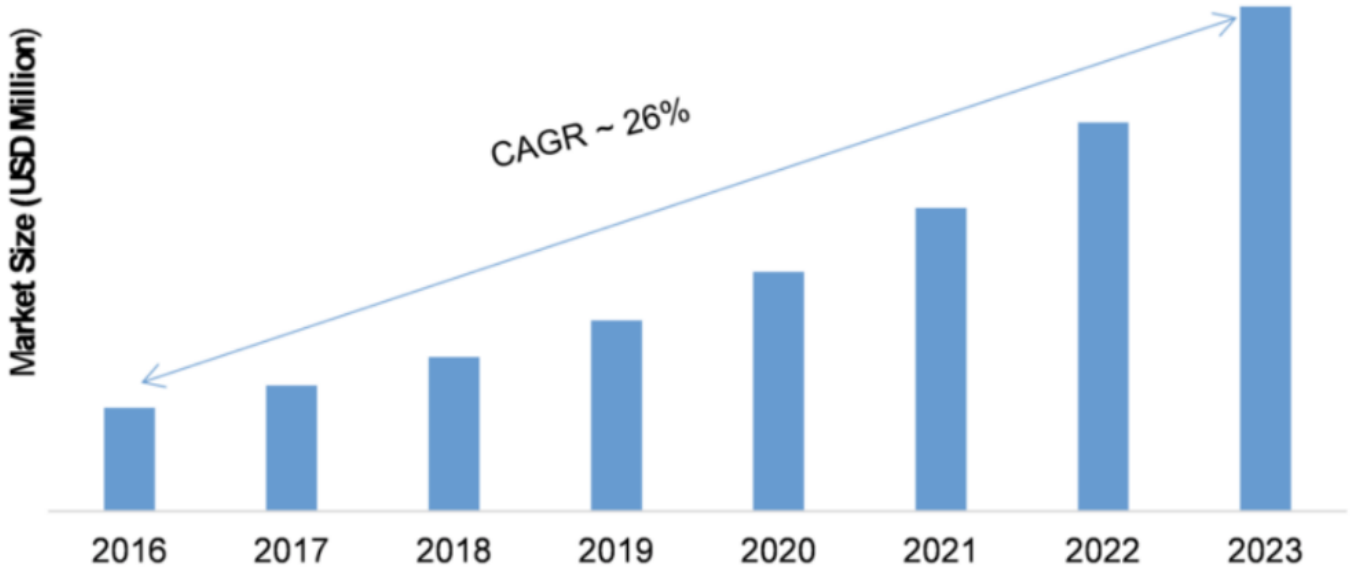
Penetration Testing Services





Corporate networks often span multiple countries, and must be tested that way.

Global Penetration Testing Market, 2017-2023 (USD Million)



Source: MRFR Analysis

The global penetration testing market is expected to reach approximately USD 2.8 billion by 2023 growing with 26% CAGR over the forecast period 2017-2023.

Key Players

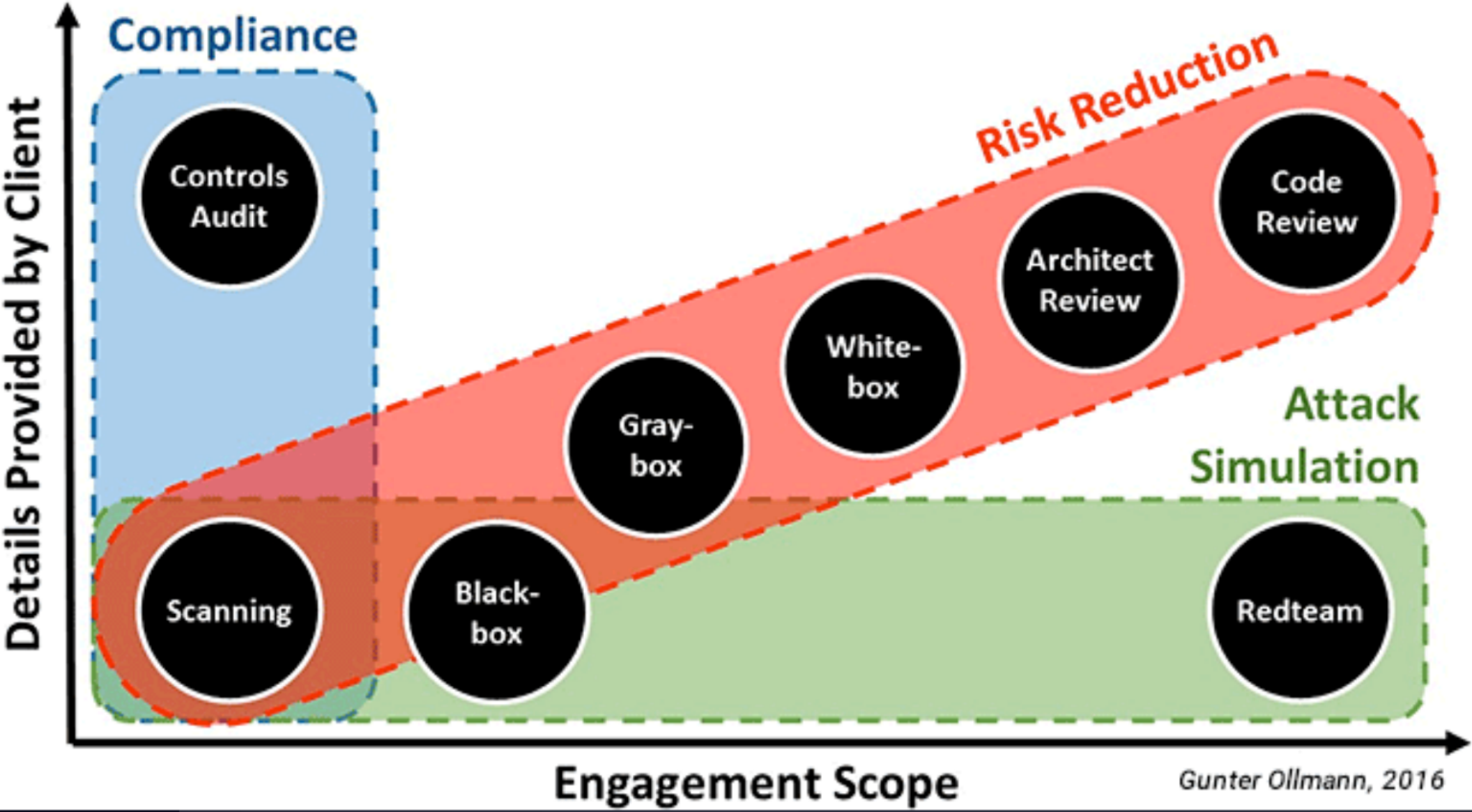
Some of the key players of penetration testing market include Core Security SDI Corporation (U.S.), Redteam Security Consulting (U.S.),Context Information Security (U.S.), Rapid7, Inc. (U.S.), Qualys, Inc. (U.S.), Veracode (U.S.), Trustwave Holdings, Inc. (U.S.), Acunetix (Malta), Hewlett Packard Enterprise (U.S.), IBM Corporation (U.S.), Cigital Inc. (U.S.), WhiteHat Security (U.S.), and Checkmarx (Israel).

Ten Reasons to Pen-Test for Compliance

1. **Meet data security regulation mandates and avoid fines.**

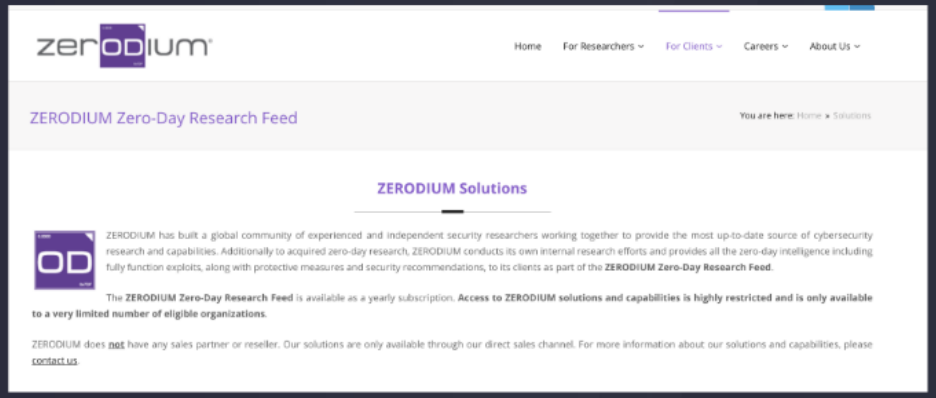
   First, pen testing is mandated by many industry-specific regulations, especially regarding technical, financial or healthcare institutions. In the payment card industry, for example, PCI-DSS regulations mandate both an annual and ongoing penetration testing after any system changes; when that occurs, both network and application layer pen testing are to be done. SOX (the Sarbanes–Oxley Act of 2002) and HIPAA (the Health Insurance Portability and Accountability Act) also require an annual penetration test from a third party. Similar provisions are requested by other data protection standards, like GLBA, FISMA, and OWASP. The international information security standard ISO 27001 also has pen testing in its guidelines. In EU, the General Data Protection Regulation (GDPR), comes into force this year on 25 May 2018; with it, the recommendation to include regular testing to assess the resilience of applications and critical infrastructure, all to aid the discovery of security vulnerabilities and to try the effectiveness of the security controls. In many cases, companies risk fines for noncompliance. Penetration tests, therefore, help comply with regulatory bodies.

