“AMP like an accelerator to successful cybersecurity strategy”

"A false sense of security is worse than a true sense of insecurity"

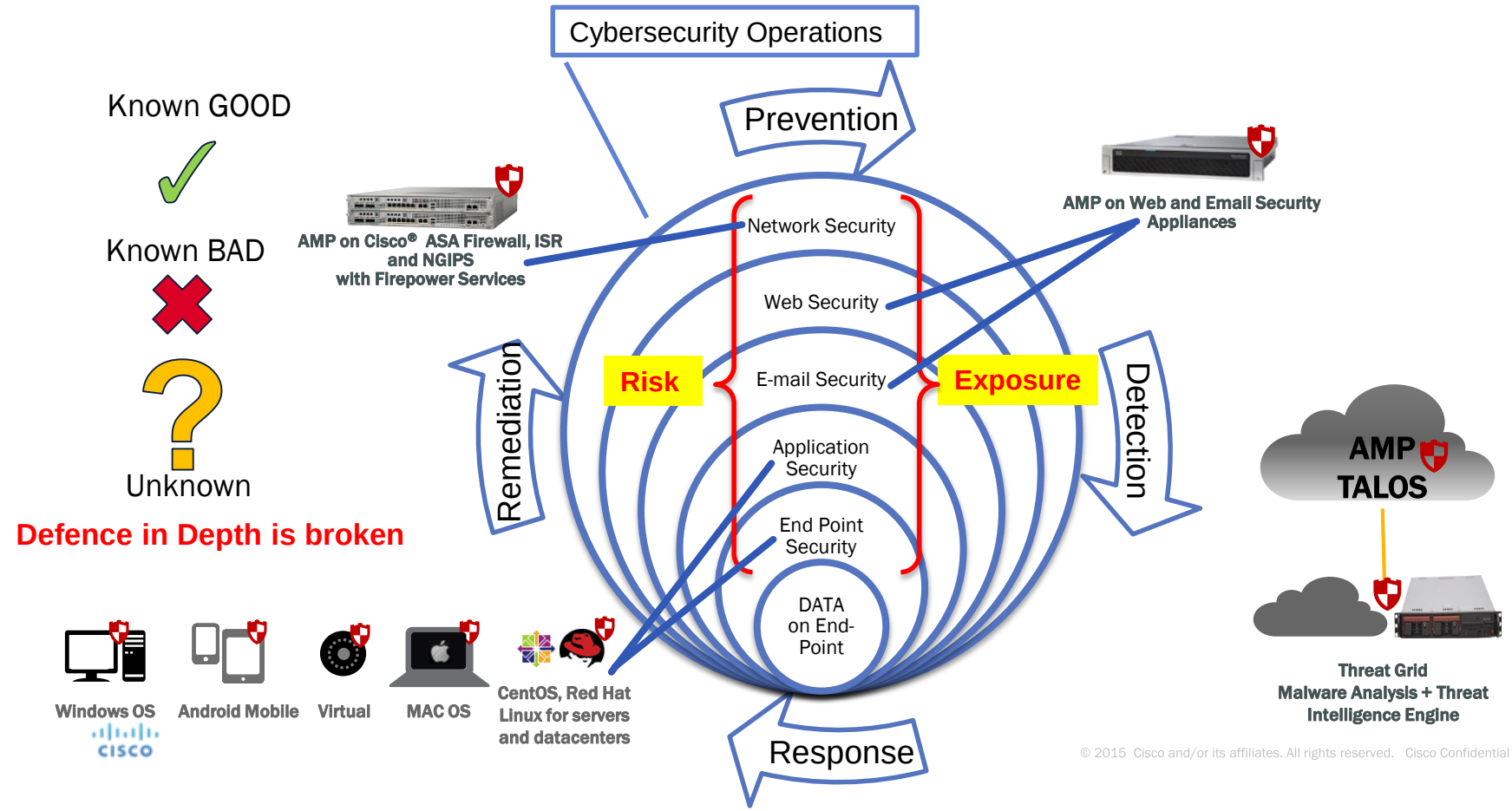
Senad Aruc

Consulting Systems Engineer -
Advanced Threats Group

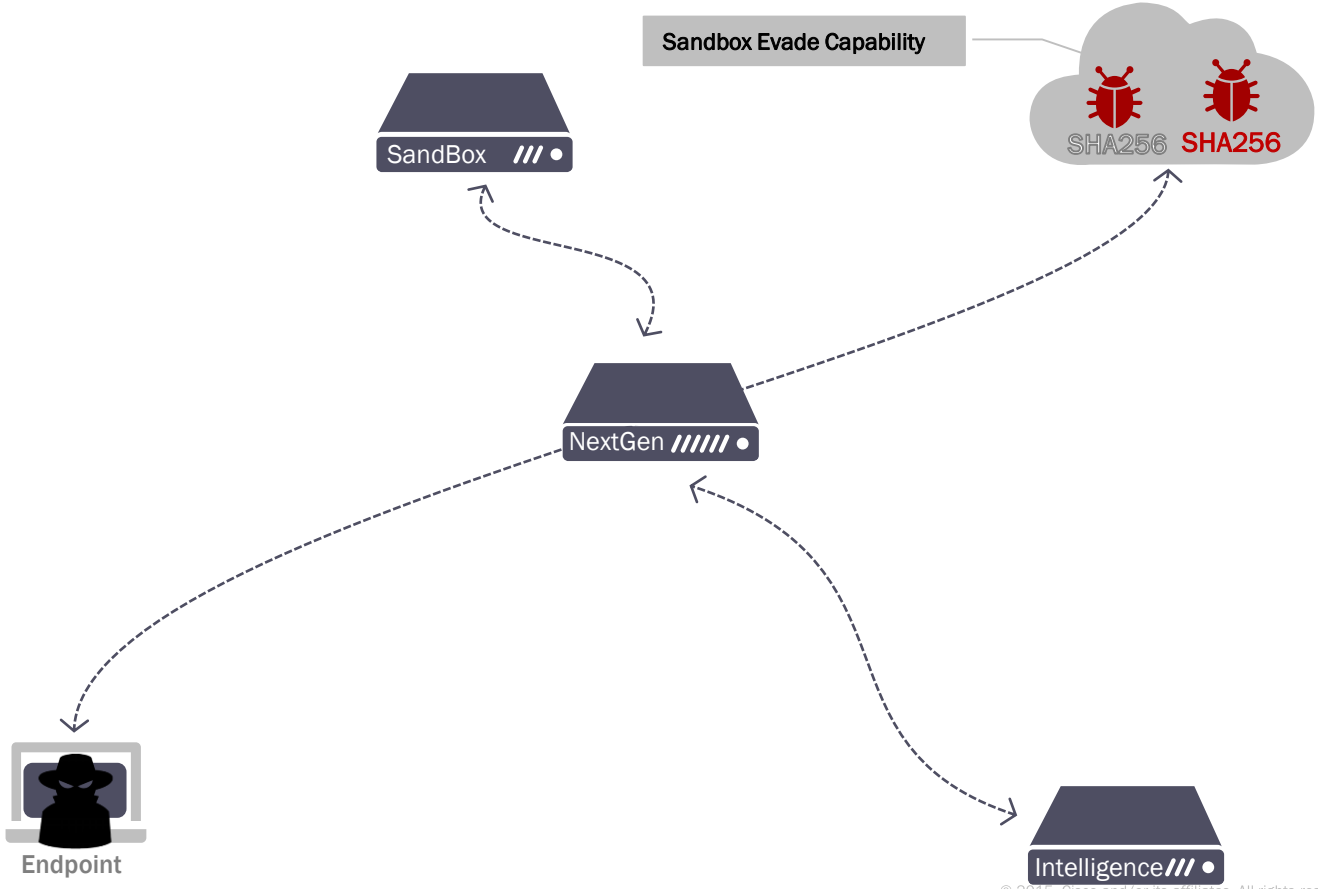
Nils Roald
Advanced Threats - North Sales Leader

