Suricata Log Analysis Results

Non-Batched

Analyzing eve-2025-11-03-0114.json ....

Severity

The provided logs indicate two different severity ratings for the same network event. The first log, with signature ID 2008116 ("ET TFTP Outbound TFTP Write Request"), has a severity rating of 1, categorized as a "Potential Corporate Privacy Violation." The second log, with signature ID 2100518 ("GPL TFTP Put"), has a severity rating of 2, categorized as "Potentially Bad Traffic."
In Suricata, a lower numerical value typically signifies a higher severity. Therefore, the alert for "ET TFTP Outbound TFTP Write Request" (severity 1) indicates a more critical event than the "GPL TFTP Put" alert (severity 2), both originating from the same outbound TFTP write request from 192.168.0.1 to 192.168.0.13.

Type

These alerts are false positives. Both alerts correlate to the same TFTP write request occurring between two internal IP addresses (192.168.0.1 to 192.168.0.13). However, the rules are designed to detect TFTP traffic either moving from an internal network to an external one (ET TFTP Outbound TFTP Write Request) or originating from an external network to an internal one (GPL TFTP Put), which does not align with the observed internal-to-internal communication.

Summary of events

At 2013-04-27T09:07:59, Suricata detected a TFTP Write Request from 192.168.0.1 (source port 57509) to 192.168.0.13 (destination port 69) over UDP, specifically attempting to write a file named "rfc1350.txt". This single network event triggered two distinct alerts: "ET TFTP Outbound TFTP Write Request" (categorized as a "Potential Corporate Privacy Violation") and "GPL TFTP Put" (categorized as "Potentially Bad Traffic"). Both alerts indicate that the traffic was allowed by the security system.

Recommendations:

These correlated alerts indicate that an internal host (192.168.0.1) initiated an insecure TFTP write request to another internal host (192.168.0.13) for "rfc1350.txt", categorized as a potential privacy violation and bad traffic. Remediation should focus on investigating the legitimacy and purpose of this specific TFTP activity. If TFTP is not authorized or necessary, block UDP port 69 on the affected hosts or network segments; otherwise, replace TFTP with a more secure, authenticated file transfer protocol like SFTP or SCP.

Analyzing eve-2025-11-03-0052.json ....

Severity

The highest severity rating found across these correlated log entries is 1, associated with the alert "ET HUNTING SQL Database Version Discovery," which is categorized as an "Attempted User Privilege Gain." This critical alert, alongside "ET SCAN Suspicious inbound to mySQL port 3306" (severity 2) and "GPL SQL MYSQL show databases attempt" (severity 3), indicates a suspicious and potentially malicious attempt to enumerate and gain information about the SQL database. All three alerts are correlated to the same network flow (flow_id 303369210772878) targeting port 3306 on 192.168.0.254, with the latter two sharing the exact same timestamp and payload data.

Type

These alerts collectively represent a true positive. The initial "Suspicious inbound to mySQL port 3306" alert is immediately followed by alerts for "SQL Database Version Discovery" and "GPL SQL MYSQL show databases attempt" within the same network flow. The payload explicitly shows SQL commands such as select @@version_comment, SELECT DATABASE(), show databases, and show tables, which are clear indicators of reconnaissance and potential exploitation attempts against the MySQL server.

Summary of events

These logs detail a series of reconnaissance activities originating from 192.168.0.254 targeting a MySQL service on the same IP address. Initially, a suspicious connection attempt to port 3306 was observed. This was followed by more aggressive actions within the same network flow, including attempts to discover the database version and enumerate available databases, as indicated by the "SQL Database Version Discovery" and "GPL SQL MYSQL show databases attempt" alerts and the contained SQL commands like select @@version_comment limit 1 and show databases.

Recommendations:

The logs show that host 192.168.0.254 is performing suspicious scans and active SQL enumeration attempts, including database version discovery and show databases queries, against its own MySQL service on port 3306. Remediation should begin with isolating 192.168.0.254 from the network to prevent further potential compromise or malicious activity. Subsequently, conduct a thorough forensic investigation of the host to determine the source of these attempts (e.g., compromised process, misconfigured application, or malicious user) and apply appropriate security patches and stricter access controls to the MySQL database.

