



Cisco Community Meet The Author

From Zero to CCIE Security: Tips to Prepare for the CCNP & CCIE Security Core exam

Omar Santos

Principal Engineer

September 22nd, 2020



Welcome to the new “Meet Authors event”

Learn from the IT expert that literally wrote the books & content
“Learn more about the latest trends in cybersecurity and the alternatives to enhance your security career”



Meet
Author



Learn the
Story behind



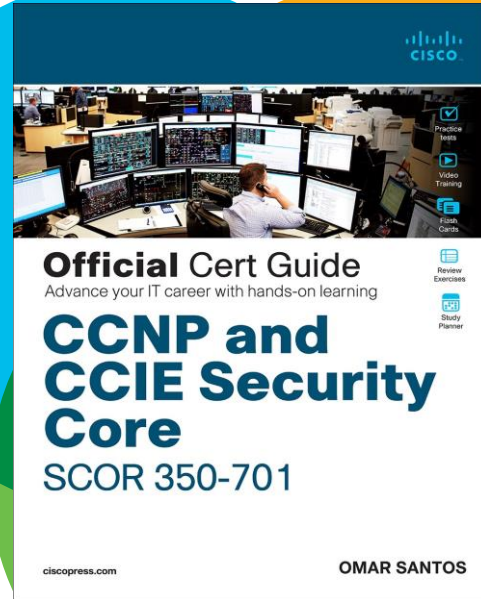
Trends &
Key Content



Clarify
Questions

Win a free signed copy!

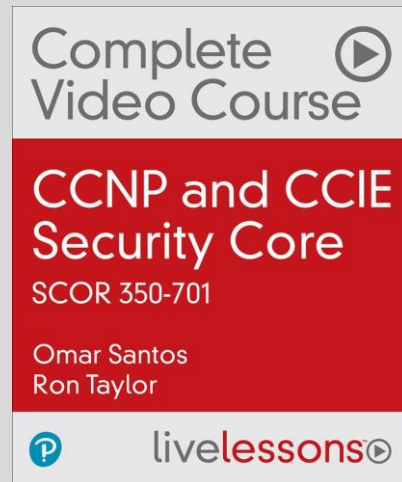
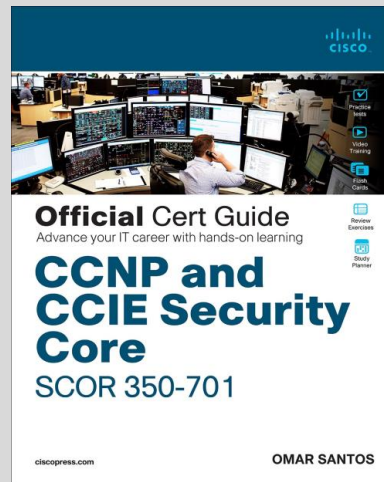
Signed by Omar



Meet the Author



Omar Santos
Principal Engineer



Author of more than 20 books
& video courses



From Zero to CCIE Security: Tips to Prepare for the CCNP & CCIE Security Core Exam

Omar Santos
Principal Engineer
Cisco PSIRT
@santosomar

Agenda

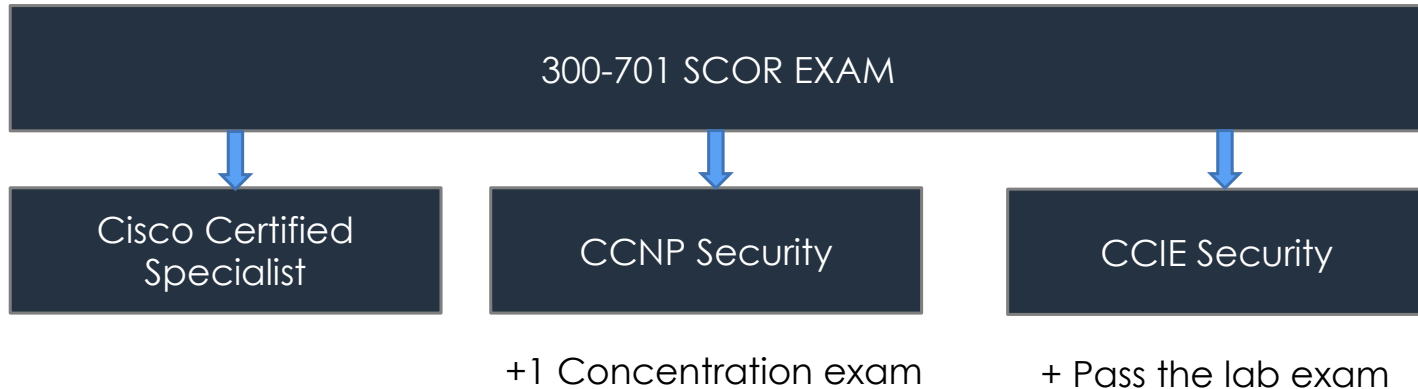
- Introduction to the CCNP and CCIE Security Certifications
- CyberOps Professional vs CCNP Security
- Cybersecurity Concepts
- Network Security
- Securing the Cloud
- Content Security
- Endpoint Protection and Detection
- Secure Network Access, Visibility, and Enforcement
- Final Preparation and Q&A