Daily Mail

Cybersecurity operations best practice - defence in depth

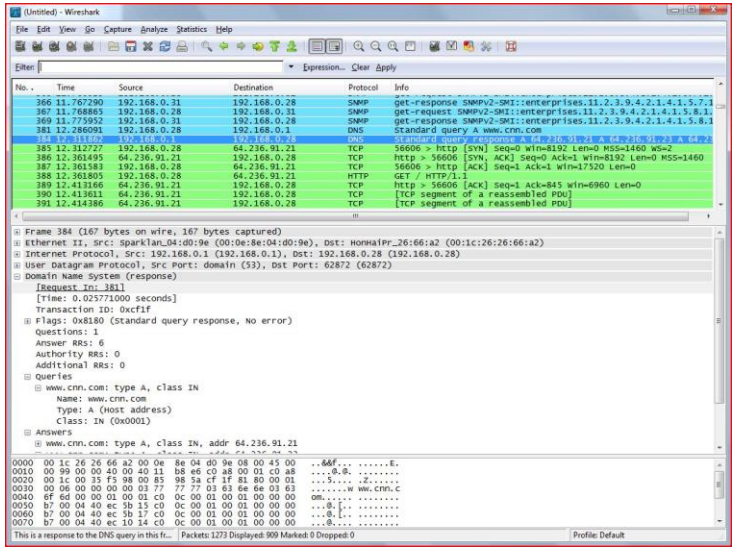


Cybersecurity problems (not the BOB and ALICE story anymore!)



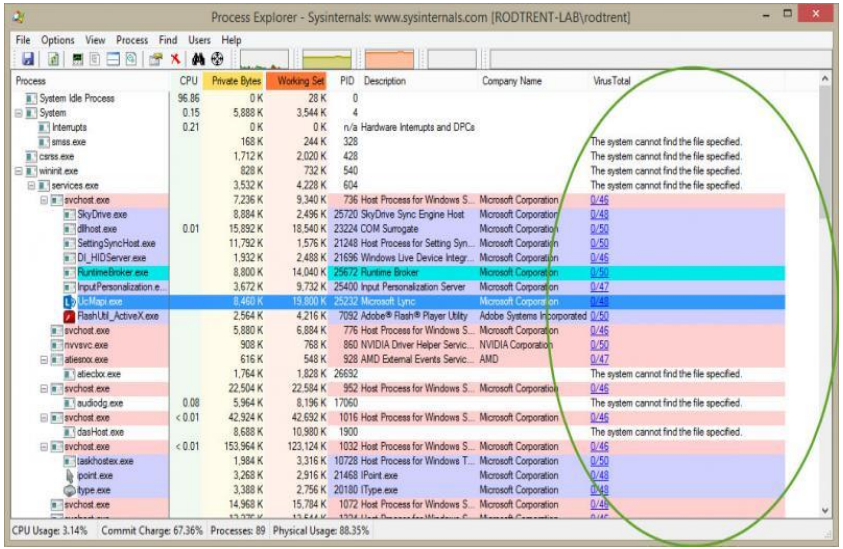
Malware on wire is not a real malware!

