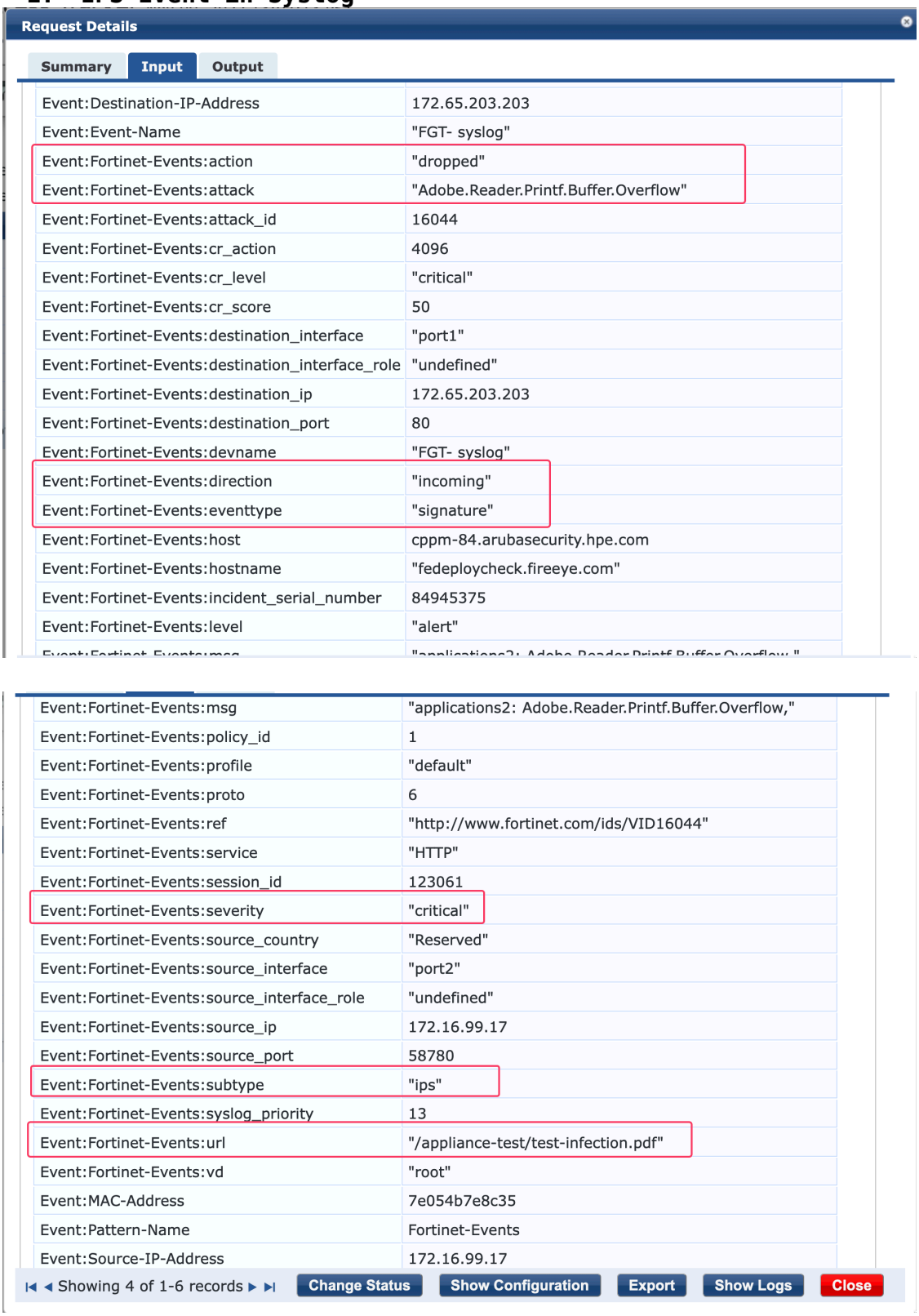
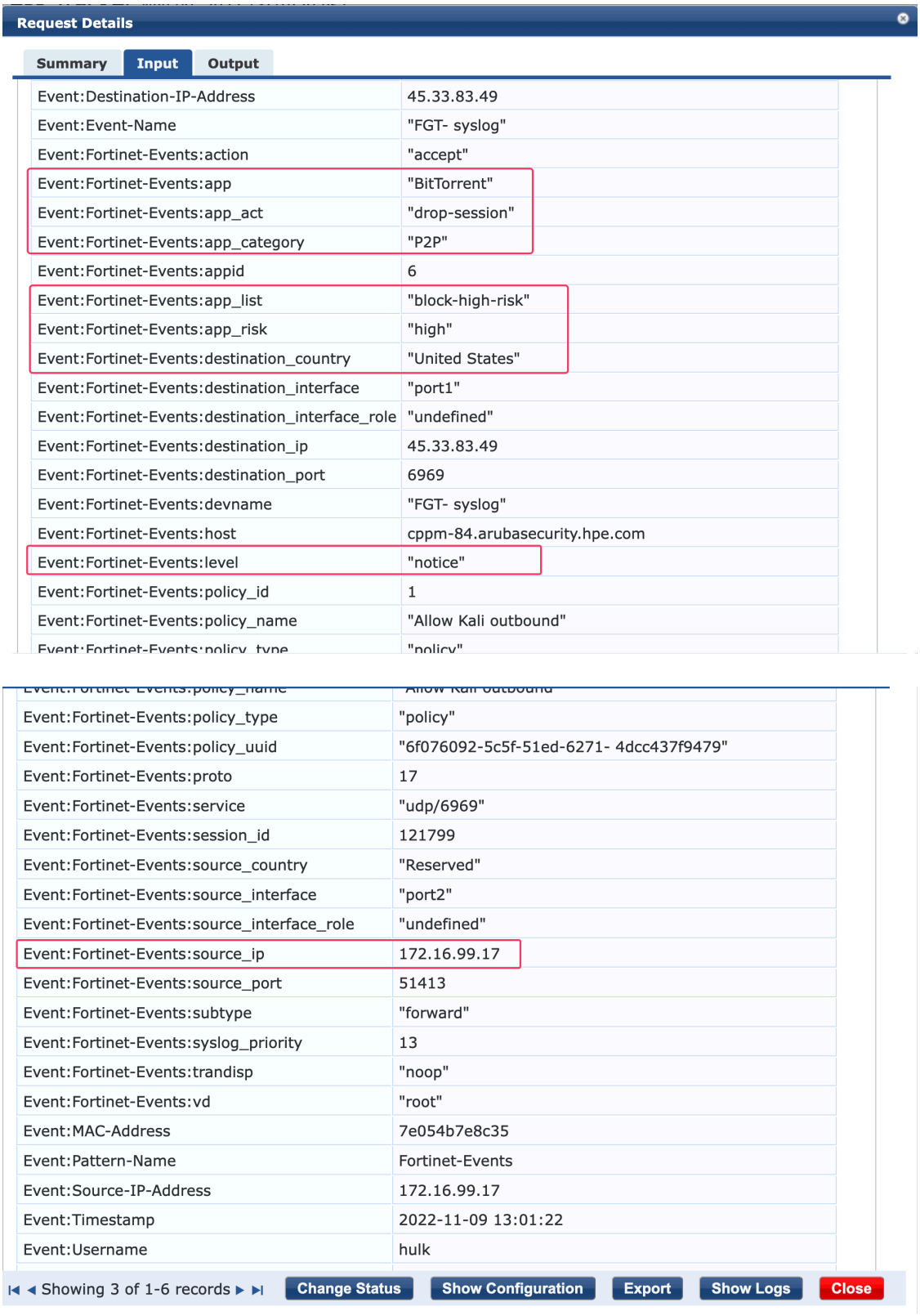