Introduction to the CCNP and CCIE Security Certifications



Implementing and Operating Cisco Security Core Technologies (SCOR) Exam

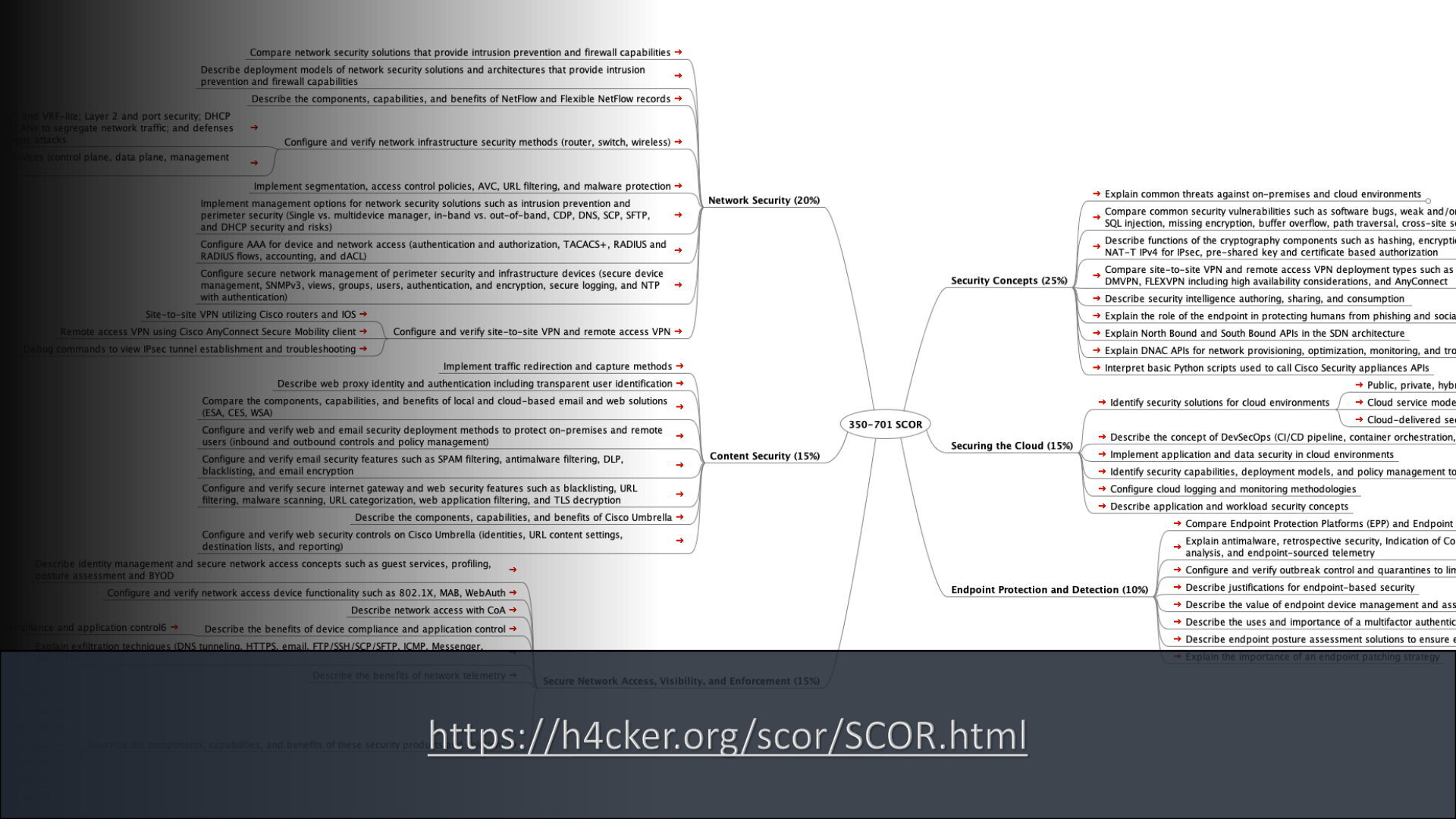
Exam Required for **CCNP Security** and **CCIE Security** Certifications



