SNEAK PEEK

Cisco Community Meet the Authors

A Cybersecurity Deep Dive with Omar Santos

January 23rd, 2020

with Omar Santos

Register Now: http://bit.ly/sneak-omar-jan23

Interact with Omar Santos in real time, learn more about his story and the story behind his publications.

Win a free signed copy of his book

During the session, we will select two winners who will receive a signed copy of the book..

Don’t miss out this opportunity!

Register

2

layer

filters

stages: act
platforms: Linux, Windows

Initial Access 11 items	Execution 32 items	Persistence 51 items	Privilege Escalation 26 items	Defense Evasion 64 items	Credential Access 19 items	Discovery 23 items	Lateral Movement 17 items	Collection 13 items	Command And Control 22 items	Exfiltration 9 items	Impact 16 items
Drive-by Compromise	CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through Module Load	BITS Jobs	Exploitation for Privilege Escalation	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Extra Window Memory Injection	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Graphical User Interface	Browser Extensions	File System Permissions Weakness	Component Firmware	Hooking	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	InstallUtil	Change Default File Association	Hooking	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	Local Job Scheduling	Component Firmware	Image File Execution Options Injection	Connection Proxy	Input Prompt	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Object Model Hijacking	New Service	Control Panel Items	Kerberoasting	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Service Stop
	Mshta	Create Account	Parent PID Spoofing	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Stored Data Manipulation
	PowerShell	DLL Search Order Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		System Shutdown/Reboot
	Regsvcs/Regasm	External Remote Services	Port Monitors	Disabling Security Tools	Password Filter DLL	Software Discovery	Windows Admin Shares		Remote Access Tools		Transmitted Data Manipulation
	Regsvr32	File System Permissions Weakness	PowerShell Profile	DLL Search Order Hijacking	Private Keys	System Information Discovery	Windows Remote Management		Remote File Copy		
	Rundll32	Hidden Files and Directories	Process Injection	DLL Side-Loading	Steal Web Session Cookie	System Network Configuration Discovery			Standard Application Layer Protocol		
	Scheduled Task	Hooking	Scheduled Task	Execution Guardrails	Two-Factor Authentication Interception	System Network Connections Discovery			Standard Cryptographic Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	Exploitation for Defense Evasion		System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Extra Window Memory Injection		System Service Discovery			Uncommonly Used Port		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Signed Script Proxy Execution	Local Job Scheduling	Sudo	File Deletion		Virtualization/Sandbox Evasion					
	Source	Logon Scripts	Sudo Caching	File System Logical Offsets							
	Space after Filename	LSASS Driver	Valid Accounts	Group Policy Modification							
	Third-party Software	Modify Existing Service	Web Shell	Hidden Files and Directories							
	Trap	Netsh Helper DLL		Hidden Window							
	Trusted Developer Utilities	New Service		HISTCONTROL							
	User Execution	Office Application Startup		Image File Execution Options Injection							
	Windows Management Instrumentation	Path Interception		Indicator Blocking							
	Windows Remote Management	Port Knocking		Indicator Removal from Tools							
	XSL Script Processing	Port Monitors		Indicator Removal on Host							
		PowerShell Profile		Indirect Command Execution							
		Redundant Access		Install Root Certificate							
		Registry Run Keys / Startup Folder		InstallUtil							
		Scheduled Task		Masquerading							
		Screensaver		Modify Registry							
		Security Support Provider		Mshta							
		Server Software Component		Network Share Connection Removal							
		Service Registry Permissions Weakness		NTFS File Attributes							
		Setuid and Setgid		Obfuscated Files or Information							
		Shortcut Modification		Parent PID Spoofing							
		SIP and Trust Provider Hijacking		Port Knocking							
		System Firmware		Process Doppelgänging							
		Systemd Service		Process Hollowing							
		Time Providers		Process Injection							
		Trap		Redundant Access							
		Valid Accounts		Regsvcs/Regasm							
		Web Shell		Regsvr32							
		Windows Management Instrumentation Event		Rootkit							
		Winlogon Helper DLL		Rundll32							
				Scripting							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

ATT&CK™ NAVIGATOR

https://mitre-attack.github.io/attack-navigator/enterprise/

3

Implementing and Operating Cisco Security Core Technologies (SCOR 350-701)

350-701 SCOR

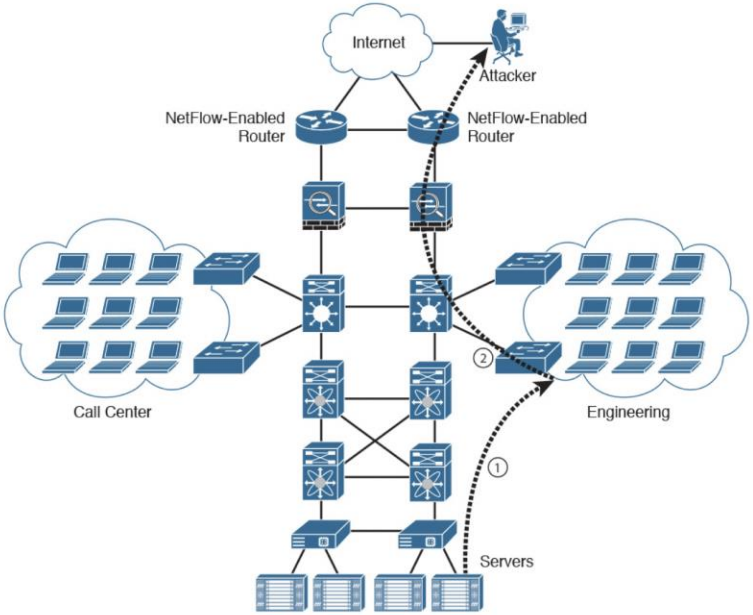
Certifications: CCNP Security, CCIE Security, Cisco Certified Specialist - Security Core