Analyzing eve-2025-11-03-0044.json ....

Severity

Both logs indicate a severity rating of 3 and are categorized as "Informational" by the signature_severity metadata. This suggests a low severity, as the alerts are for "ET INFO Internet Printing Protocol (IPP) Get-Printer-Attributes Outbound Request," which typically signifies routine network activity rather than a direct threat. The action for both alerts is "allowed," further indicating that these are informational observations of standard IPP communication from 10.10.10.49 to 10.10.10.251 over port 631.

Type

This alert should be marked as a True Positive.
The Suricata alert with signature_id 2056212 is designed to detect "ET INFO Internet Printing Protocol (IPP) Get-Printer-Attributes Outbound Request." Both logs show a src_ip 10.10.10.49 making a POST request to dest_ip 10.10.10.251 on port 631 (standard IPP port), with a Content-Type: application/ipp and User-Agent: CUPS/1.3.4. Crucially, the payload in both instances explicitly includes requested-attributes for printer-attributes, indicating the exact type of IPP request the alert signature describes. Since the alert accurately identifies the specific IPP activity it is configured to detect, it is a true positive, despite being informational in nature.

Summary of events

These logs show a client at 10.10.10.49 making two separate Internet Printing Protocol (IPP) Get-Printer-Attributes requests to a server at 10.10.10.251 on port 631, both detected as "ET INFO Internet Printing Protocol (IPP) Get-Printer-Attributes Outbound Request". The first request queries general printer capabilities, while the second, occurring shortly after, specifically queries job-related attributes for a "guest" user, both initiated by a CUPS client and allowed.

Recommendations:

Given that these alerts are informational (severity 3) and describe standard Internet Printing Protocol (IPP) Get-Printer-Attributes requests from CUPS, the activity appears legitimate and allowed. No immediate remediation is required beyond verifying that the IPP traffic between 10.10.10.49 and 10.10.10.251 is expected. If confirmed as legitimate, consider adjusting or suppressing this specific informational rule (sid: 2056212) to reduce alert noise.

Analyzing eve-2025-11-03-0022.json ....

Severity

The first log, {"timestamp":"2017-02-02T15:25:32.340685+0000", ...} has an assigned severity rating of 3, categorized as "Not Suspicious Traffic" for an "ET INFO Spotify P2P Client" alert.

The second log, {"timestamp":"2017-02-02T15:25:42.097229+0000", ...} and the third log, {"timestamp":"2017-02-02T15:25:44.159119+0000", ...} both have an assigned severity rating of 2. These two logs are correlated as they share the same flow_id (1674331865711969) and indicate multiple "GPL WEB_SERVER DELETE attempt" alerts from 10.142.160.1 to 10.142.160.101 within the same network session, categorized as "access to a potentially vulnerable web application."

Type

Here is the analysis of each Suricata alert:

Log 1 (Signature: ET INFO Spotify P2P Client): This alert is a True Positive. The alert accurately identifies "Spotify P2P Client" traffic, and its category is explicitly stated as "Not Suspicious Traffic." Since the rule's purpose is to detect and classify this specific type of benign network activity, the alert correctly fired for its intended informational purpose.

Log 2 & 3 (Signature: GPL WEB_SERVER DELETE attempt): Both of these alerts are True Positives. The payload_printable clearly shows HTTP DELETE requests originating from 10.142.160.1 to 10.142.160.101 on port 8091, which perfectly matches the signature's intent to detect "WEB_SERVER DELETE attempt." Given the alert's category, "access to a potentially vulnerable web application," this activity is considered noteworthy and potentially suspicious.

Correlation: Logs 2 and 3 show correlated activity. They share the same flow_id (1674331865711969), source (10.142.160.1:54932), and destination (10.142.160.101:8091), indicating multiple "GPL WEB_SERVER DELETE attempt" alerts occurred within the same network conversation over a short period (approximately two seconds apart).

Summary of events

Here's an explanation of the logs:
The first log indicates that Suricata detected and allowed "ET INFO Spotify P2P Client" traffic originating from 10.142.160.1 and broadcasting on UDP port 57621 to 10.142.160.255. Although flagged as an alert, it's categorized as "Not Suspicious Traffic," suggesting a Windows client is running the Spotify application.

