210-255$^{Q\&As}$

Cisco Cybersecurity Operations

QUESTION 1

How do you verify that one of your hosts is potentially compromised based on their communication destinations?

A. Search the communication destinations of the host in the Talos IP and Domain Reputation Center.

B. Analyze how much traffic the host sent and received from each IP address or domain.

C. See if any Stealthwatch alarms were triggered for the host communicating with internal hosts.

D. Check the Firepower appliance to see if malicious files were downloaded.

Correct Answer: A

QUESTION 2

What is a common artifact used to uniquely identify a detected file?

A. file size

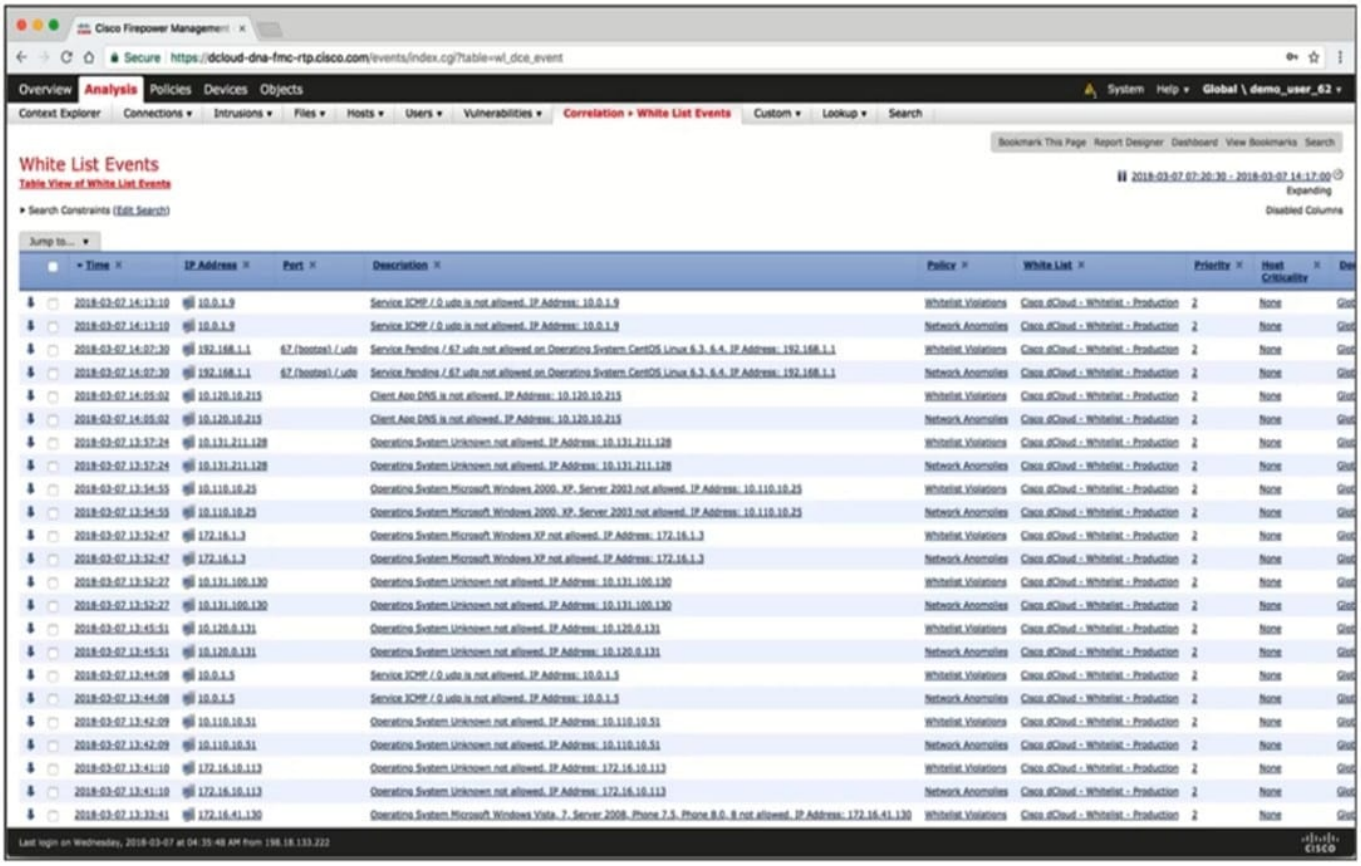
B. file extension

C. file timestamp

D. file hash

Correct Answer: D

QUESTION 3



White List Events

Table View of White List Events

▸ Search Constraints (Edit Search)

