SIEM_Logs_Incident_ByteBistro_Oct31_2025

Oct 31 09:44:05.003 workstation26 (10.0.0.26) dns: query[0x1a2b] A? www.bytebistro.com from 10.0.0.26 (workstation26) to 8.8.8.8:53
Oct 31 09:44:05.006 dns.google dns: response[0x1a2b] A 203.0.113.55 to 10.0.0.26 (workstation26):53

Oct 31 09:44:06.200 httpd[2345]: access_log: 10.0.0.26 (workstation26) - - [31/Oct/2025:09:44:06 +0000] "GET / HTTP/1.1" 200 14432 "-" "Mozilla/5.0 (Windows)"
Oct 31 09:44:10.500 httpd[2345]: access_log: 10.0.0.27 (workstation27) - - [31/Oct/2025:09:44:10 +0000] "GET /about HTTP/1.1" 200 8520 "-" "Mozilla/5.0 (Windows)"

Oct 31 09:46:00.150 kernel[web-prod-01.bytebistro.com] : TCP: Possible SYN flooding on port 80. Check SNMP counters.
Oct 31 09:46:00.200 kernel[web-prod-01.bytebistro.com] : tcp_listen_port_release: backlog limit reached for port 80
Oct 31 09:46:00.203 kernel[web-prod-01.bytebistro.com] : nf_conntrack: table full, dropping packet.
Oct 31 09:46:00.205 ss[web-prod-01.bytebistro.com]   : SYN-RECV 10240 0 0.0.0.0:80 198.51.100.200:51021
Oct 31 09:46:00.206 ss[web-prod-01.bytebistro.com]   : SYN-RECV 10235 0 0.0.0.0:80 203.0.113.45:40001
Oct 31 09:46:00.207 ss[web-prod-01.bytebistro.com]   : SYN-RECV 10230 0 0.0.0.0:80 198.51.100.71:60012

Oct 31 09:46:01.100 httpd[2345]: access_log: 192.0.2.22 (monitor) - - [31/Oct/2025:09:46:01 +0000] "GET /favicon.ico HTTP/1.1" 503 178 "-" "monitor/1.0"
Oct 31 09:46:01.250 httpd[2345]: access_log: 192.0.2.33 (bot) - - [31/Oct/2025:09:46:01 +0000] "GET / HTTP/1.1" 502 512 "-" "Mozilla/5.0 (bot)"

Oct 31 09:46:02.200 suricata: ALERT [1:1000001:0] "SYN flood detected" src_net=203.0.113.0/24 dst=203.0.113.55 pps=24600 distinct_src=1520
Oct 31 09:46:02.500 splunk: correlation:alert id=INC-4532 severity=critical msg="Correlated event: HIGH SYN RATE -> www.bytebistro.com (203.0.113.55) per kernel + web 5xx + IDS"
Oct 31 09:46:03.000 itsm: ticket INC-4532 created Priority=P1 Assigned=NetworkOps msg="Auto-created by SOC: High SYN flood"

Oct 31 09:47:00.200 kernel[web-prod-01.bytebistro.com] : net.ipv4.tcp_syncookies=1 (enabled)
Oct 31 09:47:05.500 httpd[2345]: access_log: 198.51.100.50 (healthcheck) - - [31/Oct/2025:09:47:05 +0000] "GET / HTTP/1.1" 200 14432 "-" "HealthCheck/1.0"
Oct 31 09:47:06.000 splunk: event msg="INC-4532 updated: mitigations applied; monitoring continues"
Oct 31 09:48:00.000 itsm: INC-4532 resolved resolution="Syncookies & upstream filtering; post-incident review arranged"

Oct 31 09:48:30.000 splunk: event msg="Wireshark/tcpdump capture uploaded: snippet_oct31_0944.pcap (size 2.1MB); parsed with Suricata; 5,120 SYN packets identified and correlated with kernel and web logs"