The second log shows an alert for a "GPL WEB_SERVER DELETE attempt" from 10.142.160.1 to 10.142.160.101 on port 8091, specifically an HTTP DELETE request to /pools/default/buckets/default/docs/app. This action, categorized as "access to a potentially vulnerable web application," was allowed by the rule.
The third log is another "GPL WEB_SERVER DELETE attempt" from the same source and destination as the second log, but this time it includes an HTTP DELETE request targeting /pools/default/buckets/default/docs/apple. This alert also categorizes the activity as "access to a potentially vulnerable web application" and was allowed.
Logs two and three are correlated as they share the same flow_id, source and destination IPs/ports, and signature, indicating multiple "GPL WEB_SERVER DELETE attempt" actions occurred within the same TCP connection or HTTP session from 10.142.160.1 targeting different resources on 10.142.160.101.

Recommendations:

For the "ET INFO Spotify P2P Client" alert, remediation involves reviewing organizational policy regarding peer-to-peer applications. If disallowed, the Spotify client or its associated traffic should be blocked on the network for IP 10.142.160.1, and the user should be educated on acceptable software usage.
The "GPL WEB_SERVER DELETE attempt" alerts (correlated by flow_id 1674331865711969 across the two logs) from 10.142.160.1 targeting 10.142.160.101 indicate unauthorized attempts to delete data. Remediation requires immediately isolating or blocking 10.142.160.1 from the web server 10.142.160.101, then thoroughly investigating the source for compromise and the web server for vulnerabilities and any successful data deletions. Stricter access controls should be applied to the web server to restrict HTTP DELETE method usage.

Analyzing eve-2025-11-02-2252.json ....

Severity

This log is assigned a severity rating of 1, which is categorized as "Informational." This rating indicates that the event is a "Potential Corporate Privacy Violation" due to the detection of an iTunes User Agent. The signature severity metadata further confirms this as "Informational."

Type

This alert should be marked as a True Positive. The Suricata rule ET INFO iTunes User Agent is designed to detect the presence of "iTunes" in the User-Agent string, and the log clearly shows User-Agent: iTunes/10.6. The alert correctly identified this specific activity, which the rule itself categorizes as a "Potential Corporate Privacy Violation" and a "policy-violation."

Summary of events

This Suricata log indicates an alert for a "Potential Corporate Privacy Violation" due to the detection of an "ET INFO iTunes User Agent." An internal host, 192.168.3.107, communicated with another internal host, 192.168.3.123, over TCP on destination port 5000, sending an HTTP (RTSP) request with a "User-Agent: iTunes/10.6" header, which triggered the informational alert. The connection was allowed to proceed.

Recommendations:

This alert, categorized as a "Potential Corporate Privacy Violation" due to an "iTunes User Agent," indicates informational activity rather than a direct threat. Remediation involves verifying if iTunes usage aligns with internal corporate policy. If not permitted, consider updating the policy, educating users, and potentially implementing firewall rules to block iTunes-related traffic.

Analyzing eve-2025-11-03-0112.json ....

Severity

The log explicitly assigns a severity rating of 1 within the alert section. This is further categorized as an "Informational" signature severity and falls under the "Potential Corporate Privacy Violation" category.

Type

This alert indicates a TFTP read request for "rfc1350.txt" from 192.168.0.253 to 192.168.0.10. The signature "ET TFTP Outbound TFTP Read Request" and its corresponding rule are designed to flag TFTP traffic to $EXTERNAL_NET. However, since both the source and destination IP addresses (192.168.0.253 and 192.168.0.10) are private RFC 1918 addresses, this traffic is likely internal to the network, not "outbound" to an external destination. Therefore, this alert is a false positive as the traffic does not match the "outbound" nature implied by the rule.

Summary of events

At 2013-05-01T12:24:11.972852+0000, Suricata generated an alert for an "ET TFTP Outbound TFTP Read Request." An internal host, 192.168.0.253, initiated a TFTP read request to 192.168.0.10 on UDP port 69, specifically attempting to read the file "rfc1350.txt." This event, categorized as a "Potential Corporate Privacy Violation" with informational severity, was allowed by the security system.