Malware on the wire

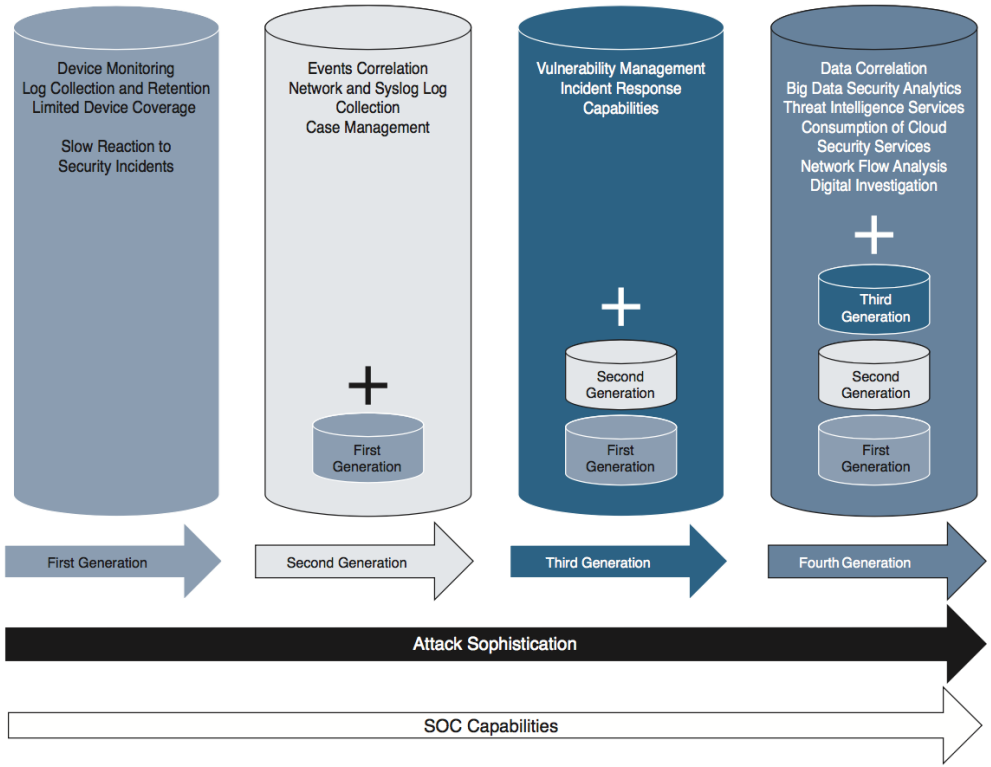


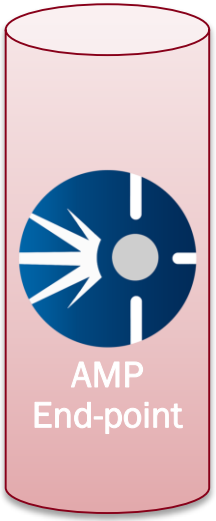
or

Malware on the endpoint



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



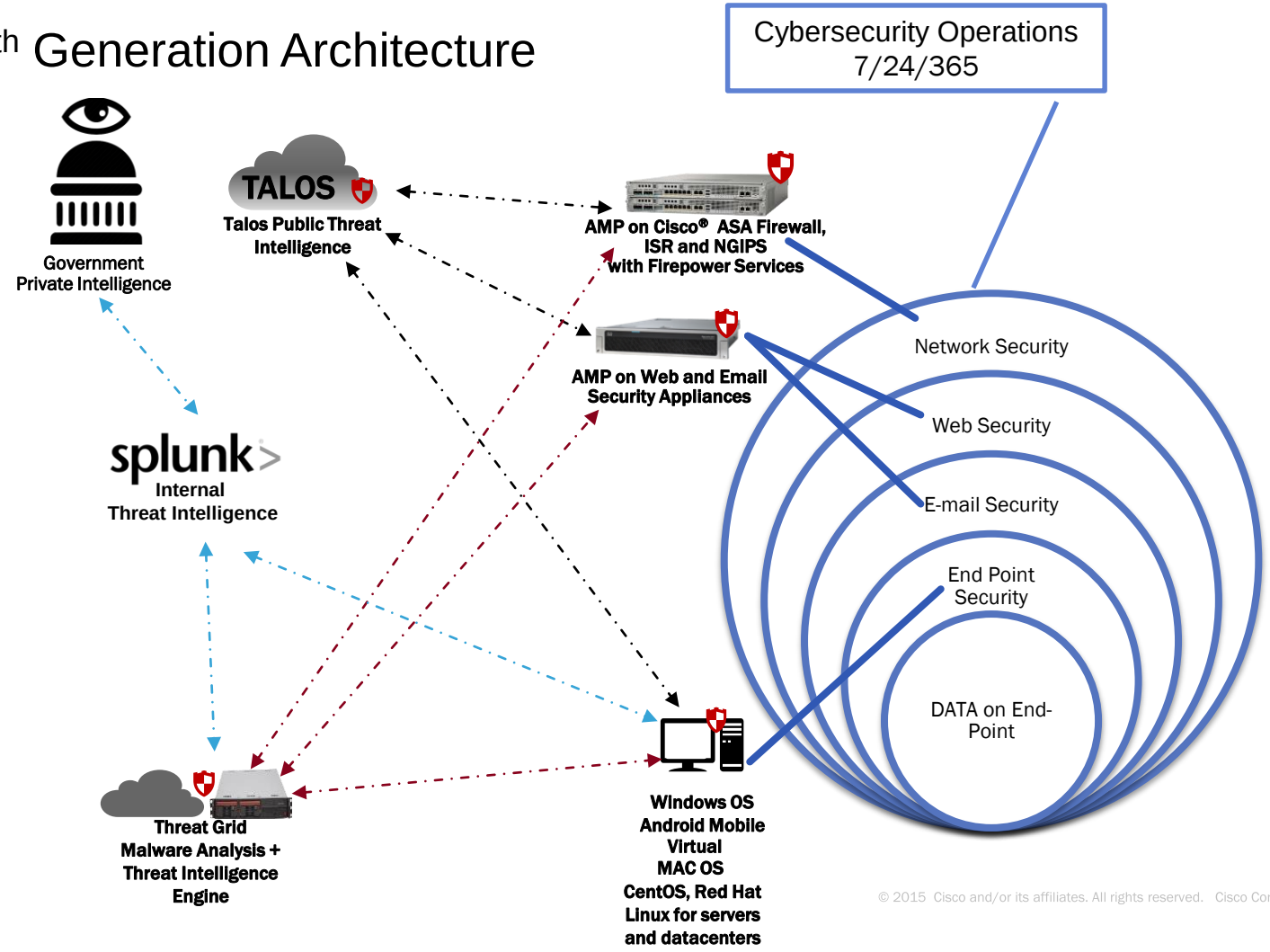


Accelerate incident response

See once, block everywhere

Make the unknown, known

CSOC 4.5th Generation Architecture



Accelerate incident response with AMP

Malware Alert → Search in the SIEM → Verify the infection → Open a ticket to IT → User is in PTO → Full disk forensics → Find the malware → Format the device → Deliver to the user

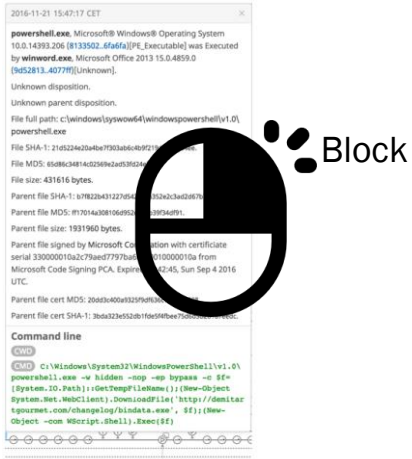
Full disk forensics for malware?

Old School

Why you need a full disk forensics?

?

...when AMP can do a process level forensics



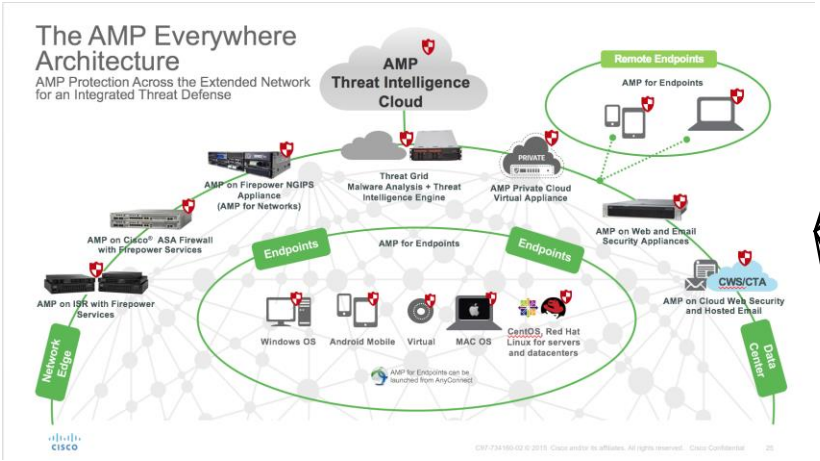
AMP

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.

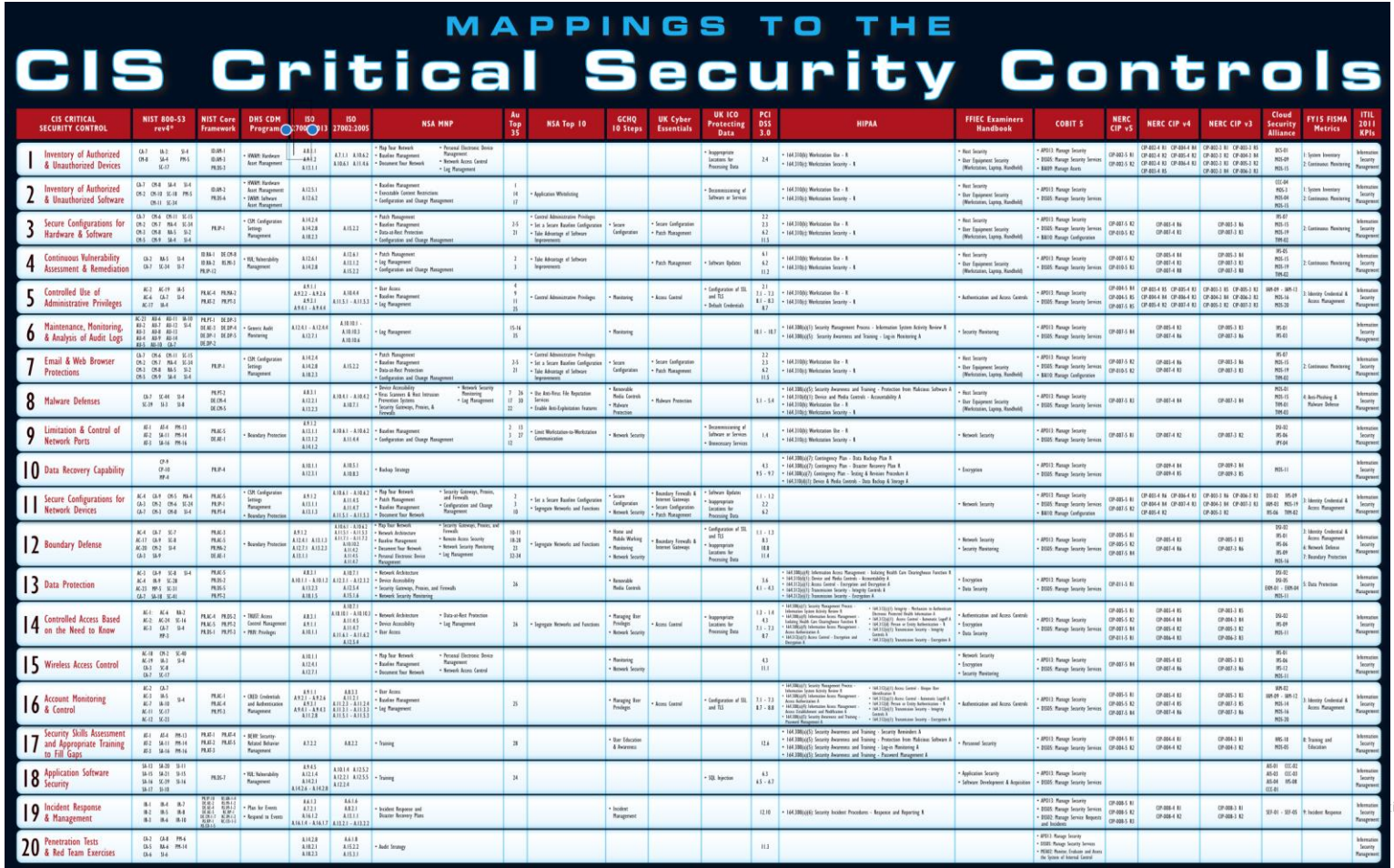
Critical cybersecurity controls NIST 2014