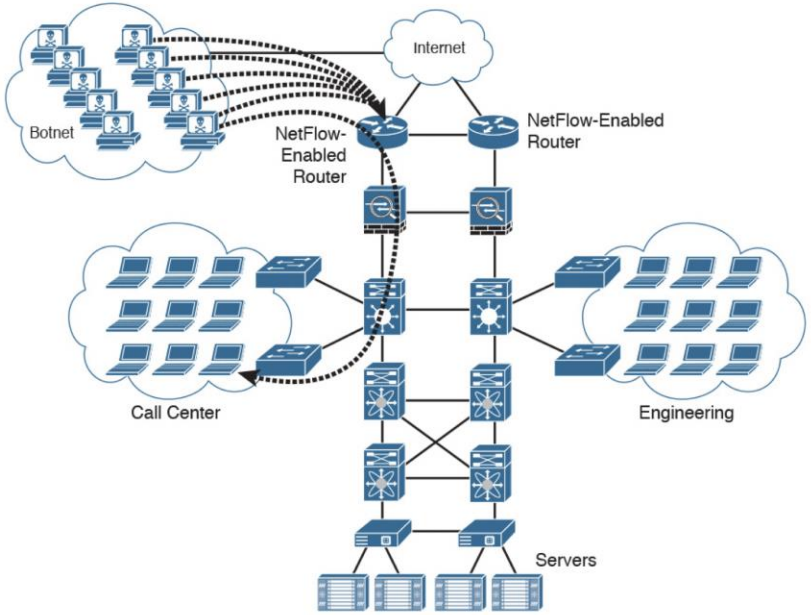
Duration: 120 minutes

Available languages: English, Japanese

https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/scor-350-701.html

4





Network Telemetry and Metadata (including NetFlow)

Security Insight Dashboard | S

dcloud-dna-stealthwatch-rtp.cisco.com/lc-landing-page/smc.html#/dashboard

Stealthwatch

Dashboards | Monitor | Analyze | Jobs

Desktop Client

Security Insight Dashboard | Inside Hosts

Alarming Hosts

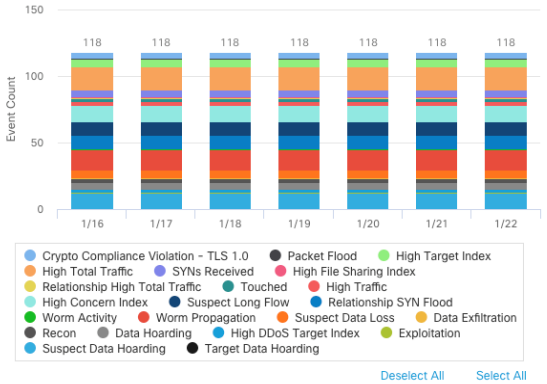
Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
9	6	3	0	1	0	1	3	1	0	0

Top Alarming Hosts

HOST	CATEGORY
10.201.3.149 End User Devices	DH EX
10.201.3.18 End User Devices	RC
10.10.101.24 End User Devices	EP
10.201.0.23 Terminal Servers	DH
10.50.10.254 End User Devices	CI
10.100.10.254 End User Devices	CI
10.30.10.254 End User Devices	CI

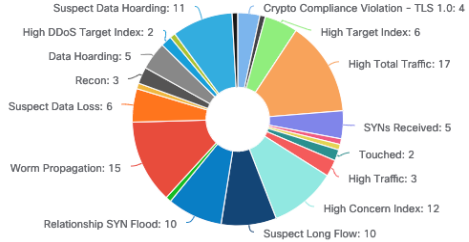
View All Hosts >

Alarms by Type



Deselect All Select All

Today's Alarms



Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low	Total
1	12	21	3	37

Flow Collection Trend

Top Applications

Check out some additional information about Omar Santos and Cisco Security sessions on the Cisco Community or Cisco.com

Omar Santos - Profile

https://blogs.cisco.com/author/omarsantos

Implementing and Operating Cisco Security Core Technologies (SCOR 350-701)

https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/scor-350-701.html

If you are not yet a registered user on the community, Click here to register and become an active participant on the community.

Hope you enjoyed this little peek into the event.

Remember it was just a peek. In January 23rd you get a chance to see the whole thing.

Register Now: http://bit.ly/sneak-omar-jan23

At the session you will be able to learn so much more and get a chance to submit questions for the expert to answer during the event.
We'll see you there!