Recommendations:

This log indicates an allowed outbound TFTP read request, flagged as a "Potential Corporate Privacy Violation." The primary remediation is to investigate the legitimacy of this TFTP activity from 192.168.0.253 to 192.168.0.10. If unauthorized, block outbound TFTP traffic at the network perimeter and internal firewalls, and enforce the use of more secure file transfer protocols like SFTP or SCP for any necessary transfers.

Analyzing eve-2025-11-03-0013.json ....

Severity

This log has an assigned severity rating of 3. The alert metadata further classifies this as "Informational," indicating it's a low-impact event typically used for monitoring specific protocol commands like SMB IPC$ share access.

Type

This alert would likely be marked as a False Positive. While the alert accurately detected SMB IPCshareaccessasdescribedbyitssignature,accessingtheIPC share access as described by its signature, accessing the IPCshareaccessasdescribedbyitssignature,accessingtheIPC share is a common and often legitimate operation within Windows environments for interprocess communication. The alert's "Informational" severity also suggests it's likely flagging benign network activity rather than a true security incident, given the lack of other correlating malicious indicators in the provided log.

Summary of events

This Suricata log indicates an informational alert for "GPL NETBIOS SMB IPC$ share access." A TCP connection from 192.168.29.1 (port 1107) to 192.168.29.133 (port 139), which is commonly used for SMB, triggered this alert. The action was allowed, meaning the network traffic was permitted to pass, and the alert is categorized as Generic Protocol Command Decode.

Recommendations:

This log indicates an informational alert regarding an allowed SMB IPCshareaccessbetween‘192.168.29.1‘and‘192.168.29.133‘onport139.Givenitsinformationalseverity,itisrecommendedtofirstverifyifthisSMBIPC share access between `192.168.29.1` and `192.168.29.133` on port 139. Given its informational severity, it is recommended to first verify if this SMB IPCshareaccessbetween‘192.168.29.1‘and‘192.168.29.133‘onport139.Givenitsinformationalseverity,itisrecommendedtofirstverifyifthisSMBIPC share access is legitimate and expected for these systems. If this communication is not intended or necessary, consider restricting SMB access to only authorized hosts or disabling SMB services on the destination system (192.168.29.133) if they are not required to reduce the attack surface.

Analyzing eve.json ....

Severity

This log collection indicates a Critical severity rating. Multiple internal hosts (192.168.3.35, 192.168.3.25, 192.168.3.65) are identified with active malware infections, including Zbot and Nemucod, engaging in Command and Control (C2) communication and downloading executables. The detection of packed executables with anti-debugging techniques further emphasizes the sophisticated and malicious nature of the detected activity.

Type

This alert should be marked as a True Positive. The Suricata rule correctly identified a DNS query for checkip.dyndns.org from 192.168.1.101, which is explicitly stated in the alert's signature and payload.
While checkip.dyndns.org can be used for legitimate purposes, the alert accurately categorizes this activity as "Reconnaissance" (MITRE T1590), indicating the device is "Retrieving External IP Address." Given the multitude of high-severity malware and suspicious activities (Trojan, Zbot, P2P, SMB attacks, PE downloads) occurring simultaneously from other internal hosts in the network, this reconnaissance-level alert from 192.168.1.101 is likely part of a broader malicious campaign or compromise, making its detection accurate and relevant to security analysis.

Summary of events

Here's an explanation of each log entry:

Log 1: An internal host, 192.168.1.101, performed a DNS query to an external server (65.32.5.111) for "checkip.dyndns.org". This activity is flagged as an informational alert for "Device Retrieving External IP Address Detected," indicating a system is attempting to discover its public IP address.

Logs 2-4: An internal host (192.168.3.35) initiated an HTTP GET request to acxerox.com (195.2.253.92) using a suspicious User-Agent (ver49). This request is simultaneously identified by three alerts as a "Possible Trojan Downloader," "Tibs/Harnig Downloader Activity," and "Hiloti Style GET to PHP," strongly suggesting a malicious download attempt.