Security Assessment and "Penetration Test"



Gunter Ollmann, 2016

Unknown unknowns: The 0day Market



Is export control being used as a backdoor way to control this, and if so, is that a good idea?

ZERODIUM Solutions

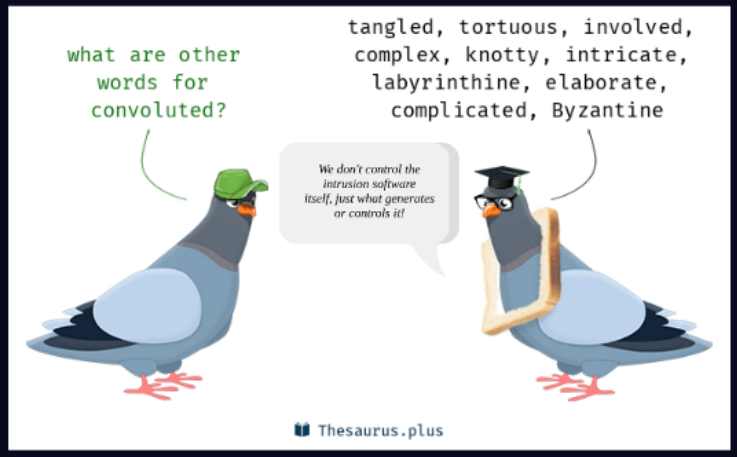
ZERODIUM has built a global community of experienced and independent security researchers working together to provide the most up-to-date source of cybersecurity research and capabilities. Additionally to acquired zero-day research, ZERODIUM conducts its own internal research efforts and provides all the zero-day intelligence including fully function exploits, along with protective measures and security recommendations, to its clients as part of the **ZERODIUM Zero-Day Research Feed**.

The **ZERODIUM Zero-Day Research Feed** is available as a yearly subscription. **Access to ZERODIUM solutions and capabilities is highly restricted and is only available to a very limited number of eligible organizations**.

ZERODIUM does **not** have any sales partner or reseller. Our solutions are only available through our direct sales channel. For more information about our solutions and capabilities, please contact us.

Is export control being used as a backdoor way to control this, and if so, is that a good idea?

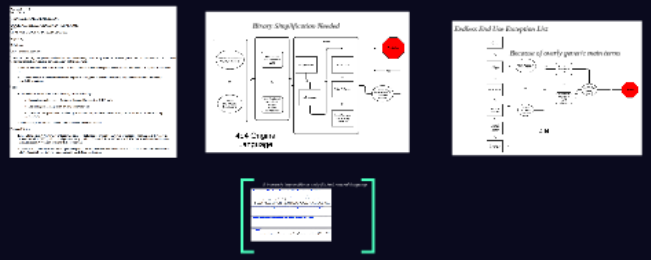
Diving into 4d4 - Intrusion Software



How people actually build Cyber Tools control language

- Ask an NGO to send in marketing documents from some company they hate
- Hash out some language from that
- Send out the language, see who complains
- Make minor changes, call it done.

A case example of what happens if you cannot derive technical terms to differentiate pen-testing tools from intrusion software



A More Rigorous Process for Control Language Analysis

- *Develop flow chart of language*
- *Perform Binary Simplification of flow chart*
- *Build Scenario Spreadsheet*
  - *Regression Testing when language changes*
- *Examine Potential Market Impact*
- *Conduct Thorough Foreign Availability Check*
- ***Look at projected future technology use***

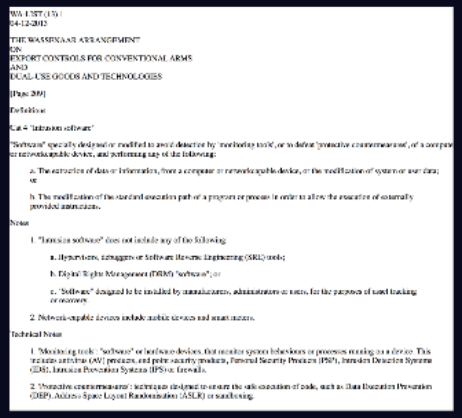
what are other words for convoluted?

tangled, tortuous, involved, complex, knotty, intricate, labyrinthine, elaborate, complicated, Byzantine

We don't control the intrusion software itself, just what generates or controls it!

Thesaurus.plus

A case example of what happens if you cannot derive technical terms to differentiate pen-testing tools from intrusion software



WA-LIST (15)
04-12-2012

THE WASSENAAR ARRANGEMENT
ON
EXPORT CONTROLS FOR CONVENTIONAL ARMS
AND
DUAL-USE GOODS AND TECHNOLOGIES

[Page 209]

Definitions

Cat 4 "intrusion software"

"Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following:

a. The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or

b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes

1. "Intrusion software" does not include any of the following:

a. Hypervisors, debuggers or software Reverse Engineering (SRE) tools;

b. Digital Rights Management (DRM) "software"; or

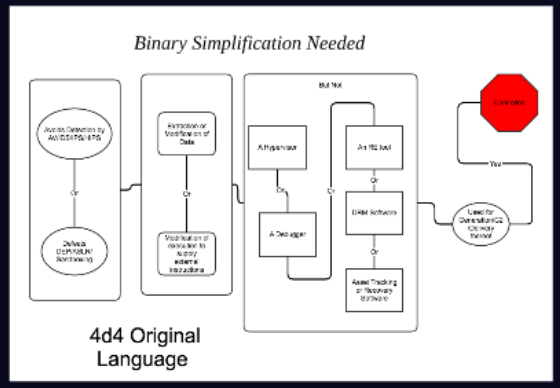
c. "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.

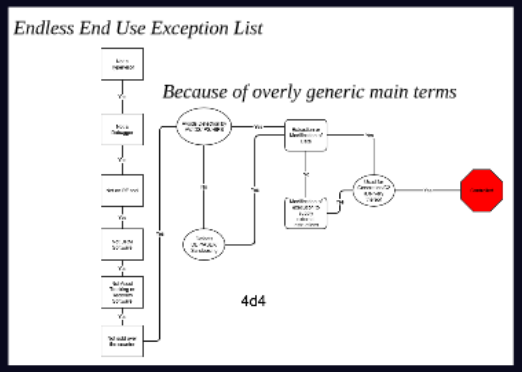
2. Network-capable devices include mobile devices and smart meters.

Technical Notes

1. 'Monitoring tools': "software" or hardware devices that monitor system behaviours or processes running on a device. This includes anti-virus (AV) products, end-point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.

2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as: Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing.





THE WASSENAAR ARRANGEMENT
ON
EXPORT CONTROLS FOR CONVENTIONAL ARMS
AND
DUAL-USE GOODS AND TECHNOLOGIES

[Page 209]

Definitions

Cat 4 "Intrusion software"

"Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a compute or networkcapable device, and performing any of the following:

a. The extraction of data or information, from a computer or networkcapable device, or the modification of system or user data; or

b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes

1. "Intrusion software" does not include any of the following:

a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;

b. Digital Rights Management (DRM) "software"; or

c. "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.