CIS Critical Security Controls (V6.0)

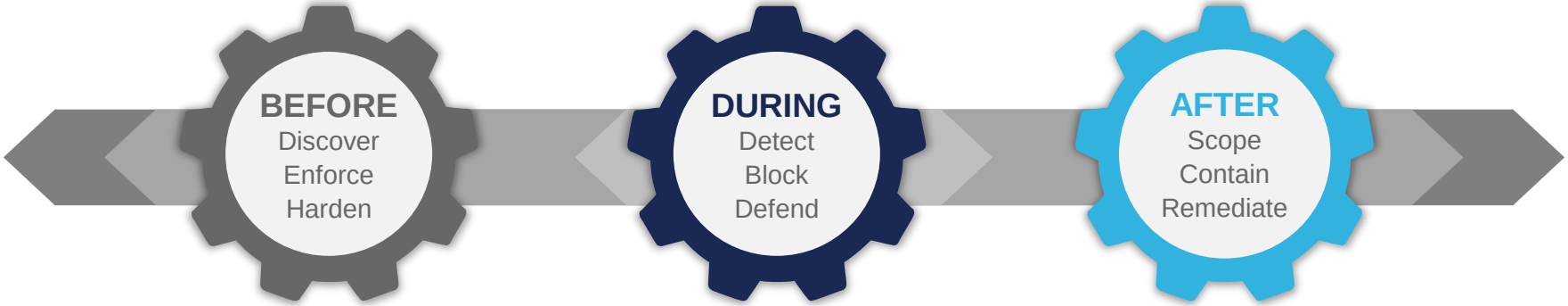
1 Inventory of Authorized and Unauthorized Devices
2 Inventory of Authorized and Unauthorized Software
3 Secure Configuration of End-User Devices
4 Continuous Vulnerability Assessment & Remediation
5 Controlled Use of Administrative Privileges
6 Maintenance, Monitoring, and Analysis of Audit Logs
7 Email 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