SCOR Exam Topics

1.0 Security Concepts	25%	▼
2.0 Network Security	20%	▼
3.0 Securing the Cloud	15%	▼
4.0 Content Security	15%	▼
5.0 Endpoint Protection and Detection	10%	▼
6.0 Secure Network Access, Visibility, and Enforcement	15%	▼

<https://learningnetwork.cisco.com/s/scor-exam-topics>



<https://h4cker.org/scor/SCOR.html>

CCNP CyberOps Professional vs CCNP Security

CyberOps Professional

- The core exam focuses on your knowledge of core cybersecurity operations including cybersecurity fundamentals, techniques, processes, and automation.
- The concentration exam focuses on incident response and digital forensics. Incident response is the process of detecting, responding to, and eradicating cyber-attacks. Digital forensics is the collection and examination of digital evidence residing on electronic devices and the subsequent response to threats and attacks.

Required exam	Recommended training
Core exam:	
350-201 CBRCOR	Performing CyberOps Using Cisco Security Technologies (CBRCOR)
First date to test: November 17, 2020	
Concentration exam:	
300-210 CBRFIR	Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)
First date to test: November 17, 2020	

- Introducing SDN
- Explaining North Bound and South Bound APIs in the SDN architecture
- Introducing Cisco ACI
- Introducing Cisco DNA and Cisco DNA Center
- Surveying Open Source SDN solutions
- Understanding the threats against SDN solutions
- Understanding the security benefits in SDN solutions

Software Defined Networking Security

- Introducing Network Programmability
- Exploring DevNet and DevNet resources for security automation
- Introducing APIs
- A brief introduction to Git
- Interpreting basic Python scripts used to call Cisco Security appliances APIs
- Exploring pxGrid
- Interacting with Cisco ISE APIs
- Interacting with network infrastructure APIs
- Integrating and automating security operations with Cisco products

Network
Programmability

- | |
|--|
| • Understanding Authentication |
| • Exploring the RADIUS protocol |
| • Surveying the TACACS+ protocol |
| • Introducing LDAP and Active Directory |
| • Surveying Kerberos |
| • Understanding Authorization |
| • Defining Accounting |
| • Exploring Identity Management |
| • Exploring multi-factor authentication and Single-Sign On |
| • Understanding Cisco DUO |
| • Introducing Cisco ISE |
| • Configuring AAA for device and network access |
| • Configuring downloadable ACLs (dACLs) |
| • Describing identity management secure network access concepts such as guest services, profiling, posture assessment and BYOD |

AAA and Identity Management

Cybersecurity fundamental
topics that you need to study
for the SCOR exam

Understanding common cybersecurity threats against on-premise and cloud environments

- Understanding malware, viruses, trojans, and rootkits
- Exploring how data breaches occur
- Surveying common application-based vulnerabilities
- Understanding different types of malware, rootkits, and trojans
- Surveying Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks
- Exploiting cross-site scripting (XSS) and cross-site request forgery (CSRF) vulnerabilities
- Exploiting authentication and authorization-based vulnerabilities
- Understanding SQL injection, path traversal, and buffer overflow vulnerabilities
- Understanding other common vulnerabilities and security weaknesses
- Explaining how attackers compromise insecure APIs
- Understanding of security threats in cloud and DevOps environments
- Explaining exfiltration techniques