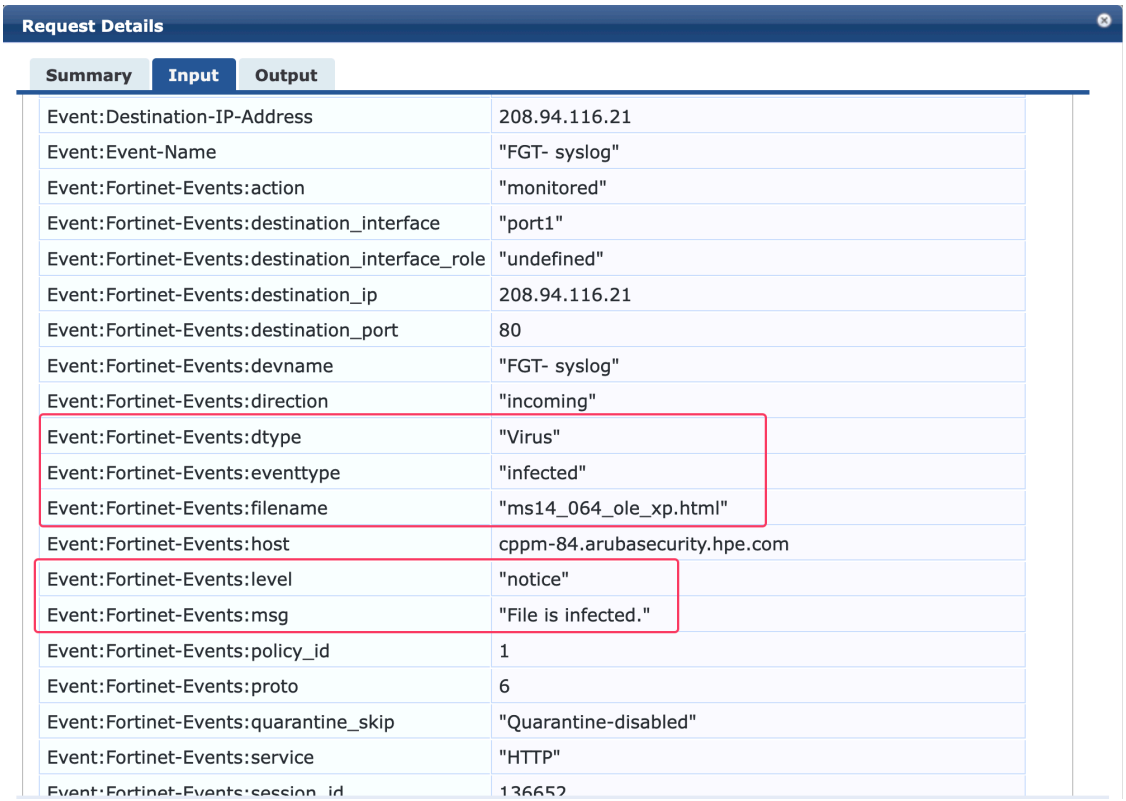
1. IPS Event in Syslog