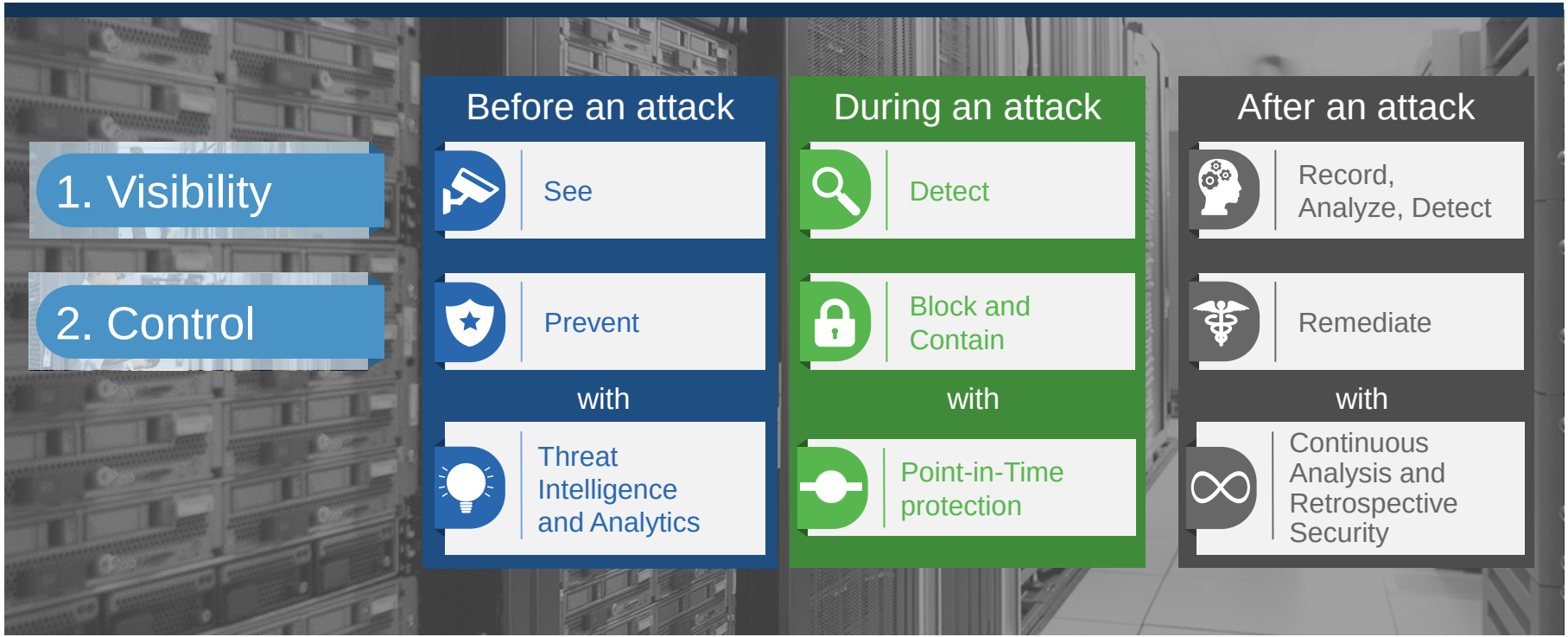
CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27001:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
1 Inventory of Authorized & Unauthorized Devices	CA-7 CM-8 | IA-3 SA-4 SC-17 | PM-5	ID.AM-1 ID.AM-3 PR.DS-3	• VMWR: Hardware Asset Management	A.8.1.1 A.8.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.3 A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personnel Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstations, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI09: Manage Assets	CIP-002-5 R1 CIP-002-5 R2	CIP-002-4 R1 CIP-002-4 R2 CIP-003-4 R5 CIP-004-4 R2 CIP-005-4 R2 CIP-007-4 R5	CIP-002-3 R1 CIP-002-3 R2 CIP-002-3 R3 CIP-003-3 R4 CIP-004-3 R2 CIP-005-3 R2 CIP-006-3 R2	DCS-01 MOS-09 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 CM-10 SI-18 CM-11 SI-34	ID.AM-1 ID.AM-2 PR.DS-6	• VMWR: Hardware Asset Management • VMWR: Software Asset Management	A.12.5.1 A.12.6.2	• Baseline Management • Executable Content Restrictions • Configuration and Change Management	• Application Whitelisting	1 14 17				• Decommissioning of Software or Services		• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstations, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services				CCC-04 MOS-1 MOS-04 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
3 Secure Configurations for Hardware & Software	CA-7 CM-6 CM-9 SI-13 CM-2 CM-7 MA-4 SI-34 CM-3 CM-8 MA-5 SI-2 CM-5 CM-9 SA-8 SI-4	PR.IP-1	• CSM: Configuration Setting Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	3-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.3	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstations, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R3	CIP-003-3 R6 CIP-007-3 R3	MS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
4 Continuous Vulnerability Assessment & Remediation	CA-2 CA-7 RA-5 SC-34 SI-4 SI-7	ID.RA-1 ID.RA-2 PR.IP-12	DE.CM-8 RS.MI-3	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstations, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R2 CIP-010-5 R2	CIP-005-4 R4 CIP-007-4 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8	MS-05 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
5 Controlled Use of Administrative Privileges	AC-2 AC-6 AC-17 AC-19 CA-7 IA-4 IA-5 SA-4	PR.AC-4 PR.AC-6 PR.PT-2	PR.NA-2 PR.PT-3	A.9.1.1 A.9.2.2 A.9.2.3 A.9.4.1 A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 25	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	2.1 2.1 - 2.2 8.1 - 8.3 8.7	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R4 CIP-005-5 R1 CIP-007-5 R5	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-007-4 R5	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-007-3 R5	IAM-09 - IAM-12 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
6 Maintenance, Monitoring, & Analysis of Audit Logs	AC-2 AU-4 AU-11 SA-10 AU-2 AU-7 AU-12 SI-4 AU-3 AU-8 AU-13 AU-6 AU-9 AU-14 AU-7 AU-10 AU-16	PR.PT-1 DE.AE-3 DE.CM-1 DE.CM-4 DE.DP-1 DE.DP-5 DE.DP-2	• Generic Audit Monitoring	A.12.4.1 - A.12.4.4 A.12.7.1	A.10.10.1 - A.10.10.3 A.10.10.6	• Log Management	15-16 35		• Monitoring			10.1 - 10.7	• 164.308(a)(1) Security Management Process – Information System Activity Review R • 164.308(a)(5) Security Awareness and Training – Log-in Monitoring A	• Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-007-4 R5 CIP-007-4 R6	CIP-007-3 R6 CIP-007-3 R6	MS-01 MS-03		Information Security Management
7 Email & Web Browser Protections	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 MA-5 SI-2 CM-5 CM-9 SA-8 SI-4	PR.IP-1	• CSM: Configuration Setting Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	3-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.3	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstations, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-007-4 R6 CIP-007-4 R3	CIP-007-3 R6 CIP-007-3 R3	MS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
8 Malware Defenses	CA-7 SC-44 SI-4 SI-39 SI-3	PR.PT-2 DE.CM-4 DE.CM-5		A.8.3.1 A.12.2.1 A.12.2.2	A.10.4.1 - A.10.4.2 A.10.7.1	• Device Accessibility • Virus Scanners & Host Intrusion Prevention Systems • Network Security Monitoring • Log Management	7 26 17 10 22	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	• Removable Media Controls • Malware Protection	• Malware Protection		5.1 - 5.4	• 164.308(a)(5) Security Awareness and Training – Protection from Malicious Software A • 164.310(d)(1) Device and Media Controls – Accountability A • 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Host Security • User Equipment Security (Workstations, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R3	CIP-007-4 R4	CIP-007-3 R4	MOS-01 MOS-15 MOS-19 TVM-01 TVM-03	4: Anti-Phishing & Malware Defense	Information Security Management
9 Limitation & Control of Network Ports	AU-1 AU-2 AU-6 CM-1 CM-3 CM-6 PM-6 PM-14 SA-11 SA-14	PR.AC-5 DE.AE-1	• Boundary Protection	A.9.1.2 A.12.5.1 A.13.1.2 A.14.1.2	A.10.6.1 - A.10.6.2 A.11.4.4	• Baseline Management • Configuration and Change Management	2 13 3 27 15	• Limit Workstation-to-Workstation Communication	• Network Security		• Decommissioning of Software or Services • Unnecessary Services	1.4	• 164.310(b) Workstation Use – R • 164.310(c) Workstation Security – R	• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R1	CIP-007-4 R2	CIP-007-3 R2	DSI-03 MS-06 IPY-04		Information Security Management
10 Data Recovery Capability		CP-9 CP-10 RP-4	PR.IP-4	A.10.1.1 A.12.3.1	A.10.5.1 A.10.8.3	• Backup Strategy						4.3 9.5 - 9.7	• 164.308(a)(7) Contingency Plan – Data Backup Plan R • 164.308(a)(7) Contingency Plan – Disaster Recovery Plan R • 164.308(a)(7) Contingency Plan – Testing & Revision Procedure A • 164.310(d)(1) Device & Media Controls – Data Backup & Storage A	• Encryption	• APO13: Manage Security • DSS05: Manage Security Services		CIP-009-4 R4 CIP-009-4 R5	CIP-009-3 R4 CIP-009-3 R5	MOS-11		Information Security Management
11 Secure Configurations for Network Devices	AC-4 CA-7 CA-3 CM-2 CA-7 CM-3 CM-6 CM-9 CM-8 SC-34 SI-4	PR.AC-5 PR.IP-1 PR.PT-4	• CSM: Configuration Setting Management • Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.3	A.10.6.1 - A.10.6.2 A.11.4.5 A.11.4.7 A.11.5.1 - A.11.5.3	• Map Your Network • Network Architecture • Baseline Management • Document Your Network • Security Gateways, Proxies, and Firewalls • Configuration and Change Management	2 3 10	• Set a Secure Baseline Configuration • Segregate Networks and Functions	• Secure Configurations • Network Security	• Boundary Firewalls & Internet Gateways • Secure Configuration • Patch Management	• Software Updates • Inappropriate Locations for Processing Data	1.1 - 1.2 2.2 6.2	• Network Security	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-005-5 R1 CIP-007-5 R2	CIP-005-4 R4 CIP-006-4 R2 CIP-007-4 R4 CIP-005-4 R2	CIP-003-3 R4 CIP-004-3 R4 CIP-007-3 R3 CIP-005-3 R2	IVS-03 IAM-03 MOS-03 MOS-04	IVS-09 MOS-19 TVM-02	3: Identity Credential & Access Management	Information Security Management
12 Boundary Defense	AC-4 CA-7 AC-17 CA-9 AC-20 CP-2 CA-3 IA-9	SC-7 SC-8 SI-4	PR.AC-3 PR.AC-5 PR.PM-7 DE.AE-1	• Boundary Protection	A.9.1.2 A.12.4.1 A.12.7.1 A.13.1.1	A.13.1.3 A.13.2.3	A.10.6.1 - A.10.6.2 A.11.5.1 - A.11.5.3 A.11.7.1 - A.11.7.2 A.10.10.2 A.11.4.2 A.11.4.5 A.11.4.7	• Map Your Network • Network Architecture • Baseline Management • Document Your Network • Personal Electronic Device Management • Security Gateways, Proxies, and Firewalls • Remote Access Security • Network Security Monitoring • Log Management	10-11 18-20 23 22-24	• Segregate Networks and Functions	• Home and Mobile Working • Monitoring • Network Security	• Boundary Firewalls & Internet Gateways	• Configuration of SSL and TLS • Inappropriate Locations for Processing Data	1.1 - 1.3 8.1 10.8 11.4	• Network Security • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R1 CIP-007-4 R6	CIP-005-3 R1 CIP-007-3 R6	DSI-02 MS-01 MS-06 MOS-16	3: Identity Credential & Access Management 4: Network Defense 7: Boundary Protection	Information Security Management
13 Data Protection	AC-3 CA-9 AC-4 IA-9 AC-23 MP-3 CA-7 SA-18	SC-8 SI-4 SC-41	PR.DS-5 PR.DS-7 PR.DS-5 PR.PT-2	• Boundary Protection	A.8.2.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5	A.10.7.1 A.12.2.1 - A.12.2.2 A.12.5.4 A.15.1.4	26		• Removable Media Controls			3.6 4.1 - 4.3	• 164.308(a)(4) Information Access Management – Isolating Health Care Clearinghouse Function R • 164.310(d)(1) Device and Media Controls – Accountability A • 164.312(a)(1) Access Control – Encryption and Decryption A • 164.312(e)(1) Transmission Security – Integrity Controls A • 164.312(e)(1) Transmission Security – Encryption A	• Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-011-5 R1			DSI-02 DSI-05 EDM-01 - EDM-04 MOS-17	5: Data Protection	Information Security Management
14 Controlled Access Based on the Need to Know	AU-1 AU-2 AU-3 AU-6 AU-9 AU-12 CA-7 SI-4	PR.AC-4 PR.AC-5 PR.PT-1 PR.PT-3	PR.DS-2 PR.PT-3	• TRUST: Access Control Management • PRIV: Privileges	A.8.3.1 A.9.1.1 A.10.1.1	A.10.7.1 A.10.10.1 - A.10.10.2 A.11.4.1 A.11.4.3 A.11.4.4 A.11.4.6 - A.11.4.7 A.12.5.4	• Network Architecture • Device Accessibility • User Access • Data-at-Rest Protection • Log Management	26	• Segregate Networks and Functions	• Managing User Privileges • Network Security	• Access Control	• Inappropriate Locations for Processing Data	1.3 - 1.4 4.3 7.1 - 7.3 8.7	• 164.308(a)(3) Security Management Process – Information System Activity Review R • 164.308(a)(4) Information Access Management – Isolating Health Care Clearinghouse Function R • 164.308(a)(4) Information Access Management – Access Authorization A • 164.312(a)(1) Access Control – Encryption and Decryption A • 164.312(e)(1) Transmission Security – Encryption A	• Authentication and Access Controls • Encryption • Data Security	• APO12: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4 CIP-011-5 R1	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-006-4 R2	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-006-3 R2	DSI-02 MS-09 MOS-15		Information Security Management
15 Wireless Access Control	AC-18 AC-19 CA-3 CA-7	SC-40 SC-8 SC-17		A.10.1.1 A.12.4.1 A.12.7.1		• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control			• Monitoring • Network Security			4.3 11.1	• 164.308(a)(3) Security Management Process – Information System Activity Review R • 164.308(a)(5) Security Awareness and Training – Protection from Malicious Software A • 164.308(a)(5) Security Awareness and Training – Log-in Monitoring A • 164.308(a)(5) Security Awareness and Training – Password Management A	• Network Security • Encryption • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	MS-01 MS-04 MS-12 MOS-11		Information Security Management
16 Account Monitoring & Control	AC-2 AC-3 AC-7 IA-10 AC-17 SC-17 AC-13 SC-23	CA-7 IA-5 SI-4	PR.AC-1 PR.AC-4 PR.PT-3	• CRED: Credentials and Authentication Management	A.9.1.1 A.9.2.1 - A.9.2.6 A.9.2.3 A.9.4.1 - A.9.4.3 A.11.2.8	A.8.3.2 A.11.2.1 A.11.2.3 - A.11.2.4 A.11.3.1 - A.11.3.3 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	25		• Managing User Privileges • Monitoring	• Access Control	• Configuration of SSL and TLS	7.1 - 7.3 8.7 - 8.8	• 164.308(a)(3) Security Management Process – Information System Activity Review R • 164.308(a)(4) Information Access Management – Access Authorization A • 164.308(a)(4) Information Access Management – Access Establishment and Modification A • 164.308(a)(5) Security Awareness and Training – Password Management A • 164.312(a)(1) Access Control – Automatic Logoff A • 164.312(d) Person or Entity Authentication – A • 164.312(e)(1) Transmission Security – Integrity Controls A • 164.312(e)(1) Transmission Security – Encryption A	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-004-4 R2 CIP-005-4 R2 CIP-007-4 R5	CIP-005-3 R3 CIP-007-3 R5 CIP-007-3 R6	IAM-02 IAM-09 - IAM-12 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
17 Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1 AT-2 AT-3 AT-4 SA-11 SA-14 PM-13 PM-14 PM-16	PR.AT-1 PR.AT-2 PR.AT-3	• BEHV: Security-Related Behavior Management	A.7.2.2	A.8.2.2	• Training	28		• User Education & Awareness			12.6	• 164.308(a)(5) Security Awareness and Training – Security Reminders A • 164.308(a)(5) Security Awareness and Training – Protection from Malicious Software A • 164.308(a)(5) Security Awareness and Training – Log-in Monitoring A • 164.308(a)(5) Security Awareness and Training – Password Management A	• Personnel Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R1 CIP-004-5 R2	CIP-004-4 R1 CIP-004-4 R2	CIP-004-3 R1 CIP-004-3 R2	HRS-10 MOS-03	8: Training and Education	Information Security Management
18 Application Software Security	SA-10 SA-11 SA-15 SA-17 SA-18 SC-29 SI-10	SA-20 SA-21 SI-15 SI-16	PR.DS-7	• VUL: Vulnerability Management	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.4 - A.14.2.8	A.12.5.2 A.12.6.1 A.14.1.2 A.14.1.3 A.14.2.2 - A.14.2.4	• Training	24			• SQL Injection	6.3 6.5 - 6.7		• Application Security • Software Development & Acquisition	• APO13: Manage Security • DSS05: Manage Security Services				AIS-01 AIS-03 AIS-04 CCC-01 CCC-03 IVS-08		Information Security Management
19 Incident Response & Management	IR-1 IR-2 IR-3 IR-4 IR-5 IR-6 IR-7 IR-8 IR-9 IR-10	PR.IP-10 RS.RP-1 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5 RS.MI-1 RS.MI-2 RS.IM-1 RS.IM-2	• Plan for Events • Respond to Events	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	A.6.1.4 A.8.2.1 A.13.1.1 A.13.2.1 - A.13.2.2	• Incident Response and Disaster Recovery Plans			• Incident Management			12.10	• 164.308(a)(6) Security Incident Procedures – Response and Reporting R	• Security Incident Management	• APO13: Manage Security • DSS05: Manage Security Services • DSS02: Manage Service Requests and Incidents	CIP-008-5 R1 CIP-008-5 R2 CIP-008-5 R3	CIP-008-4 R1 CIP-008-4 R2	CIP-008-3 R1 CIP-008-3 R2	SEF-01 - SEF-05	9: Incident Response	Information Security Management
20 Penetration Tests & Red Team Exercises	CA-2 CA-5 CA-8 RA-5 PM-14 SI-6			A.18.2.8 A.18.2.1 A.18.2.3	A.6.1.8 A.15.2.2 A.15.3.1	• Audit Strategy						11.3			• APO13: Manage Security • DSS05: Manage Security Services • MEA02: Monitor, Evaluate and Assess the System of Internal Control						Information Security Management