Cryptography Concepts

- Introducing Cryptography and Cryptanalysis
- Understanding encryption protocols
- Describing hashing algorithms
- Introducing Public Key Infrastructure (PKI)
- Introducing certificate authorities (CAs) and certificate enrollment
- Surveying SSL and TLS implementations
- Surveying IPsec implementations
- Describing the functions of other cryptographic components and implementations

Network Security concepts
needed for the CCNP & CCIE
Security SCOR exam

• Defining Network Visibility and Segmentation
• Introducing NetFlow and IPFIX
• Describing the components, capabilities, and benefits of NetFlow and Flexible NetFlow records
• Configuring NetFlow
• Exploring Cisco Stealthwatch
• Deploying Cisco Stealthwatch Cloud
• Designing and Deploying Cisco Stealthwatch
• Exploring the Cisco TrustSec Solution
• Describing the benefits of device compliance and application control
• Enforcing policies with Cisco ISE
• Segmenting the network with Cisco ISE
• Understanding microsegmentation
• Configuring and verify network access device functionality such as 802.1X, MAB, WebAuth
• Describing network access with CoA
• Integrating different security systems using pxGrid
• Exploring Cisco Encrypted Traffic Analytics (ETA)

Secure Network Access, Visibility and Segmentation

- | |
|--|
| • Configuring and verifying network segmentation using VLANs and VRF-lite |
| • Configuring and verifying port security |
| • Configuring and verifying DHCP snooping |
| • Configuring and verifying Dynamic ARP inspection |
| • Configuring and verifying storm control |
| • Configuring and verifying PVLANS to segregate network traffic |
| • Configuring and verifying defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks |
| • Understanding the control plane, data plane, and management plane |
| • Hardening network infrastructure security devices |
| • Configuring secure network management of perimeter security and infrastructure devices |

Infrastructure Security

- Introducing Cisco's Next-Generation Firewalls
- Surveying the Cisco Firepower Management Center (FMC)
- Exploring the Cisco Firepower Device Manager (FDM)
- Comparing network security solutions that provide intrusion prevention and firewall capabilities
- Describing deployment models of network security solutions and architectures that provide firewall capabilities
- Segmenting the network with Cisco Next-Generation Firewalls
- Implementing access control policies
- Configuring AVC, URL filtering, and malware protection
- Troubleshooting Cisco Next-Generation Firewalls

Cisco Next- Generation Firewalls

- Introducing Cisco's Next-Generation Intrusion Prevention Systems
- Describing deployment models of network security solutions and architectures that provide intrusion prevention capabilities
- Configuring Cisco Next-Generation Intrusion Prevention Systems
- Troubleshooting Cisco's Next-Generation Intrusion Prevention Systems

Cisco Next-Generation Intrusion Prevention Systems

- Introduction to IPSec Site-to-site and remote access VPNs
- Configuring IPSec site-to-site VPNs
- Configuring Traditional Site-to-site VPN utilizing Cisco routers
- Configuring DMVPN
- Configuring FlexVPN
- Configuring Site-to-site VPN utilizing Cisco routers
- Troubleshooting Site-to-site VPN implementations

Site-to-site VPN Implementations

- Introducing Remote Access VPNs
- Exploring Clientless Remote Access VPNs
- Surveying Remote access VPN implementations using Cisco AnyConnect Secure Mobility client
- Configuring Remote Access VPN in Cisco ASA
- Configuring Remote Access VPN in Cisco FTD
- Troubleshooting Remote Access VPN implementations

Remote Access VPN

DNA Center Demo



Detailed Demos

<https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-analytics-assurance/demos/whiteboard.html#~stickynav=1>

<https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-analytics-assurance/demos/instant-demo.html>

Firepower Demo



ThreatGrid Demo



Securing the
Cloud



- | |
|---|
| • Introducing the different cloud deployment and service models |
| • Surveying patch management in the cloud |
| • Performing security assessments in cloud environments |
| • Exploring the concepts of DevSecOps |
| • Implementing application and data security in cloud environment |
| • Identifying security capabilities, deployment models, and policy management to secure the cloud |
| • Configuring cloud logging and monitoring methodologies |
| • Describing application and workload security concepts |

Securing the Cloud

NIST

**National Institute of
Standards and Technology**
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

**Recommendations of the National Institute
of Standards and Technology**

Peter Mell
Timothy Grance

A MUST READ!!!

