Firepower Management Center | Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence | Deploy | admin

Bookmark This Page | Report Designer | Dashboard | View Bookmarks | Search | Predefined Searches

Events By Priority and Classification (switch workflow)

2020-06-26 15:08:38 - 2020-06-26 16:35:40
Expanding

▸ Search Constraints (Edit Search Save Search)

Drilldown of Event, Priority, and Classification | Table View of Events | Packets

Jump to...

	Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	Message	Classification	Generator	Source User	Application Protocol	Client
▾	2020-06-26 16:35:13	low	2	↓	10.50.24.25		10.50.168.28		56353 / tcp	2500 / tcp	Unknown (Unknown)	0	POLICY-OTHER eicar test string download attempt (1:37732:4)	Misc Activity	Standard Text Rule	No Authentication Required		
▾	2020-06-26 16:34:03	low	2	↓	10.50.24.25		10.50.168.28		56311 / tcp	2500 / tcp	Unknown (Unknown)	0	POLICY-OTHER eicar test string download attempt (1:37732:4)	Misc Activity	Standard Text Rule	No Authentication Required		
▾	2020-06-26 16:32:53	low	2	↓	10.50.24.25		10.50.168.28		56255 / tcp	2500 / tcp	Unknown (Unknown)	0	POLICY-OTHER eicar test string download attempt (1:37732:4)	Misc Activity	Standard Text Rule	No Authentication Required		
▾	2020-06-26 16:31:43	low	2	↓	10.50.24.25		10.50.168.28		56109 / tcp	2500 / tcp	Unknown (Unknown)	0	POLICY-OTHER eicar test string download attempt (1:37732:4)	Misc Activity	Standard Text Rule	No Authentication Required		

Page 1 of 1 Displaying rows 1-4 of 4 rows

View | Copy | Delete | Review | Download Packets

View All | Copy All | Delete All | Review All | Download All Packets

10
ng

Web Application	IOC	Ingress Security Zone	Egress Security Zone	Device	Security Context	Ingress Interface	Egress Interface	Ingress Virtual Router	Egress Virtual Router	Intrusion Policy	Access Control Policy	Access Control Rule	Network Analysis Policy
		inside	transfer-outside	FTD-SCH-01		inside	outside			Paudler_default_IPS_Policy	ACP_FTD-SCH	in-inside_#14	Balanced Security and Connectivity
		inside	transfer-outside	FTD-SCH-01		inside	outside			Paudler_default_IPS_Policy	ACP_FTD-SCH	in-inside_#14	Balanced Security and Connectivity
		inside	transfer-outside	FTD-SCH-01		inside	outside			Paudler_default_IPS_Policy	ACP_FTD-SCH	in-inside_#14	Balanced Security and Connectivity
		inside	transfer-outside	FTD-SCH-01		inside	outside			Paudler_default_IPS_Policy	ACP_FTD-SCH	in-inside_#14	Balanced Security and Connectivity

Events By Priority and Classification (switch workflow)

2020-06-26 15:08:38 - 2020-06-26 16:43:09
Expanding

▸ Search Constraints (Edit Search Save Search)

Drilldown of Event, Priority, and Classification | Table View of Events | Packets

Event Information

Event	POLICY-OTHER eicar test string download attempt (1:37732:4)
Timestamp	2020-06-26 16:42:15
Classification	Misc Activity
Priority	low
Ingress Security Zone	inside
Egress Security Zone	transfer-outside
Device	FTD-SCH-01
Ingress Interface	inside
Egress Interface	outside
Source IP	10.50.24.25
Source Port / ICMP Type	56620 / tcp
Destination IP	10.50.168.28
Destination Port / ICMP Code	2500 / tcp
Intrusion Policy	Paudler_default_IPS_Policy
Access Control Policy	ACP_FTD-SCH
Access Control Rule	in-inside_#14
Rule	alert tcp any any -> any any (msg:"POLICY-OTHER eicar test string download attempt"; flow:established; file_data; content:"7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+"; fast_pattern:only; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop; reference:url,www.eicar.org/86-0-Intended-use.html; classtype:misc-activity; sid:37732; rev:4; gid:1;)

Actions

Packet Information

FRAME 1 (Expand All)

- **Frame 1: 1374 bytes on wire** (1374 bytes captured (10992 bits))
- **Ethernet II** (Src: BC:EA:FA:C5:9C:08, Dst: A4:6C:2A:9F:C4:C2)
- **Internet Protocol Version 4** (Src: 10.50.24.25, Dst: 10.50.168.28)
- **Transmission Control Protocol** (Src Port: 56620 (56620), Dst Port: 2500 (2500), Seq: 1, Ack: 1, Len: 1320)
- **Data** (1320 bytes)
- **Packet Text**
- **Packet Bytes**

Displaying row 1 of 10 rows Page 1 of 10

Copy | Delete | Review | Download Packet
Copy All | Delete All | Review All | Download All Packets

Connection Events (switch workflow)

2020-06-26 15:08:38 - 2020-06-26 16:46:25
Expanding

▸ Search Constraints (Edit Search Save Search)

Connections with Application Details | Table View of Connection Events

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device	Security Context
▾	2020-06-26 16:45:21	2020-06-26 16:45:46	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56743 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:44:11	2020-06-26 16:44:35	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56707 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:43:00	2020-06-26 16:43:25	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56650 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:41:50	2020-06-26 16:42:15	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56620 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:40:40	2020-06-26 16:41:05	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56573 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:39:30	2020-06-26 16:39:54	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56524 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:38:19	2020-06-26 16:38:44	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56485 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:37:09	2020-06-26 16:37:34	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56430 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:36:08	2020-06-26 16:36:24	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56405 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:34:57	2020-06-26 16:35:13	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56353 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:33:38	2020-06-26 16:34:03	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56311 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:32:37	2020-06-26 16:32:53	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56255 / tcp	2500 / tcp							FTD-SCH-01	
▾	2020-06-26 16:28:52	2020-06-26 16:31:43	Block	Intrusion Block	10.50.24.25		10.50.168.28		inside	transfer-outside	56109 / tcp	2500 / tcp							FTD-SCH-01	

Page 1 of 1 Displaying rows 1–13 of 13 rows

View
View All