Our Threat-Centric Model



OpenDNS Investigate	Advanced Malware Protection (AMP)	
OpenDNS Umbrella		Cognitive Threat Analytics (CTA)
ASA & AnyConnect	FirePOWER	OpenDNS Investigate
ISE & TrustSec	WSA/ESA > CWS/CAS/CES	Threat Grid

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



Continuous Analysis and Retrospective Security

Only AMP Continuously Monitors and Analyzes All File Activity, Regardless of Disposition

Across all control points


Email

Web


Network


Endpoints


Mobile

Take advantage of key capabilities


Identify a threat's point of origin


Track it's rate of progression and how it spread

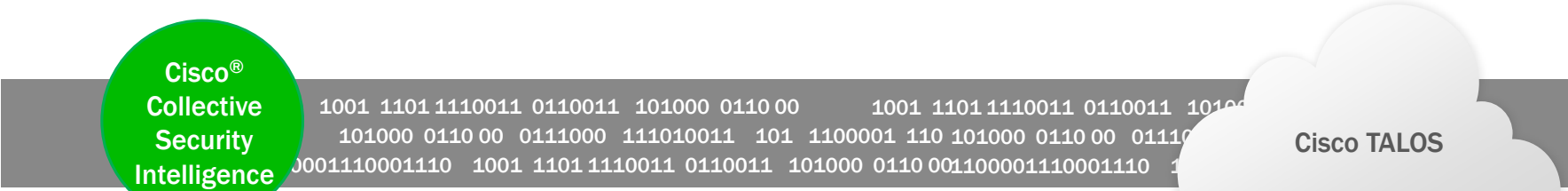

See where it's been


See what it is doing


Surgically target and remediate

To answer the questions that matter…

Threat Intelligence
TALOS



Email

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

Endpoints

Web

- 13 billion web requests
- 24x7x365 operations
- 4.3 billion web blocks per day
- 40+ languages
- 1.1 million incoming malware samples per day
- AMP Community
- Private/Public Threat Feeds