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

NIST Cloud Computing Related Publications

<https://www.nist.gov/itl/nist-cloud-computing-related-publications>



Content Security



Introducing Cisco Content Security Solutions

Implementing traffic redirection and capture methods

Describing web proxy identity and authentication including transparent user identification

Comparing the components, capabilities, and benefits of local and cloud-based email and web solutions

Configuring and verifying web security deployment methods to protect onpremises and remote users

Configuring and verifying email security features

Configuring and verifying secure internet gateway and web security features

Describing the components, capabilities, and benefits of Cisco Umbrella

Configuring and verifying web security controls on Cisco Umbrella

Exploring Cisco Umbrella Investigate

Content Security

Overview

Deployments >

Policies >

Reporting >

Admin >

Investigate

threat response >

Threat Response Integration Demo

Documentation

Support Platform

Learning Center

Privacy Policy

Terms Of Service

© Cisco Systems

Malware: 1 request blocked in the last 24 hours [View Trend](#) | [View Details](#)Command and Control: 0 requests blocked in the last 24 hours [View Trend](#) | [View Details](#)Cryptomining: 0 requests blocked in the last 24 hours [View Trend](#) | [View Details](#)

FILTERS

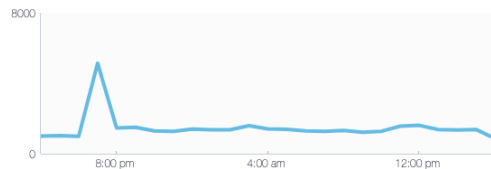
Deployment Health

 Active Networks
0 / 0 Active Active Roaming Clients
1 / 1 Active Active Virtual Appliances
5 / 5 Active

Network Request Breakdown

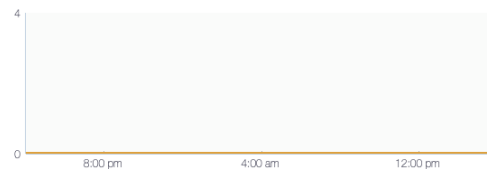
Total DNS Requests

36.7K Total, ▲ 122%

[VIEW ACTIVITY](#)

Total Proxy Requests

0 Total, - %

[VIEW ACTIVITY](#)

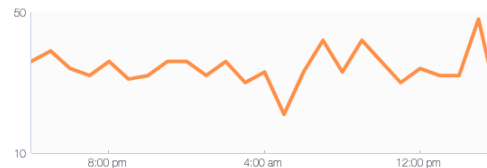
Total Blocks

850 Total, ▼ 4%

[VIEW ACTIVITY](#)

Security Blocks

850 Total, ▼ 4%

[VIEW ACTIVITY](#)

- Overview
- Deployments >
- Policies >
- Reporting >
- Core Reports**
- Security Activity
- Admin >
- Investigate
- threat response** >
- Threat Response Integration Demo
- Documentation
- Support Platform
- Learning Center
- Privacy Policy
- Terms Of Service
- © Cisco Systems

TIME

- In the Last Hour
- Last 24 Hours**
- Yesterday
- This Week
- Last 30 Days

EVENT TYPE

- Antivirus
- Cisco AMP
- Integration
- Security Category**

Group Events by Type

RESPONSE

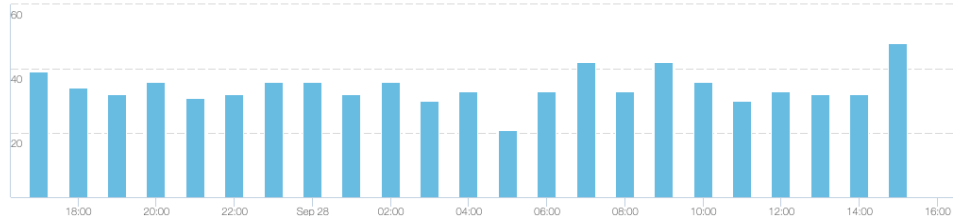
- Allowed
- Blocked**

Search Security Activity

Advanced ▾

IDENTITY wkst1

All Security Activity (Last 24 Hours)



LAST 24 HOURS

INTEGRATION BLOCKED wkst1 Sep 28, 2019 at 5:02 PM

Event Details (1 of 100)