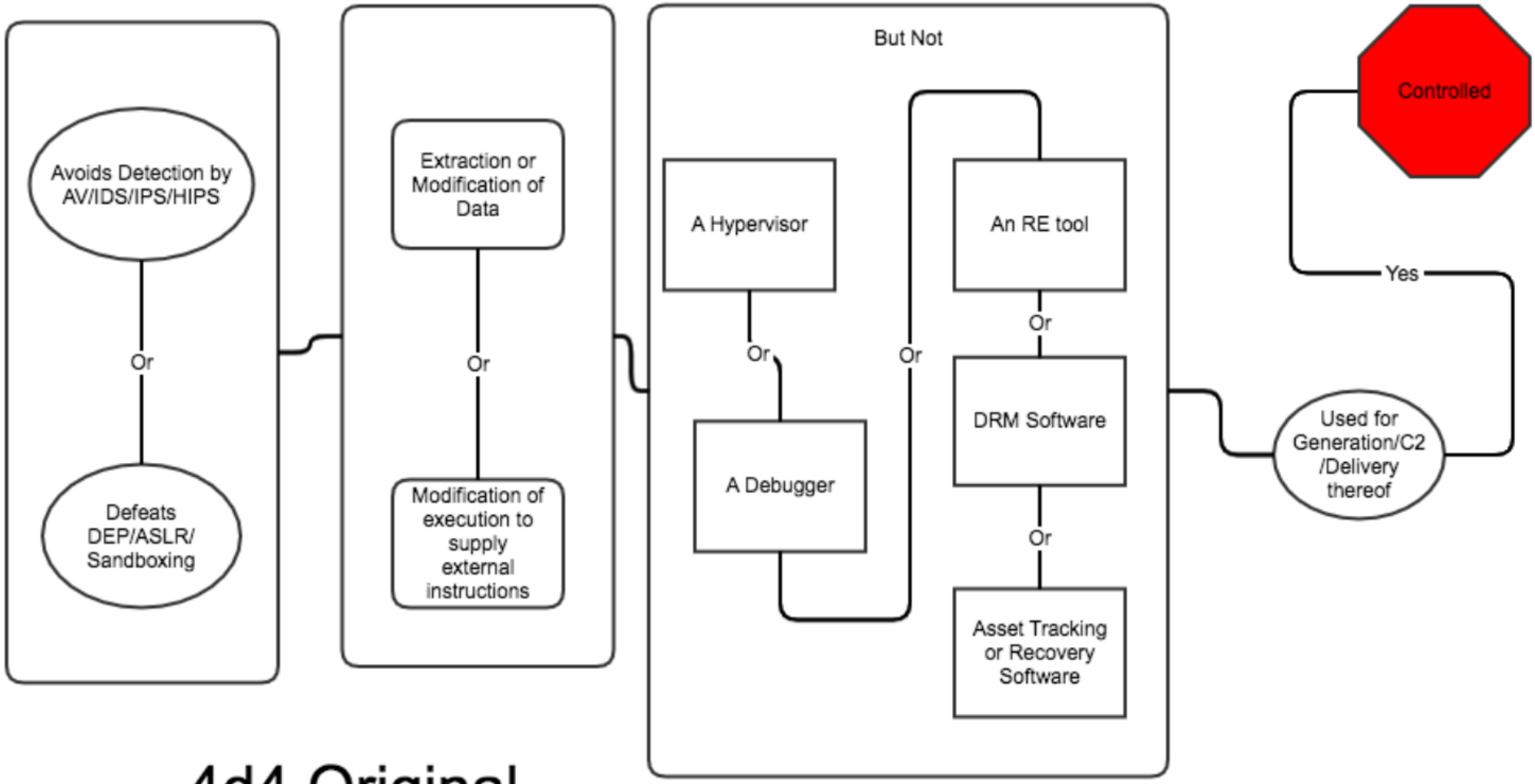
2. Network-capable devices include mobile devices and smart meters.

Technical Notes

1. 'Monitoring tools': "software" or hardware devices, that monitor system behaviours or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.

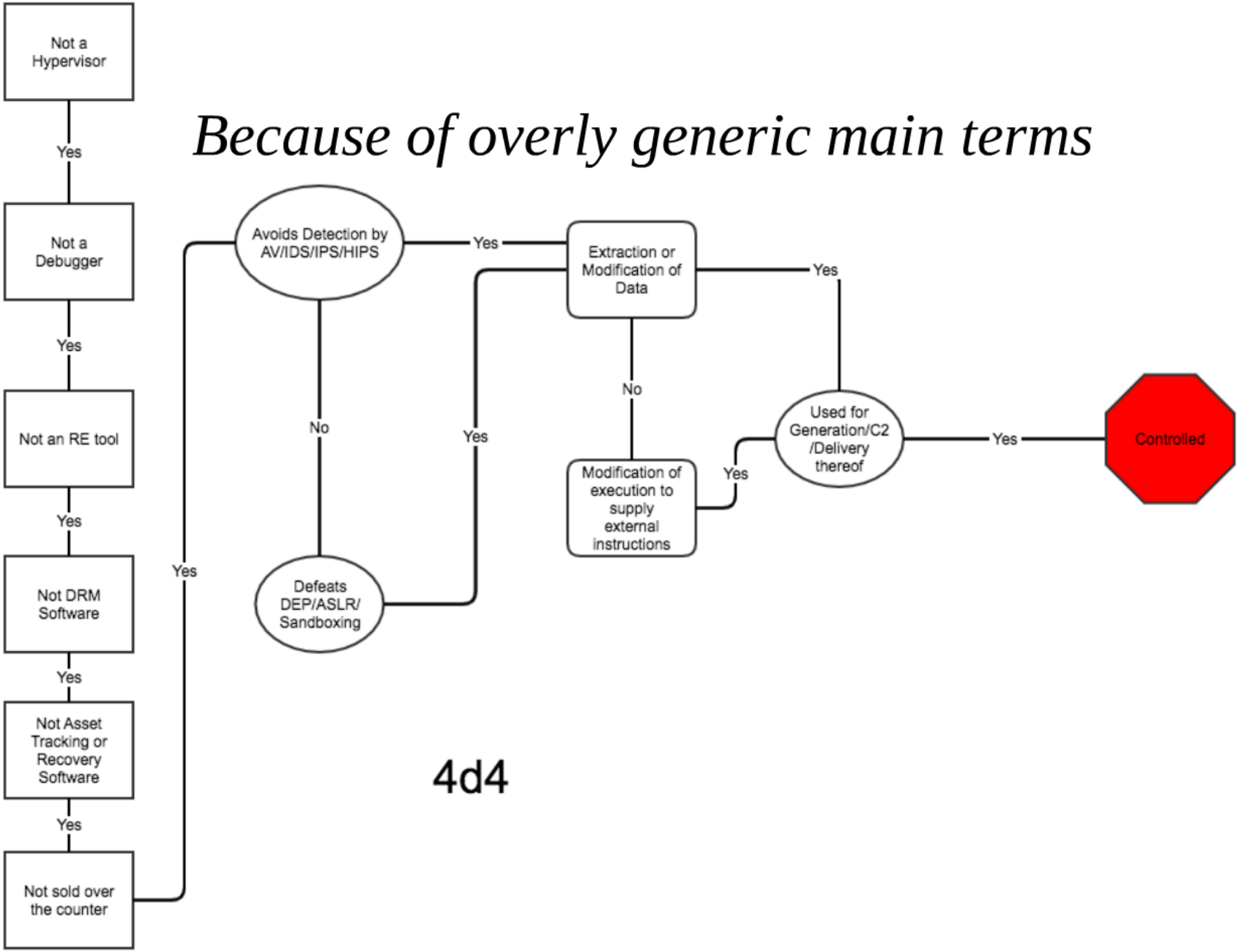
2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) or sandboxing.