Networks

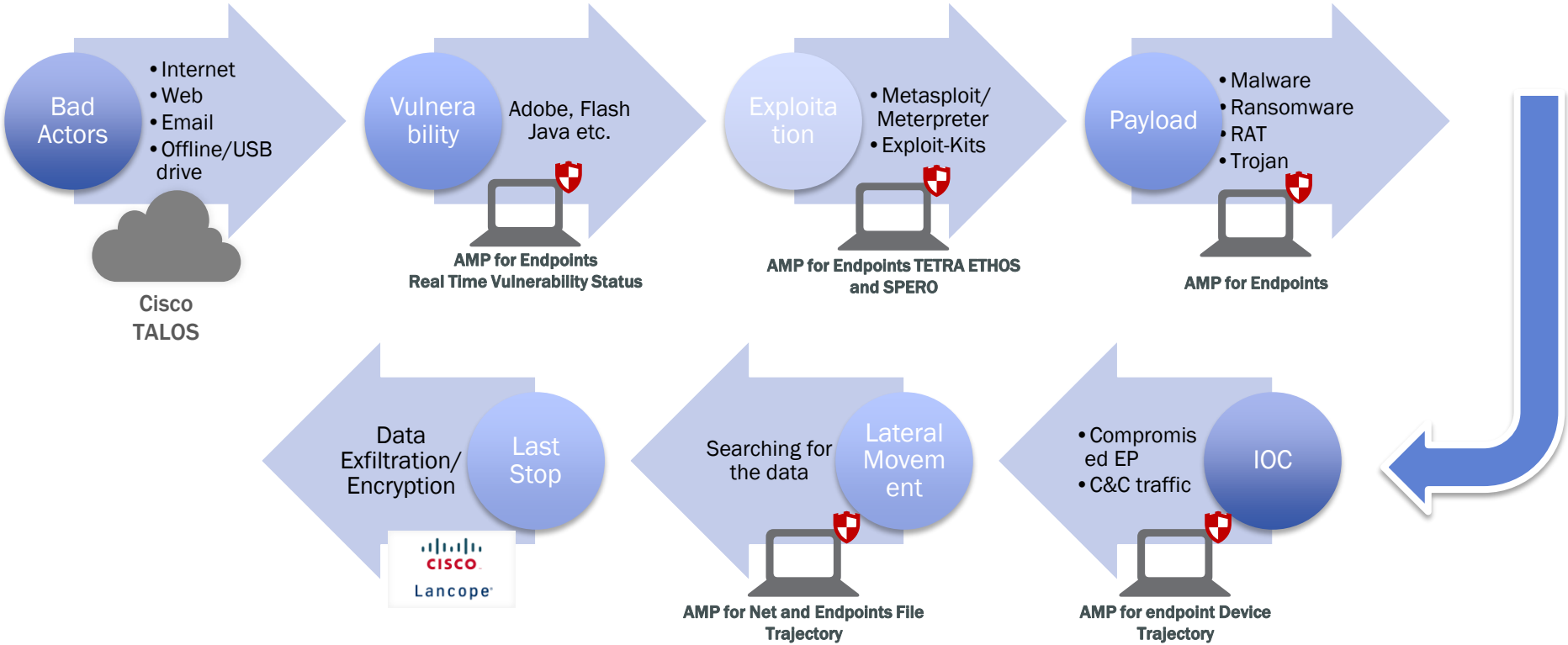
IPS

- Talos Security Intelligence
- AMP Threat Grid Intelligence
- AMP Threat Grid Dynamic Analysis
  10 million files/month
- Advanced Microsoft and Industry Disclosures
- Snort and ClamAV Open Source Communities
- AEGIS Program

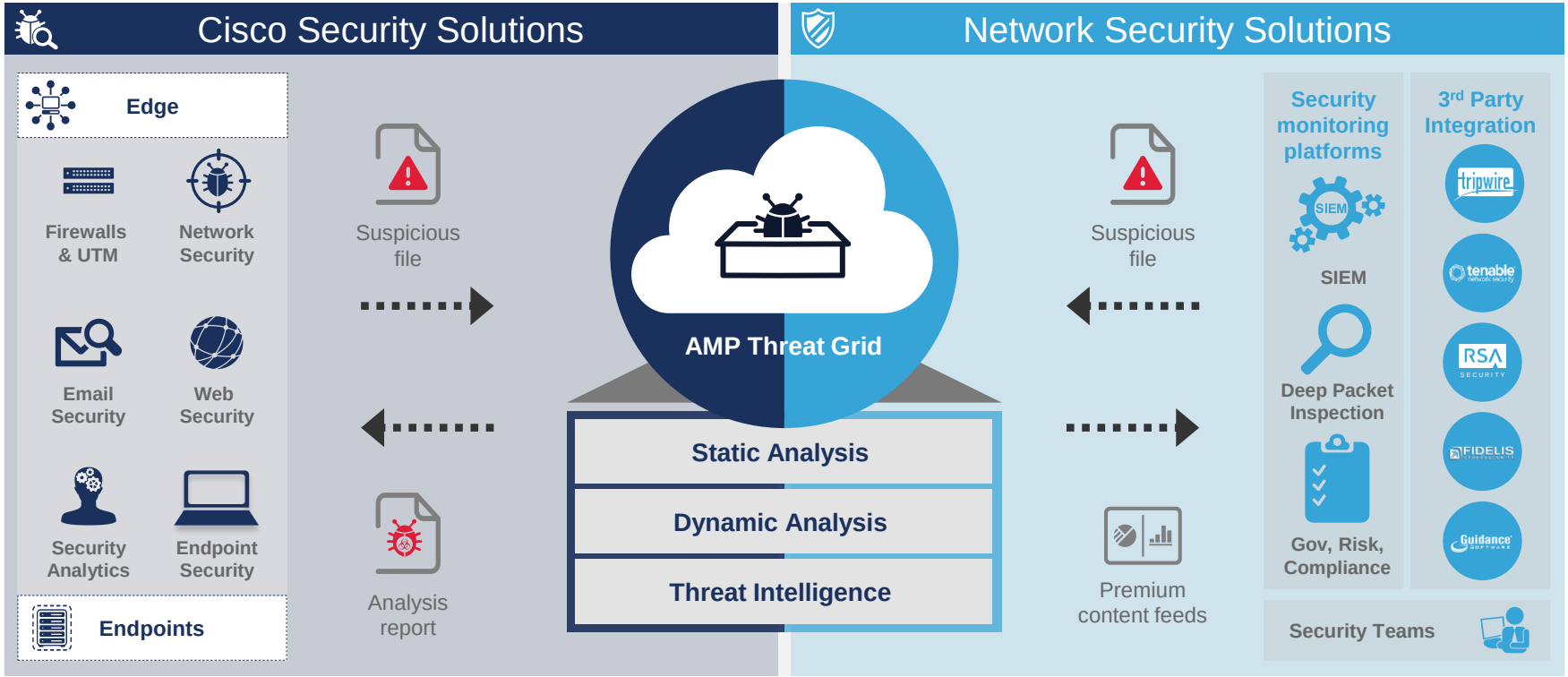
Devices

Automatic updates in real time

Attack life cycle (Kill Chain)