2. Application Control in Syslog



3. AntiVirus in Syslog



Event:Destination-IP-Address	208.94.116.21
Event:Event-Name	"FGT- syslog"
Event:Fortinet-Events:action	"monitored"
Event:Fortinet-Events:destination_interface	"port1"
Event:Fortinet-Events:destination_interface_role	"undefined"
Event:Fortinet-Events:destination_ip	208.94.116.21
Event:Fortinet-Events:destination_port	80
Event:Fortinet-Events:devname	"FGT- syslog"
Event:Fortinet-Events:direction	"incoming"
Event:Fortinet-Events:dtype	"Virus"
Event:Fortinet-Events:eventtype	"infected"
Event:Fortinet-Events:filename	"ms14_064_ole_xp.html"
Event:Fortinet-Events:host	cppm-84.arubasecurity.hpe.com
Event:Fortinet-Events:level	"notice"
Event:Fortinet-Events:msg	"File is infected."
Event:Fortinet-Events:policy_id	1
Event:Fortinet-Events:proto	6
Event:Fortinet-Events:quarantine_skip	"Quarantine-disabled"
Event:Fortinet-Events:service	"HTTP"
Event:Fortinet-Events:session_id	136652

Event:Fortinet-Events:quarantine_skip	"Quarantine-disabled"
Event:Fortinet-Events:service	"HTTP"
Event:Fortinet-Events:session_id	136652
Event:Fortinet-Events:source_interface	"port2"
Event:Fortinet-Events:source_interface_role	"undefined"
Event:Fortinet-Events:source_ip	172.16.99.17
Event:Fortinet-Events:source_port	42830
Event:Fortinet-Events:subtype	"virus"
Event:Fortinet-Events:syslog_priority	13
Event:Fortinet-Events:vd	"root"
Event:Fortinet-Events:virus	"VBS/Agent.QSF!tr.dldr"
Event:Fortinet-Events:virus_id	8160367
Event:MAC-Address	7e054b7e8c35
Event:Pattern-Name	Fortinet-Events
Event:Source-IP-Address	172.16.99.17
Event:Timestamp	2022-11-09 13:02:30
Event:Username	hulk
Tips:Service	Ingress-Event