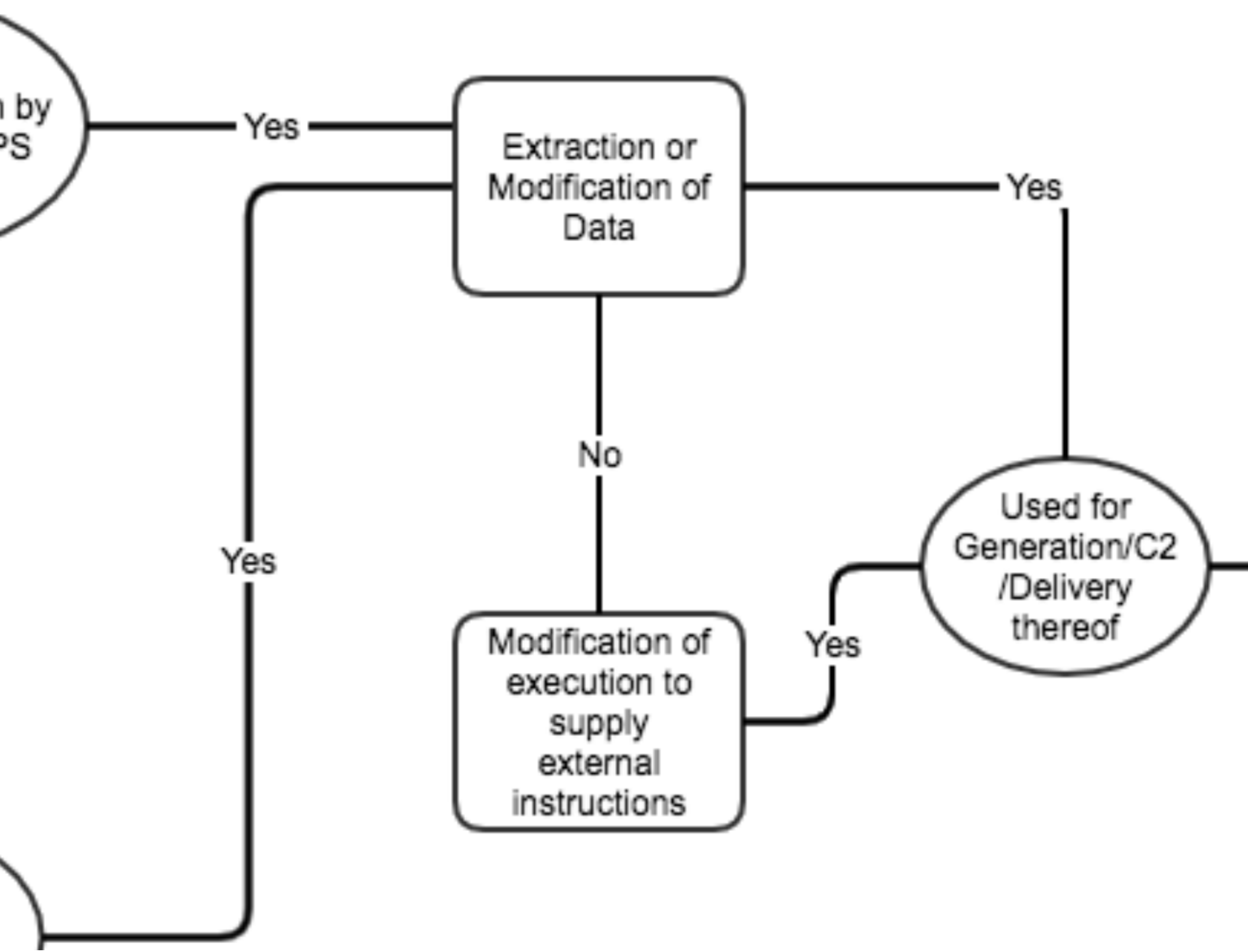
Binary Simplification Needed



4d4 Original Language

Endless End Use Exception List




n by
PS
Yes
Extraction or Modification of Data
Yes
No
Yes
Used for Generation/C2 /Delivery thereof
Yes
Modification of execution to supply external instructions
Yes

It is nearly impossible to truly fix bad control language

1. What changes were made to the Wassenaar Arrangement list in 2017 for intrusion software and why were they made?

Based on the extensive public feedback on the May 2015 rule (80 FR 28853) that BIS proposed, the U.S. went back to Wassenaar in 2016 and 2017 to negotiate changes to the text in order to minimize the negative impacts the entries would have. The changes that were published are the result of those negotiations. https://www.bis.doc.gov/index.php/regulations/federal-register-notices/17-regulations/816-federal-register-notices-2015#FR28853

There are two changes that were made to the text. First, Notes were added to the entry for the "technology" for the "development" of "intrusion software". The note clarifies that technology exchanged for vulnerability disclosure or cyber incident response purposes (as defined) are not controlled.

The second change is a Note added to the 4.D.4 control on the command and delivery platform for "intrusion software". The note clarifies that software that provides software updates or upgrades are not controlled by the entry, as long as the software is not designed to update "intrusion software" or command and delivery platforms, or turn something into "intrusion software" or a command and delivery platform.

3. Does the publication of these changes now mean that the U.S. is controlling these items? Do I need to start applying for export licenses?

No. The text that was published was the text that was agreed to by the Wassenaar Arrangement. In order for it to become law in the U.S. the U.S. government would need to publish a rule implementing these changes. Because no rule has been published yet, there are no new controls on these entries at this time.

2. Does BIS believe these changes address all of the concerns that have been raised with these entries?

No. These are the changes that we have been able to get agreement on, at this time, with other Wassenaar Arrangement members and do not address all of the concerns raised. BIS considers these changes to be the first step in addressing the concerns.

4. What's next?

We have not decided on a next step yet. There are a range of possible actions we could take, including returning to Wassenaar in 2018 to negotiate further changes to the text, publishing a rule to implement the text, or publishing a notice of inquiry or proposed rule for further comment.

A More Rigorous Process for Control Language Analysis

- *Develop flow chart of language*
- *Perform Binary Simplification of flow chart*
- *Build Scenario Spreadsheet*
    - *Regression Testing when language changes*
- *Examine Potential Market Impact*
- *Conduct Thorough Foreign Availability Check*
- ***Look at projected future technology use***

How people actually build Cyber Tools control language

- Ask an NGO to send in marketing documents from some company they hate
- Hash out some language from that
- Send out the language, see who complains!
- Make minor changes, call it done.

5a1j - Network Surveillance/Breach Detection

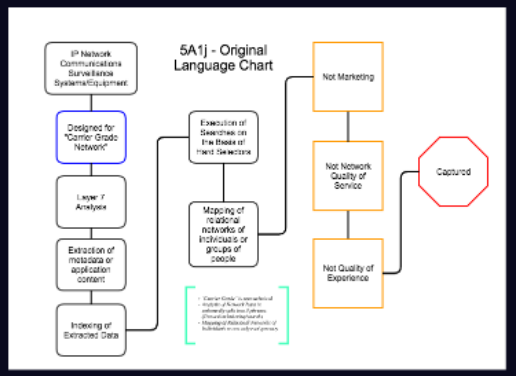
5. A. 1. j. IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:

1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
   a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
   b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
   c. Indexing of extracted data; and
2. Being specially designed to carry out all of the following:
   a. Execution of searches on the basis of "hard selectors"; and
   b. Mapping of the relational network of an individual or of a group of people.

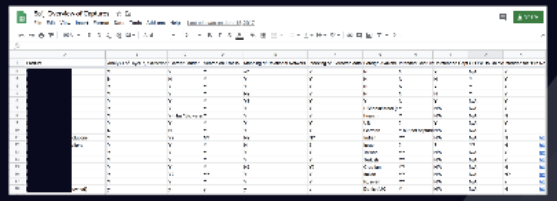
Note *5.A.1.j. does not apply to systems or equipment, specially designed for any of the following:*

a. Marketing purposes;
b. Network Quality of Service (QoS);or
c. Quality of Experience (QoE).

Build and Analyze Flowchart



Market Analysis



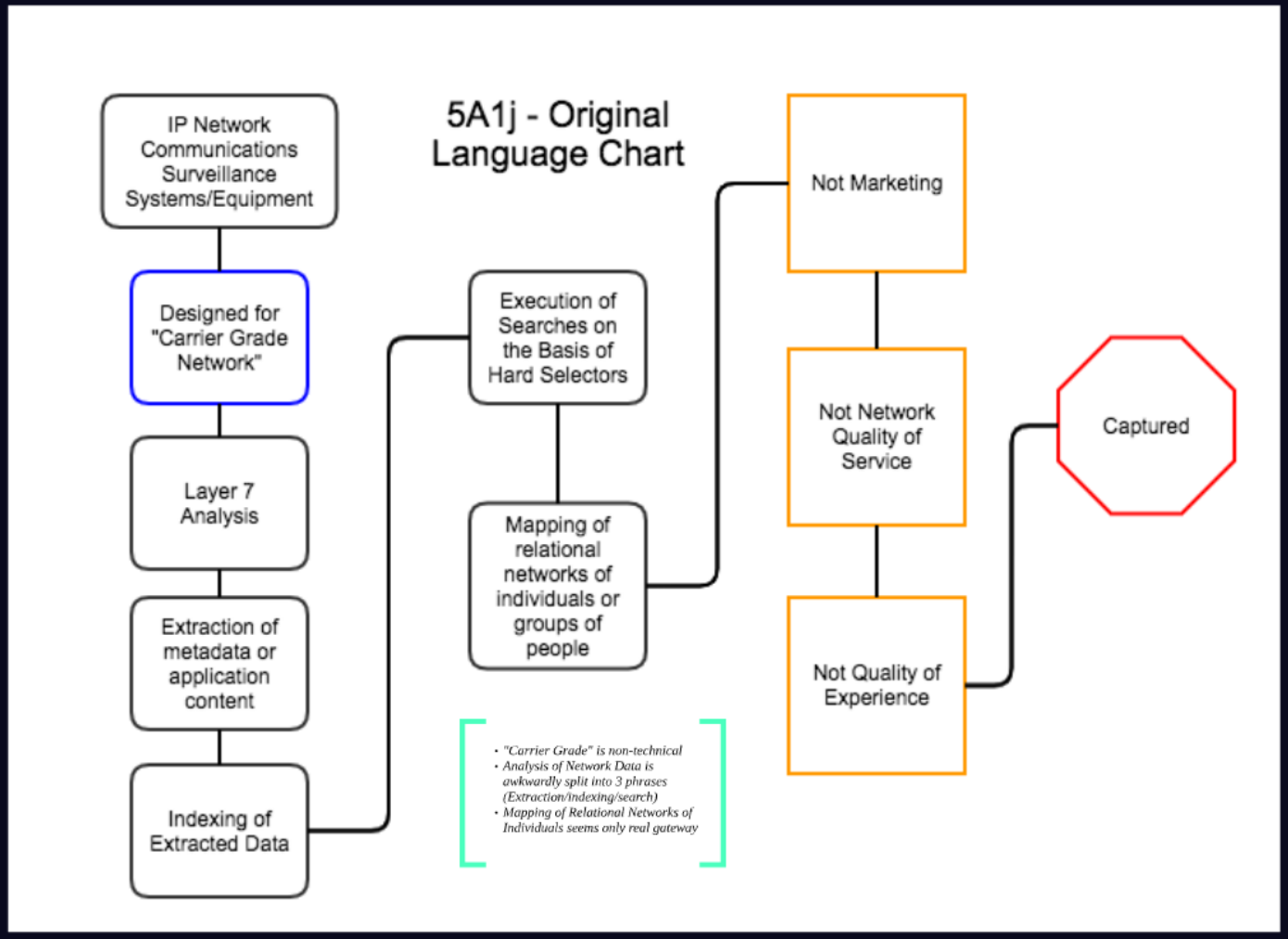
5. A. 1. j. IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:

1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
    a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
    b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
    c. Indexing of extracted data; and
2. Being specially designed to carry out all of the following:
    a. Execution of searches on the basis of "hard selectors"; and
    b. Mapping of the relational network of an individual or of a group of people.

Note *5.A.1.j. does not apply to systems or equipment, specially designed for any of the following:*

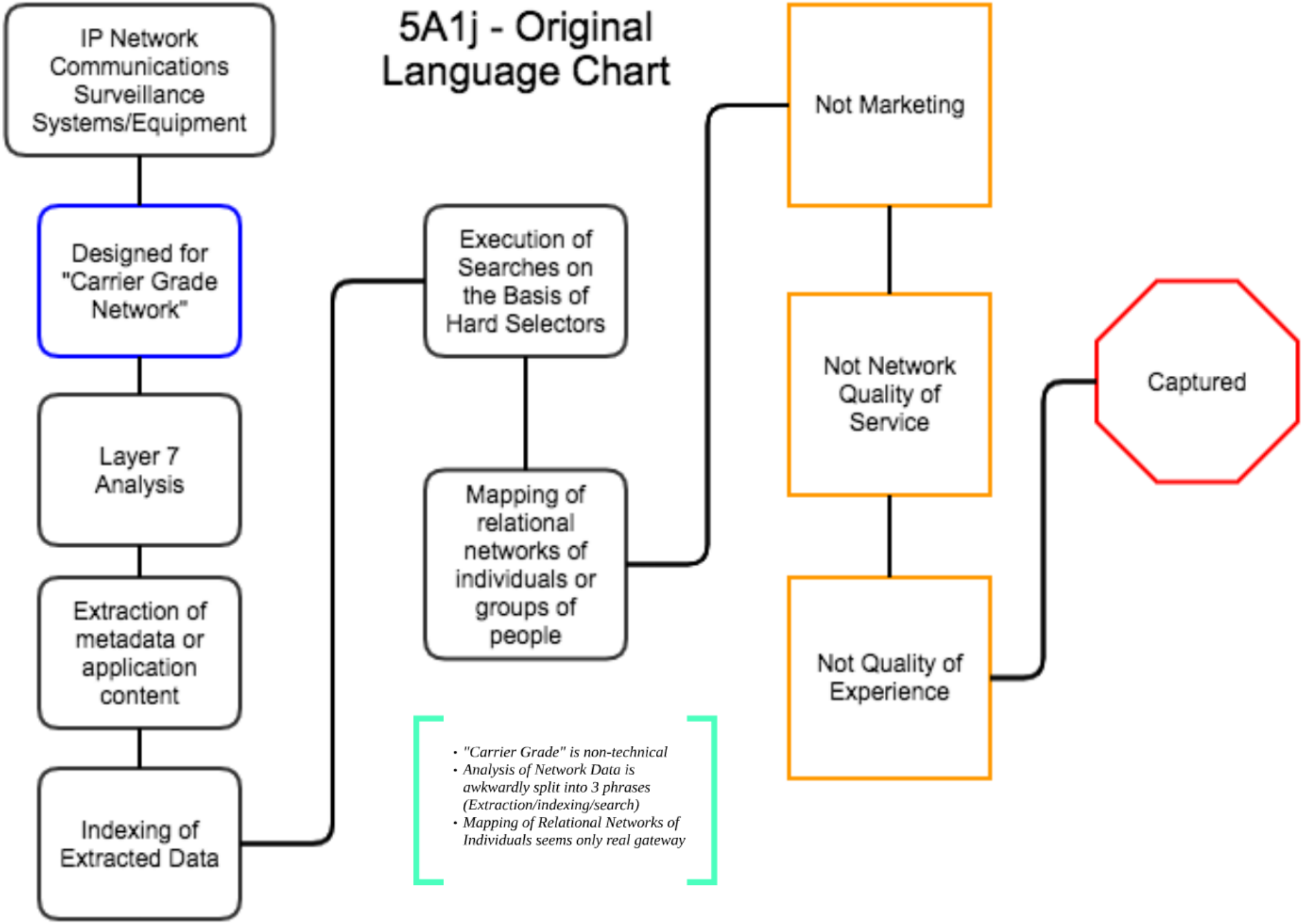
a. Marketing purpose;
b. Network Quality of Service (QoS);or
c. Quality of Experience (QoE).

Build and Analyze Flowchart




Report: Web monitoring devices made by U.S. firm Blue Coat detected in Iran, Sudan

5A1j - Original Language Chart



- *"Carrier Grade" is non-technical*
- *Analysis of Network Data is awkwardly split into 3 phrases (Extraction/indexing/search)*
- *Mapping of Relational Networks of Individuals seems only real gateway*

National Security

Report: Web monitoring devices made by U.S. firm Blue Coat detected in Iran, Sudan

By **Ellen Nakashima**
July 8, 2013

American-made devices used for Internet monitoring have been detected on government and commercial computer networks in Iran and Sudan, in apparent violation of U.S. sanctions that ban the sale of goods, services or technology to the autocratic states, according to new research.

Several of the devices, manufactured by California-based Blue Coat Systems, were also discovered in Syria. Although Blue Coat tools have been identified in Syria in the past, the new research indicates that the government of President Bashar al-Assad has more of the monitoring devices than previously known.

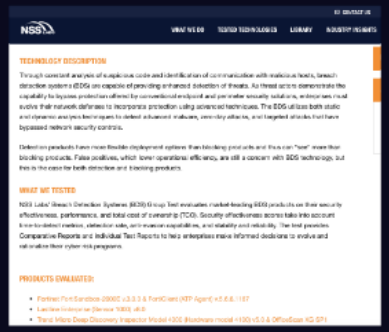
Market Analysis

5a1j Overview of Captures

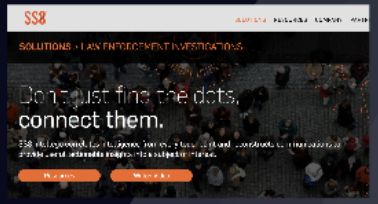
File Edit View Insert Format Data Tools Add-ons Help Last edit was on June 15, 2017

Share

	A	B	C	D	E	F	G	H	I	J	K	
1	Product	Analysis of Layer 7, extraction	"Carrier Grade"	Search on Emails	Mapping of Relational Network	Indexing of Extracted data	Foreign Availabili	Intended Capture	Unintended Capt	CLOSE to Uninte	Intended for "Bre	No
2	[redacted]	Y	Y	Y	y?	Y	N	N	Y	N/A	Y	
3		N	N	Y	Y	Y	N	N	N	Y	Y	
4		Y	Y	Y	Y	Y	N	N	Y	Y	Y	
5		Y	Y	Y	N?	Y	N	N	N	Y	Y	
6		Y	Y	Y	Y?	Y	Y	N	Y	N/A	Y	
7		Y	Y	Y	Y	Y	US/India/Israel (S	Y	N/A	N/A	Y	
8		Y	Y (Has "Big versi	Y	Y	Y	French	Y	N/A	N/A	N	
9		Y	Y	Y	Y	Y	US	?	Y	N/A	Y	
10		N	N	Y	Y	Y	German	Y but not capture	N/A	N/A	Y	
11	olutions	Y	Y?	N?	N?	N?	Indian	Y?	N/A	N/A	N	htt
12	ations	Y	Y	Y	N	?	Israel	?	?	Y?	N	htt
13		Y	Y	Y	Y	Y	Taiwan	Y?	N/A	N/A	Y	htt
14		Y	Y	Y	Y	Y	Turkish	Y?	N/A	N/A	Y	htt
15		Y	Y	Y	N?	Y?	Croatian	Y?	N/A	N/A	N	htt
16		Y	Y?	Y?	Y	Y	Italian	Y?	N/A	N/A	N?	htt
17		Y	Y	Y	Y	Y	Russian	Y?	N/A	N/A	?	htt
18	owned)	y	y	y	y	y	Danish/UK	Y	N/A	N/A	N	htt