Introducing Threat Grid Everywhere



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
Process Created a File in the Windows Startup Folder	Severity: 80 Confidence: 50
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
Process Modified File in a User Directory	Severity: 70 Confidence: 80
Process Disabled Internet Explorer Proxy	Severity: 70 Confidence: 70
Process Modified an Executable File	Severity: 60 Confidence: 100
DNS Response Contains Low Time to Live (TTL) Value	Severity: 35 Confidence: 20

Examine files with context-driven analysis

Static and Dynamic analysis execute automatically

“Outside looking in” approach

No presence in the VM

Proprietary techniques for static and dynamic analyses

Observing all changes to local host and network communications

Capability to pivot on any data element

Downloadable analysis JSON, in minutes

Accurately identify attacks, in near real time

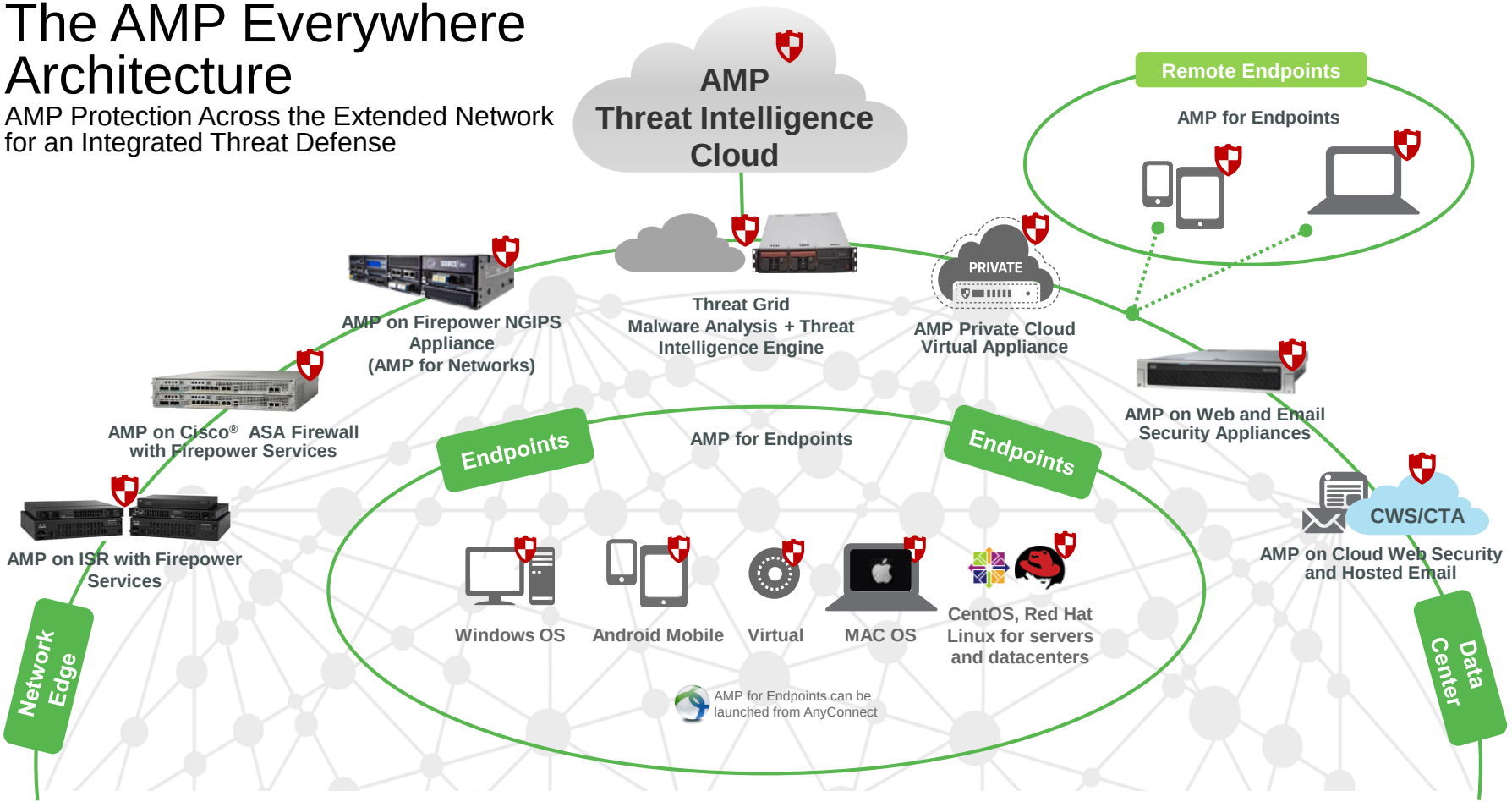
Detailed report identifying key behavioral indicators and threat score

Dynamic Analysis: Process tree visualization

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

The AMP Everywhere Architecture

AMP Protection Across the Extended Network for an Integrated Threat Defense



AMP like an accelerator to successful cybersecurity strategy

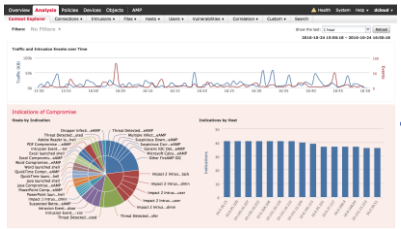

Windows OS

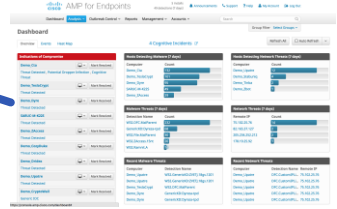

Android Mobile


Virtual


MAC OS


CentOS, Red Hat Linux for servers and datacenters




Unified Control Center

People
Formal Training
Internal Training
On-the-Job Experience
Vendor-Specific Training

SOC
MSSP

Technology
Endpoint
Netflow
Incident Detection/ Management
Network Monitoring
Forensics
Threat Intel

Process
Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned

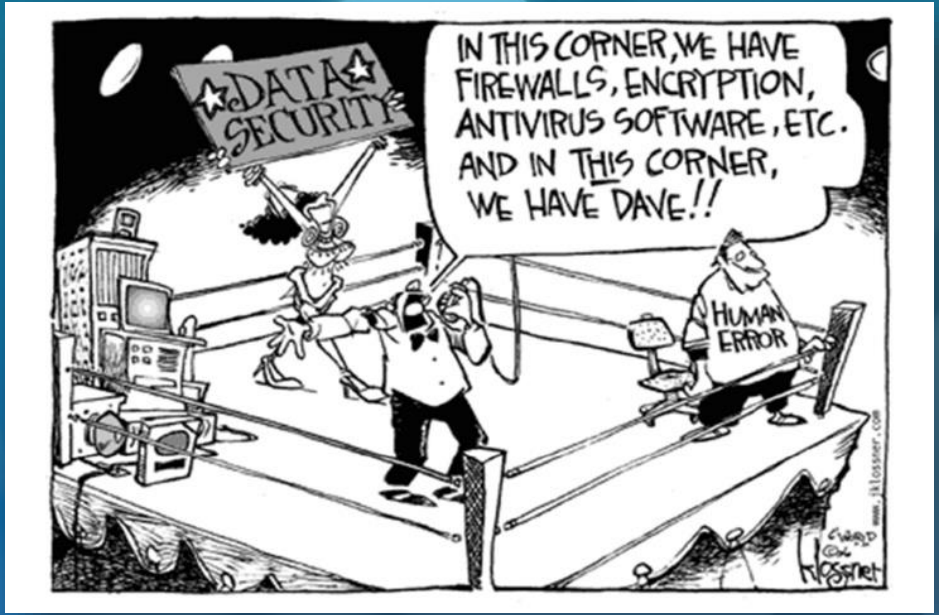

Play Books


Process Level

AMP
TALOS


AMP on Cisco® ASA Firewall, ISR and NGIPS with Firepower Services

Lancope®



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: saruc@cisco.com

Q/A

NSS LABS
RECOMMENDED

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