2018-03-07 07:20:30 - 2018-03-07 14:17:00
Expanding

Disabled Columns

	▾ Time	IP Address	Port	Description	Policy	White List	Priority	Host Criticality	De
□	2018-03-07 14:13:10	10.0.1.9		Service ICMP / 0 udp is not allowed. IP Address: 10.0.1.9	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 14:13:10	10.0.1.9		Service ICMP / 0 udp is not allowed. IP Address: 10.0.1.9	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 14:07:30	192.168.1.1	67 (bootps) / udp	Service Pending / 67 udp not allowed on Operating System CentOS Linux 6.3, 6.4. IP Address: 192.168.1.1	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 14:07:30	192.168.1.1	67 (bootps) / udp	Service Pending / 67 udp not allowed on Operating System CentOS Linux 6.3, 6.4. IP Address: 192.168.1.1	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 14:05:02	10.120.10.215		Client App DNS is not allowed. IP Address: 10.120.10.215	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 14:05:02	10.120.10.215		Client App DNS is not allowed. IP Address: 10.120.10.215	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:57:24	10.131.211.128		Operating System Unknown not allowed. IP Address: 10.131.211.128	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:57:24	10.131.211.128		Operating System Unknown not allowed. IP Address: 10.131.211.128	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:54:55	10.110.10.25		Operating System Microsoft Windows 2000, XP, Server 2003 not allowed. IP Address: 10.110.10.25	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:54:55	10.110.10.25		Operating System Microsoft Windows 2000, XP, Server 2003 not allowed. IP Address: 10.110.10.25	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:52:47	172.16.1.3		Operating System Microsoft Windows XP not allowed. IP Address: 172.16.1.3	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:52:47	172.16.1.3		Operating System Microsoft Windows XP not allowed. IP Address: 172.16.1.3	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:52:27	10.131.100.130		Operating System Unknown not allowed. IP Address: 10.131.100.130	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:52:27	10.131.100.130		Operating System Unknown not allowed. IP Address: 10.131.100.130	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:45:51	10.120.0.131		Operating System Unknown not allowed. IP Address: 10.120.0.131	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:45:51	10.120.0.131		Operating System Unknown not allowed. IP Address: 10.120.0.131	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:44:08	10.0.1.5		Service ICMP / 0 udp is not allowed. IP Address: 10.0.1.5	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:44:08	10.0.1.5		Service ICMP / 0 udp is not allowed. IP Address: 10.0.1.5	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:42:09	10.110.10.51		Operating System Unknown not allowed. IP Address: 10.110.10.51	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:42:09	10.110.10.51		Operating System Unknown not allowed. IP Address: 10.110.10.51	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:41:10	172.16.10.113		Operating System Unknown not allowed. IP Address: 172.16.10.113	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:41:10	172.16.10.113		Operating System Unknown not allowed. IP Address: 172.16.10.113	Network Anomalies	Cisco dCloud - Whitelist - Production	2	None	Glo
□	2018-03-07 13:33:41	172.16.41.130		Operating System Microsoft Windows Vista, 7, Server 2008, Phone 7.5, Phone 8.0, 8 not allowed. IP Address: 172.16.41.130	Whitelist Violations	Cisco dCloud - Whitelist - Production	2	None	Glo

Last login on Wednesday, 2018-03-07 at 04:35:48 AM from 198.18.133.222

Refer to the exhibit. Which function of the Cisco Firepower Management Console correlation rules does the screenshot demonstrate?

A. operating system whitelist events

B. whitelisted true positive events

C. whitelisted false positive events

D. whitelisted command and control communication events

Correct Answer: B

QUESTION 4

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. Which term defines the initial event in the NIST SP800- 61 r2?

A. instigator

B. precursor

C. online assault

D. trigger

Correct Answer: B

QUESTION 5

Which incident handling phase contains evidence gathering and handling?

A. containment, eradication, and recovery

B. identification

C. post incident

D. preparation

Correct Answer: C