When the same companies make two products for different end uses on one technology base it can be an interesting sign



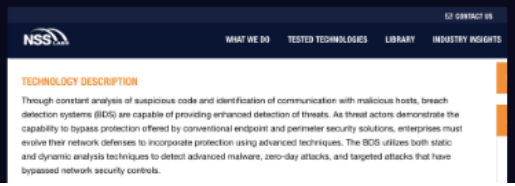
Market Analysis

5a1j Overview of Captures

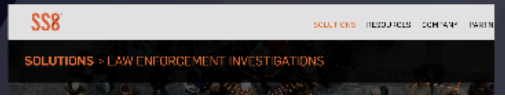
File Edit View Insert Format Data Tools Add-ons Help Last edit was on June 15, 2017

Share

	A	B	C	D	E	F	G	H	I	J	K
1	Product	Analysis of Layer 7, extraction	"Carrier Grade"	Search on Emails	Mapping of Relational Network	Indexing of Extracted data	Foreign Availabili	Intended Capture	Unintended Capt	CLOSE to Uninte	Intended for "Bre
2	[redacted]	Y	Y	Y	y?	Y	N	N	Y	N/A	Y
3		N	N	Y	Y	Y	N	N	N	Y	Y
4		Y	Y	Y	Y	Y	N	N	Y	Y	Y
5		Y	Y	Y	N?	Y	N	N	N	Y	Y
6		Y	Y	Y	Y?	Y	Y	N	Y	N/A	Y
7		Y	Y	Y	Y	Y	US/India/Israel ($	Y	N/A	N/A	Y
8		Y	Y (Has "Big versi	Y	Y	Y	French	Y	N/A	N/A	N
9		Y	Y	Y	Y	Y	US	?	Y	N/A	Y
10		N	N	Y	Y	Y	German	Y but not capture	N/A	N/A	Y
11	olutions	Y	Y?	N?	N?	N?	Indian	Y?	N/A	N/A	N
12	ations	Y	Y	Y	N	?	Israel	?	?	Y?	N
13		Y	Y	Y	Y	Y	Taiwan	Y?	N/A	N/A	Y
14		Y	Y	Y	Y	Y	Turkish	Y?	N/A	N/A	Y
15		Y	Y	Y	N?	Y?	Croatian	Y?	N/A	N/A	N
16		Y	Y?	Y?	Y	Y	Italian	Y?	N/A	N/A	N?
17		Y	Y	Y	Y	Y	Russian	Y?	N/A	N/A	?
18	owned)	y	y	y	y	y	Danish/UK	Y	N/A	N/A	N



When the same companies make two products for different end uses on one technology base it can be an interesting sign



TECHNOLOGY DESCRIPTION

Through constant analysis of suspicious code and identification of communication with malicious hosts, breach detection systems (BDS) are capable of providing enhanced detection of threats. As threat actors demonstrate the capability to bypass protection offered by conventional endpoint and perimeter security solutions, enterprises must evolve their network defenses to incorporate protection using advanced techniques. The BDS utilizes both static and dynamic analysis techniques to detect advanced malware, zero-day attacks, and targeted attacks that have bypassed network security controls.

Detection products have more flexible deployment options than blocking products and thus can "see" more than blocking products. False positives, which lower operational efficiency, are still a concern with BDS technology, but this is the case for both detection and blocking products.

WHAT WE TESTED

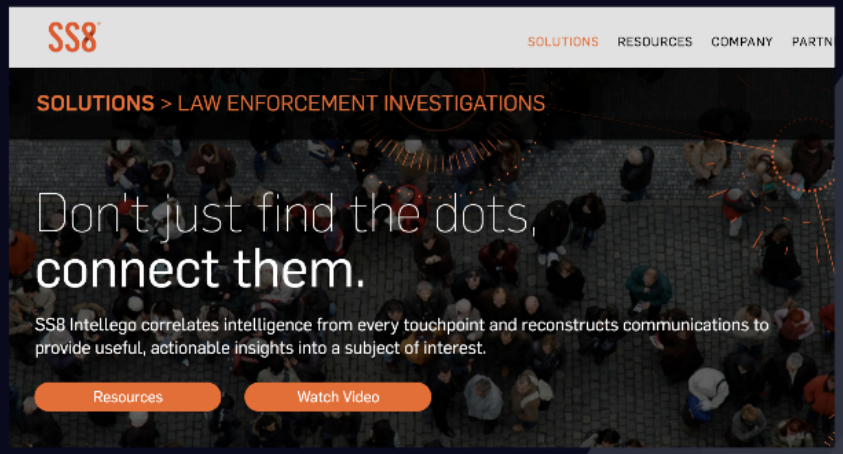
NSS Labs' Breach Detection Systems (BDS) Group Test evaluates market-leading BDS products on their security effectiveness, performance, and total cost of ownership (TCO). Security effectiveness scores take into account time-to-detect metrics, detection rate, anti-evasion capabilities, and stability and reliability. The test provides Comparative Reports and individual Test Reports to help enterprises make informed decisions to evolve and rationalize their cyber risk programs.

PRODUCTS EVALUATED:

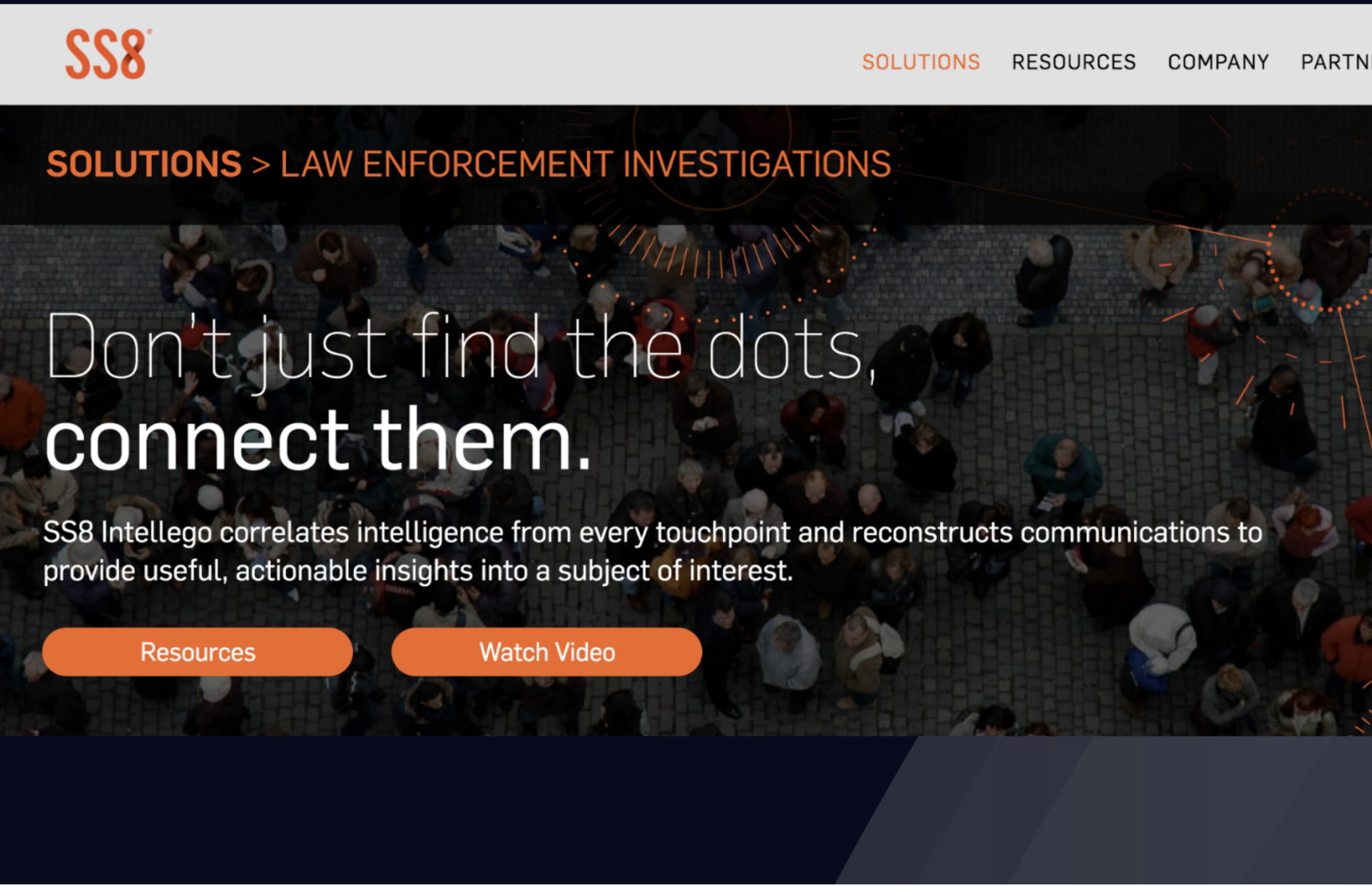
- Fortinet FortiSandbox-2000E v.3.0.0 & FortiClient (ATP Agent) v.5.6.6.1167
- Lastline Enterprise (Sensor 1000) v8.0
- Trend Micro Deep Discovery Inspector Model 4000 (Hardware model 4100) v5.0 & OfficeScan XG SP1