<p>Date & Time Sep 28, 2019 at 5:02 PM</p> <p>Destination www.easycounter.com</p>	<p>Identity wkst1 ★ Policy</p> <p>Categories Threat Response, Software/Technology</p> <p>Internal IP 198.18.133.36</p>	<p>External IP 64.100.12.6</p> <p>Result Blocked</p> <p>DNS Record Type A</p>
--	--	---

Overview

Deployments

Policies

Reporting

Admin

Investigate

[Investigate UI Documentation](#)
[Support](#)
[SEARCH](#) [PATTERN SEARCH](#)



THREAT SAMPLE (SHA256)

bf2cdd1dc2e20c42d2451c83b8280490879b3515aa6c15ab297419990e017142

SHA1 4d004abb5a9085d713e6c3a79269c67f65484db

MD5 da8b478f6c1fa76858b67b1329bac447

Threat Score: **95**

Magic Type: PE32 executable (GUI) Intel 80386, for MS Windows

Size: 84992 bytes

First Seen: Jul, 22, 2019 19:26:20 UTC

[Full Sample Data from Threat Grid](#)

BEHAVIORAL INDICATORS

Indicator	Severity	Confidence
Artifact Flagged Malicious by Antivirus Service	100	95
Machine Learning Model Identified Executable Artifact as Likely Malicious	90	90
An HTTP Request Was Made to a Numeric IP Address	75	80
Static Analysis Flagged Artifact As Anomalous	60	80
File Uploaded to the Network	60	80
Executable Artifact Imports Tool Help Functions	50	70
Potential Code Injection Detected	50	50
Outbound Communications to Nginx Web Server	25	25
Outbound HTTP POST Communications	25	25
Executable Imported the IsDebuggerPresent Symbol	20	20
PE Contains Section with Blank or No Name	5	60
PE COFF Header Timestamp is Not Set	5	60
PE COFF Header Timestamp is Set to Date Prior to 1999	5	60

Network Connections

Overview

Deployments

Policies

Reporting

Admin

Investigate

Investigate UI Documentation

Support

[SEARCH](#) [PATTERN SEARCH](#)

178.17.167.51

INVESTIGATE



Details for 178.17.167.51

Hosting 0 malicious domains for 1 week

This IP is currently in the Umbrella block list as malware

Security Categories: Malware

Threat Types: APT

AS

Prefix	ASN	Network Owner Description
178.17.160.0/20	AS 43289	TRABIA, MD 86400
178.17.160.0/20	AS 43289	TRABIA, MD 86400

Malicious domains hosted by 178.17.167.51

No info to display

Associated Samples

POWERED BY CISCO AMP THREAT GRID

No info to display

DNS Resolution

Domain	Categories	TTL(s)	First Seen ▾	Last Seen ▾
Total Domains: 3 TTL(s): 3600				
178-17-167-51.static.as43289.net		3600	February 14, 2019	August 11, 2019
178-17-167-51.static.host		3600	August 27, 2016	August 27, 2016

ESA Demo



Endpoint Protection and Detection



<ul style="list-style-type: none">• Explaining the role of the endpoint in protecting humans from phishing and social engineering attacks
<ul style="list-style-type: none">• Describing justifications for endpoint-based security
<ul style="list-style-type: none">• Comparing Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR) solutions
<ul style="list-style-type: none">• Describing the value of endpoint device management and asset inventory such as MDM
<ul style="list-style-type: none">• Describing the uses and importance of a multifactor authentication (MFA) strategy
<ul style="list-style-type: none">• Describing endpoint posture assessment solutions to ensure endpoint security
<ul style="list-style-type: none">• Explaining the importance of an endpoint patching strategy
<ul style="list-style-type: none">• Explaining antimalware, retrospective security, and Indicators of Compromise (IOC)
<ul style="list-style-type: none">• Describing dynamic file analysis and endpoint-sourced telemetry
<ul style="list-style-type: none">• Configuring and verifying outbreak control and quarantines to limit infection
<ul style="list-style-type: none">• Deploying Cisco AnyConnect Network Visibility Module (NVM)

Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

Refresh All Auto-Refresh ▾

mac (Default) ▾

30 days ▾ 2019-08-29 21:08 2019-09-28 21:08 UTC

41.5% compromised ?

