CISCO ASA SAMPLES:

FTP DATA TRANSFER:

Jul 16 11:56:41 alienvault %ASA-6-303002: FTP connection from inside:192.168.1.100/3330 to outside:176.204.244.50/21, user demoftp Retrieved file demodda.pgp

Blacklisted URL WITH OTX:

Data source name: cisco-asa

Event Type ID: 338008

Data source ID: 8005

Jul 16 11:56:38 alienvault %ASA-4-338008: Dynamic Filter dropped blacklisted TCP traffic from inside:192.168.1.100/56450 (91.252.90.11/56450) to outside:5.104.175.235/80 (5.104.175.235/80), destination 5.104.175.235 resolved from dynamic list: 5.104.175.235/255.255.255.255, threat-level: very-high, category: Malware

Jul 24 10:19:58 alienvault %ASA-4-338008: Dynamic Filter dropped blacklisted TCP traffic from inside:192.168.100.76/56450 (147.78.18.184/56450) to outside:195.154.240.80/80 (195.154.240.80/80), destination 195.154.240.80 resolved from dynamic list: 195.154.240.80/255.255.255.255, threat-level: very-high, category: Malware

FORTIGATE LOG SAMPLE:

Jul 24 11:10:21 alienvault date=2014-05-11 time=18:52:15 devname=JLL\_FW devid=FG200B3910602686 logid=0419016384 type=utm subtype=ips eventtype=signature level=alert vd="root" severity=low srcip=210.211.97.223 dstip=192.168.100.45 srcintf="port2" dstintf="Vlan\_3" policyid=49 identidx=0 sessionid=388914 status=detected proto=6 service=http count=1 attackname="ZmEu.Vulnerability.Scanner" srcport=38281 dstport=80 attackid=30024 sensor="all\_default\_pass" ref="http://www.fortinet.com/ids/VID30024" incidentserialno=1432164121 msg="web\_app3: ZmEu.Vulnerability.Scanner,"

ARUBA EXAMPLE:

DSN: ARUBA-6.X

DATA SOURCE ID: 1624

Jul 24 08:38:28 alienvault sapd[920]: <127000> <ERRS> |AP HWISE-d8:c7:c8:ce:dc:78@192.168.100.37 sapd| |ids-ap| AP(d8:c7:c8:6d:c7:80): Rogue AP: An AP classified an access point(BSSID 00:1d:7e:53:92:a6 and SSID linksys on CHANNEL 6) as rogue because it matched the MAC (00:1d:7e:53:92:a6) with IP (192.168.100.43)

ORACLE EXAMPLE:

DSN: ORACLE

DATA SOURCE ID: 1651

Jul 24 10:02:41 alienvault Oracle Audit[2063]: SESSIONID: 333 ENTRYID: 1 STATEMENT: 1 USERID: SANTIAGO ACTION: 100 RETURNCODE: 0 COMMENT$TEXT: Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=192.168.100.70)(PORT=42731)) PRIV$USED: 5