	Y	Russian	Y?	N/A	N/A	?	http
	y	Danish/UK	Y	N/A	N/A	N	http

When the same companies make two products for different end uses on one technology base it can be an interesting sign



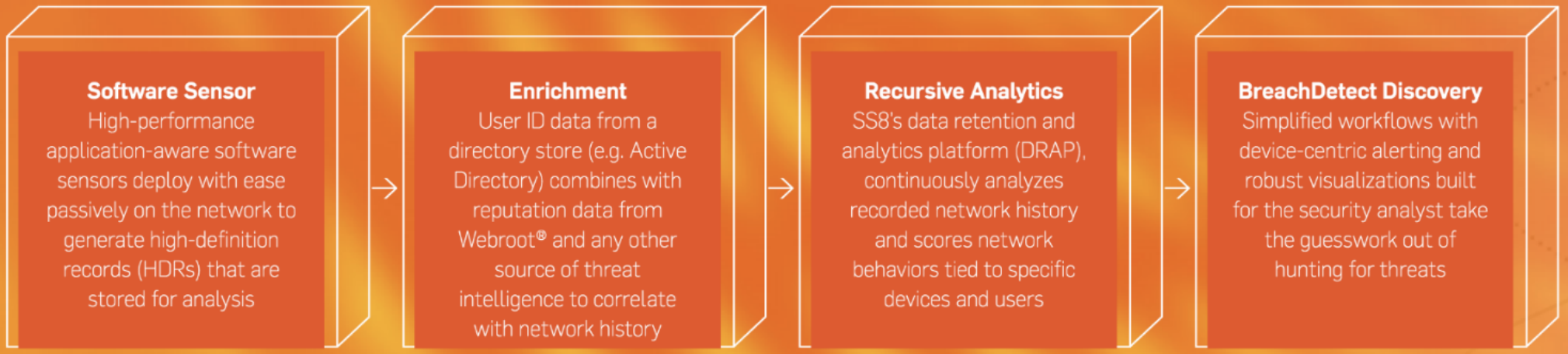
ne technology base it can



be an interesting sig

Advanced Threat Detection

SS8 BreachDetect provides device-centric alerting and powerful network investigation capabilities that accelerates threat detection times and reduces or eliminates threat dwell time.



Emerging Controls on AI

ECCN 0D521 No. 1

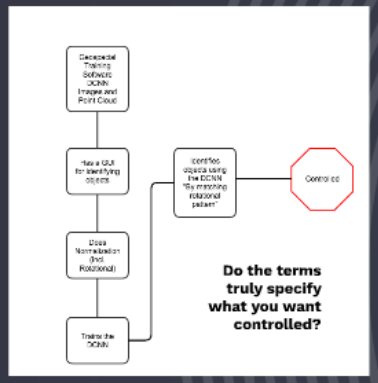
Geospatial imagery "software" "specially designed" for training a Deep Convolutional Neural Network to automate the analysis of geospatial imagery and point clouds, and having all of the following:

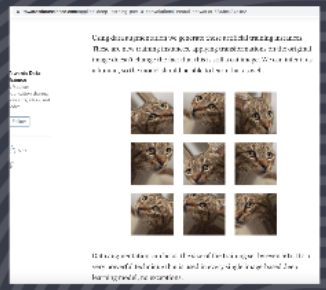
1. Provides a graphical user interface that enables the user to identify objects (*e.g.*, vehicles, houses, etc.) from within geospatial imagery and point clouds in order to extract positive and negative samples of an object of interest;

2. Reduces pixel variation by performing scale, color, and rotational normalization on the positive samples;

3. Trains a Deep Convolutional Neural Network to detect the object of interest from the positive and negative samples; and

4. Identifies objects in geospatial imagery using the trained Deep Convolutional Neural Network by matching the rotational pattern from the positive samples with the rotational pattern of objects in the geospatial imagery.





ECCN 0D521 No. 1

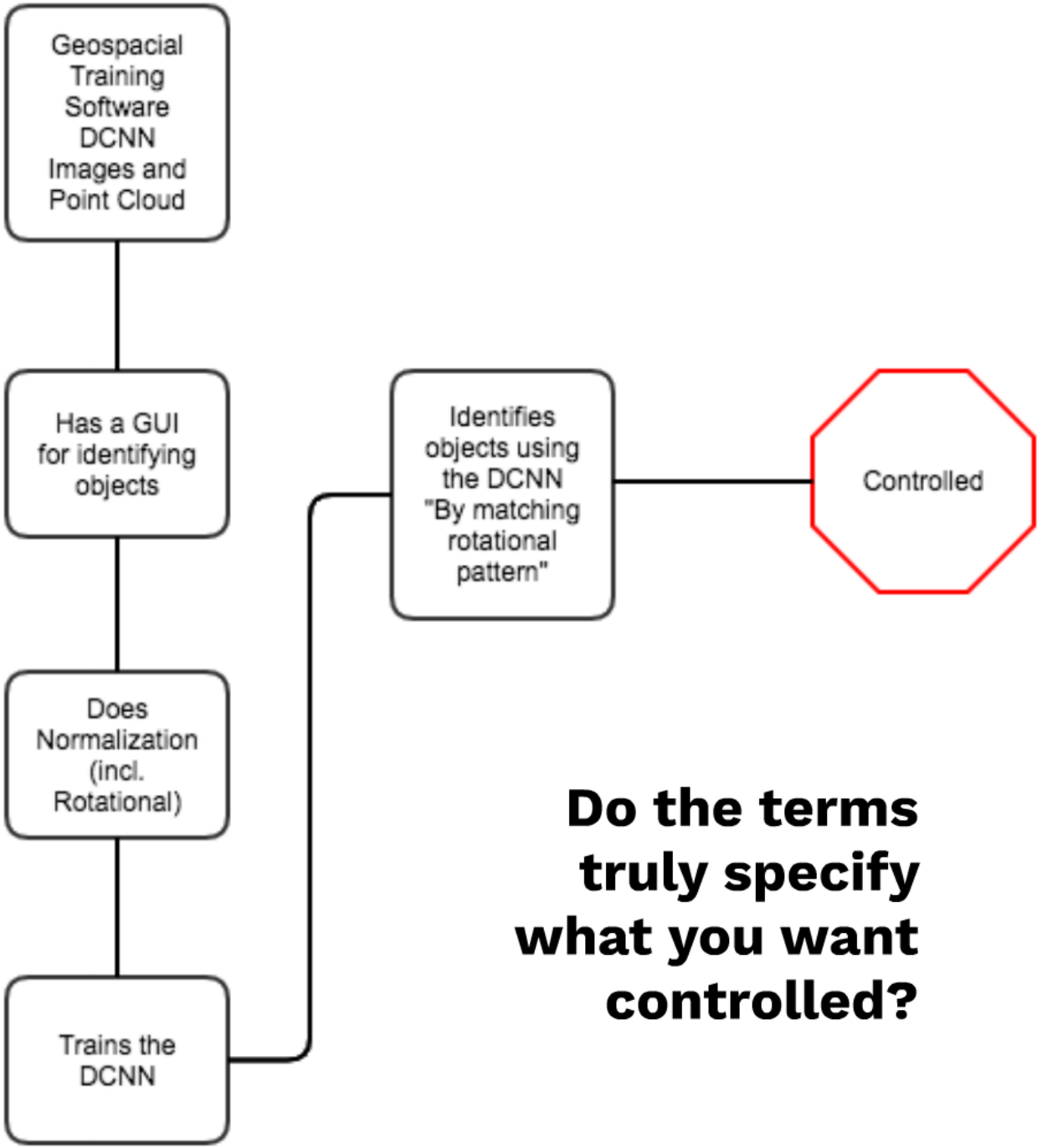
Geospatial imagery "software" "specially designed" for training a Deep Convolutional Neural Network to automate the analysis of geospatial imagery and point clouds, and having all of the following:

1. Provides a graphical user interface that enables the user to identify objects (*e.g.*, vehicles, houses, etc.) from within geospatial imagery and point clouds in order to extract positive and negative samples of an object of interest;

2. Reduces pixel variation by performing scale, color, and rotational normalization on the positive samples;

3. Trains a Deep Convolutional Neural Network to detect the object of interest from the positive and negative samples; and

4. Identifies objects in geospatial imagery using the trained Deep Convolutional Neural Network by matching the rotational pattern from the positive samples with the rotational pattern of objects in the geospatial imagery.