Inbox Status

● 22 Require Attention ● 0 In Progress ● 0 Resolved

Cognitive Threat Analytics



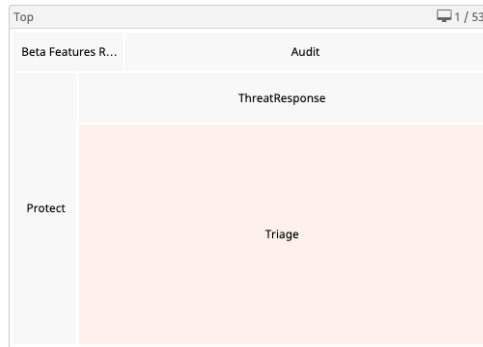
Compromises ?

✉ Inbox

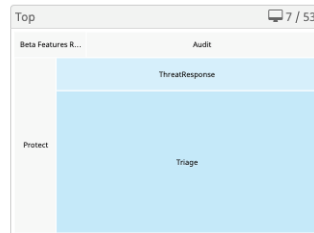


Quarantined Detections ?

🔊 Quarantine Events



Vulnerabilities View



Threat Grid Analysis

0 Automatic Analysis Submissions
 1 Retroactive Threat Detections

Statistics

177 Thousand Files Scanned
 27.1 Thousand Network Connections Logged

Connectors

53 Connectors
 2 Installs
 0 Install Failures

Quick Start

- 🖥️ Set Up Windows Connector
- 🍏 Set Up Mac Connector
- 🐧 Set Up Linux Connector

Significant Compromise Artifacts ?

FILE	17f746d8...a02402ae cmd.exe	<input type="checkbox"/> 3
IP	75.102.25.76	<input type="checkbox"/> 2
FILE	90489ea6...da4b7a9f 90489ea6082c921fa7623df3b6...	<input type="checkbox"/> 1
FILE	c9a02ed8...5c3b3f1a wpforms-form-templates-pac...	<input type="checkbox"/> 1
FILE	eed6f56e...00d3f89d wpforms-aweber-1.0.7.zip	<input type="checkbox"/> 1

Compromise Event Types ?

2 event types muted

Medium	Threat Detected	<input type="checkbox"/> 18
High	Executed malware	<input type="checkbox"/> 13
High	Cloud Recall Detection	<input type="checkbox"/> 4
High	Cloud Recall Quarantine Successful	<input type="checkbox"/> 4
High	DFC Threat Detected	<input type="checkbox"/> 4

AMP Demo





Submit Your
Questions Now!



Use the Q&A panel to submit your
questions, our expert will respond.

Extra Resources and References

Cisco Press News

The new study guide for the Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide is under production. Will be available on Nov 26, 2020 [[Learn more](#)]

Cisco Press -Cisco Certification Program Update

<http://www.ciscopress.com/promotions/new-cisco-certifications-142035>

Other useful resources:

CCNP and CCIE Security Core SCOR 350-701 Complete Video Course (Video Training)

<https://www.ciscopress.com/store/ccnp-and-ccie-security-core-scor-350-701-complete-video-9780136583363>

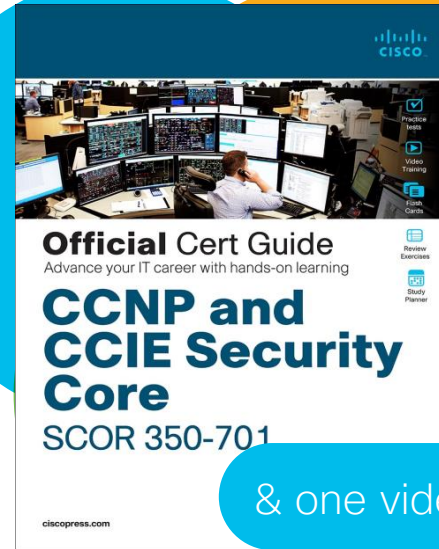
The NIST Definition of Cloud Computing

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

NIST Cloud Computing Related Publications

<https://www.nist.gov/itl/nist-cloud-computing-related-publications>

Congratulations
winners!



& one video course

We'll contact you via email

Thank you for Your Time!

Please help to complete the survey

Your opinion is important and help us to improve



Thanks For Joining today!