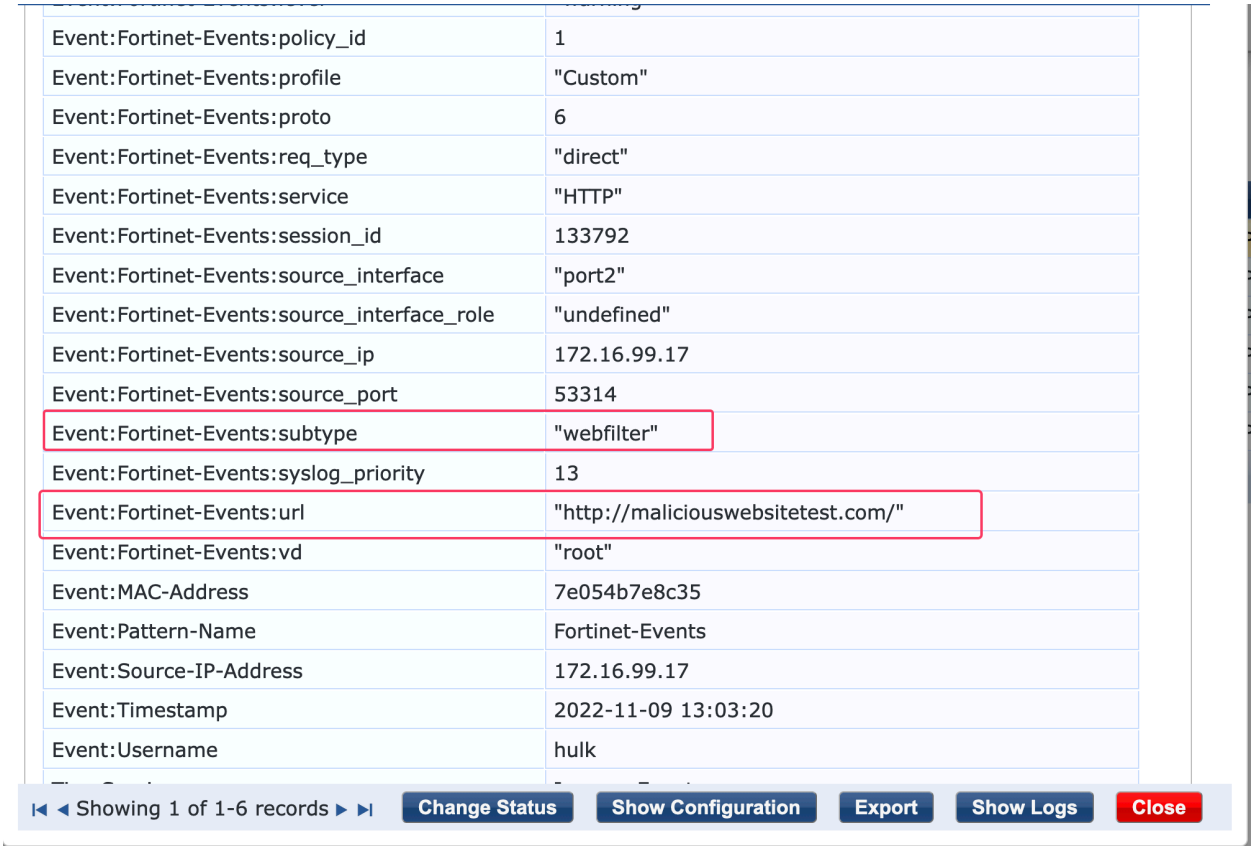
◂ Showing 2 of 1-6 records ▸ | Change Status | Show Configuration | Export | Show Logs | Close

4. Malicious Website Test

Request Details

Summary | Input | Output

Event:Destination-IP-Address	50.63.7.226
Event:Event-Name	"FGT- syslog"
Event:Fortinet-Events:action	"blocked"
Event:Fortinet-Events:category_description	"Malicious Websites"
Event:Fortinet-Events:cr_action	4194304
Event:Fortinet-Events:cr_level	"high"
Event:Fortinet-Events:cr_score	30
Event:Fortinet-Events:destination_interface	"port1"
Event:Fortinet-Events:destination_interface_role	"undefined"
Event:Fortinet-Events:destination_ip	50.63.7.226
Event:Fortinet-Events:destination_port	80
Event:Fortinet-Events:devname	"FGT- syslog"
Event:Fortinet-Events:eventtype	"ftgd_blk"
Event:Fortinet-Events:host	cppm-84.arubasecurity.hpe.com
Event:Fortinet-Events:hostname	"maliciouswebsitetest.com"
Event:Fortinet-Events:level	"warning"
Event:Fortinet-Events:policy_id	1
Event:Fortinet-Events:profile	"Custom"
Event:Fortinet-Events:proto	6
Event:Fortinet-Events:req_type	"direct"



Event:Fortinet-Events:policy_id	1
Event:Fortinet-Events:profile	"Custom"
Event:Fortinet-Events:proto	6
Event:Fortinet-Events:req_type	"direct"
Event:Fortinet-Events:service	"HTTP"
Event:Fortinet-Events:session_id	133792
Event:Fortinet-Events:source_interface	"port2"
Event:Fortinet-Events:source_interface_role	"undefined"
Event:Fortinet-Events:source_ip	172.16.99.17
Event:Fortinet-Events:source_port	53314
Event:Fortinet-Events:subtype	"webfilter"
Event:Fortinet-Events:syslog_priority	13
Event:Fortinet-Events:url	"http://maliciouswebsitetest.com/"
Event:Fortinet-Events:vd	"root"
Event:MAC-Address	7e054b7e8c35
Event:Pattern-Name	Fortinet-Events
Event:Source-IP-Address	172.16.99.17
Event:Timestamp	2022-11-09 13:03:20
Event:Username	hulk