Do the terms truly specify what you want controlled?

Using data augmentation we generate these artificial training instances. These are new training instances, applying transformations on the original image doesn't change the fact that this is still a cat image. We can infer it as a human, so the model should be able to learn that as well.

Data augmentation can boost the size of the training set by even 50x. It's a very powerful technique that is used in every single image-based deep learning model, no exceptions.

Image Processing | Artificial Neural Networks | Computer Science

Can we make an image recognition system that is (rotation, scale, brightness, saturation) Invariant?

2 Answers

Chomba Bupe, knows about image processing.
Answered Feb 26, 2016 · Author has **1.1k** answers and **3.9m** answer views

Of course, it can be achieved by several techniques such as SIFT, SURF or the ConvNets.

But it's interesting to note that transfer learning is the best approach to achieve reliable invariant recognition systems.

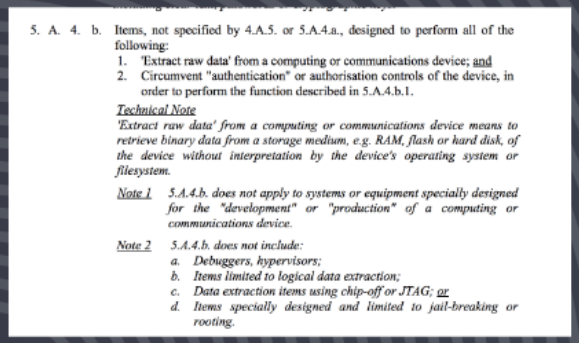
For example I teach a recognition system to recognize object A, lets assume there is limited training data for object A so that the system is incapable of generalizing well after training. Now the same system is also taught to recognize object B but this time around there is enough data for object B.

Ofir Nachum, I work on ML at Google Brain
Answered Feb 26, 2016 · Upvoted by Alberto Bietti, PhD student in machine learning. Former ML engineer

Yes, there are generally three ways to do this (in the context of ML-based systems like convolutional neural nets):

- **Preprocess the input data to enforce uniform measures.** For example, normalize the pixel values to have mean 0 and standard deviation 1. Or, if you can figure out what the image is rotated by, undo the rotation before you pass it in to your classifier.
- **Augment your training data with random transformations.** You can create new training data by taking your existing data and applying random rotations.

Forensics Tools



5. A. 4. b. Items, not specified by 4.A.5. or 5.A.4.a., designed to perform all of the following:
   1. 'Extract raw data' from a computing or communications device; and
   2. Circumvent "authentication" or authorisation controls of the device, in order to perform the function described in 5.A.4.b.1.

Technical Note

'Extract raw data' from a computing or communications device means to retrieve binary data from a storage medium, e.g. RAM, flash or hard disk, of the device without interpretation by the device's operating system or filesystem.

Note 1 *5.A.4.b. does not apply to systems or equipment specially designed for the "development" or "production" of a computing or communications device.*

Note 2 *5.A.4.b. does not include:*
   a. Debuggers, hypervisors;
   b. Items limited to logical data extraction;
   c. Data extraction items using chip-off or JTAG; or
   d. Items specially designed and limited to jail-breaking or rooting.

Ask yourself: What is rooting and what is jailbraking and is that technology different?

5. A. 4. b. Items, not specified by 4.A.5. or 5.A.4.a., designed to perform all of the following:

1. 'Extract raw data' from a computing or communications device; and
2. Circumvent "authentication" or authorisation controls of the device, in order to perform the function described in 5.A.4.b.1.

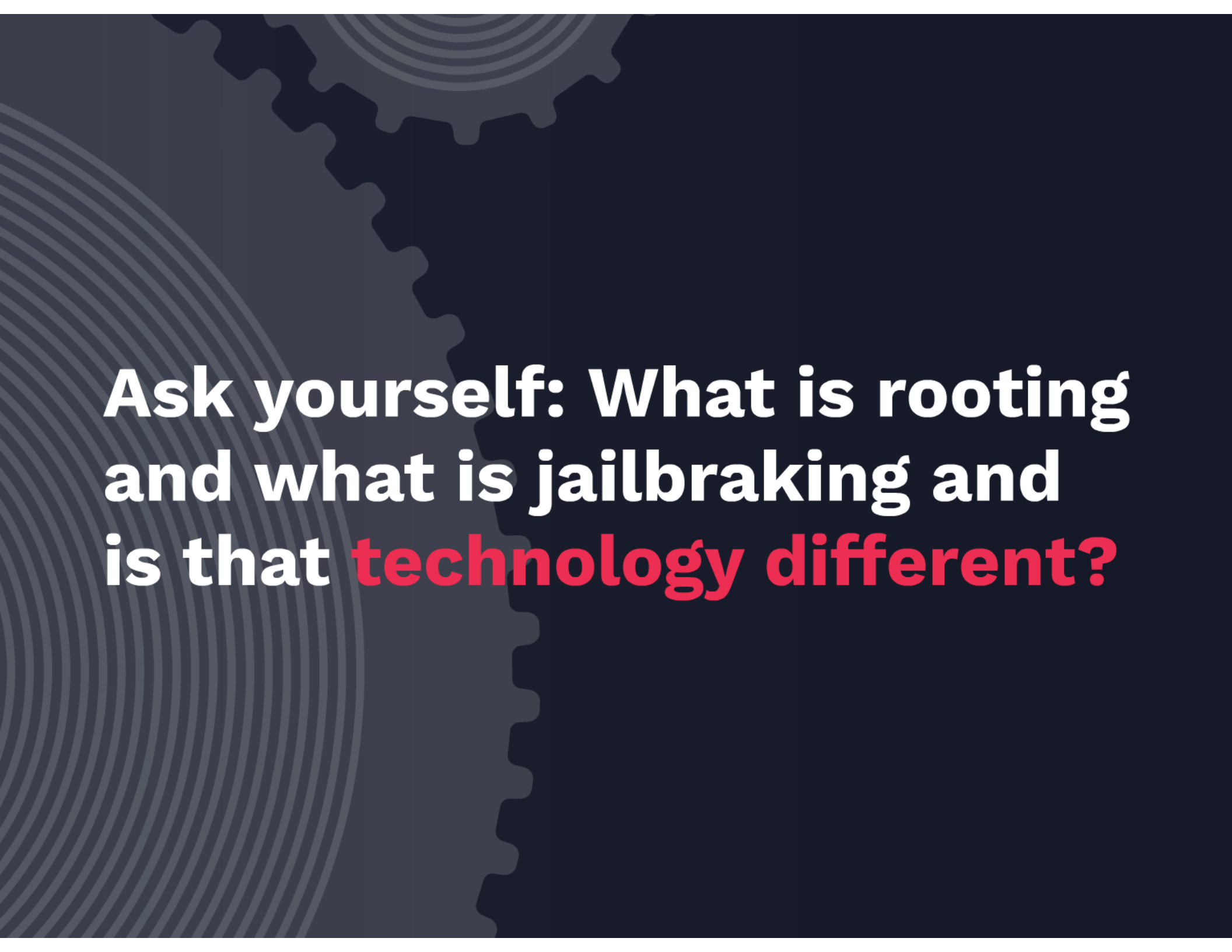
Technical Note

'Extract raw data' from a computing or communications device means to retrieve binary data from a storage medium, e.g. RAM, flash or hard disk, of the device without interpretation by the device's operating system or filesystem.

Note 1 *5.A.4.b. does not apply to systems or equipment specially designed for the "development" or "production" of a computing or communications device.*

Note 2 *5.A.4.b. does not include:*

a. Debuggers, hypervisors;
b. Items limited to logical data extraction;
c. Data extraction items using chip-off or JTAG; or
d. Items specially designed and limited to jail-breaking or rooting.


Ask yourself: What is rooting and what is jailbraking and is that technology different?

Conclusion: We need to revisit our process

Giving up on performance charactaristics or defining products by technical specifications means giving up on technology control itself

We've also largely given up on international uniformity in purpose and action

Giving up on performance charactaristics or defining products by technical specifications means giving up on technology control itself

We've also largely given up on international uniformity in purpose and action