Logs 5-7: From the same internal host (192.168.3.35), a concurrent HTTP GET request was made to acxerox.com (195.2.253.92) for a different PHP file (/tdfpmmn/hnkppz.php). Similar to the previous incident, this request triggered alerts for a "Suspicious User-Agent," "Tibs/Harnig Downloader Activity," and "Hiloti Style GET to PHP," indicating multiple, simultaneous malware download attempts from the same source.

Logs 8-9: These logs are the server's response to the request in logs 5-7. The external server (195.2.253.92) sent a Windows executable file (hnkppz.php) to 192.168.3.35, despite declaring its content type as "text/html." Suricata correctly identified this as a "Possible Windows executable sent when remote host claims to send html content" and a "PE EXE or DLL Windows file download," confirming successful malware delivery.

Logs 10-11: This is the server's response to the request in logs 2-4. The external server (195.2.253.92) delivered another Windows executable (hohhveswgc.php) to 192.168.3.35, again mislabeling it as "text/html." Like the previous response, this was flagged as a "Windows file download" and a "Possible Windows executable sent when remote host claims to send html content," indicating another instance of successful malware delivery.

Logs 12-14: Another HTTP GET request from 192.168.3.35 to acxerox.com (195.2.253.92) for /tdfpmmn/wtqanbo.php was detected, exhibiting the same "Suspicious User-Agent," "Tibs/Harnig Downloader Activity," and "Hiloti Style GET to PHP" characteristics. This signals continued and persistent attempts by the client to download malicious payloads.

Logs 15-18: A fourth distinct HTTP GET request from 192.168.3.35 to acxerox.com (195.2.253.92) for /tdfpmmn/bhanx.php triggered four alerts. These alerts, including "ET MALWARE TrojanDownloader Win32/Harnig.gen-P Reporting," confirm the malicious nature of the traffic and specifically identify it as command and control (C2) activity for Win32/Harnig malware.

Logs 19-20: The internal host 192.168.3.35 made yet another HTTP GET request to acxerox.com (195.2.253.92) for /tbuhrblyis/flvfbp.php, again using a suspicious User-Agent. This event is categorized as a "Possible Trojan Downloader" and "Hiloti Style GET to PHP," indicating ongoing attempts to retrieve malicious payloads.

Log 21: An internal host (192.168.3.35) sent an HTTP POST request to go-thailand-now.com (96.0.203.90), including a "UA-CPU: x86" header. This activity is classified as "ET INFO Observed UA-CPU Header," which is an informational alert for miscellaneous network activity.

Logs 22-25, 34-35, 45-52: Multiple internal hosts (192.168.10.127, .128, .120, .125, .126, .129) are repeatedly attempting IPCunicodeshareaccesstootherinternalhosts(192.168.10.101,192.168.10.102)overSMB/NetBIOS. These"GPLNETBIOSSMB−DSIPC unicode share access to other internal hosts (192.168.10.101, 192.168.10.102) over SMB/NetBIOS. These "GPL NETBIOS SMB-DS IPCunicodeshareaccesstootherinternalhosts(192.168.10.101,192.168.10.102)overSMB/NetBIOS. These"GPLNETBIOSSMB−DSIPC unicode share access" alerts indicate active network enumeration or lateral movement attempts within the internal network.

Logs 26, 36: Internal host 192.168.10.128 is observed communicating with an external IP (64.127.109.133) via HTTP using a "BTWebClient" User-Agent. These alerts are flagged as "ET P2P BTWebClient UA uTorrent in use," indicating a potential corporate policy violation related to BitTorrent client usage.

Log 27: The internal host 192.168.10.128 is sending a BitTorrent DHT ping request to an external IP (72.20.34.145) on port 6881. This "ET P2P BitTorrent DHT ping request" is flagged as a potential corporate privacy violation due to active peer-to-peer network activity.

Logs 28-33, 40, 48-51: Multiple internal hosts (192.168.10.124, 192.168.10.125, 192.168.10.127, 192.168.10.128) are attempting UPnP SUBSCRIBE requests to 192.168.10.100 on port 2869. These repeated alerts for "ET SCAN UPnP SUBSCRIBE Inbound - Possible CallStranger Scan (CVE-2020-12695)" suggest an active reconnaissance or exploitation attempt targeting UPnP services on the host.

Logs 37-38: Internal host 192.168.10.128 initiated a BitTorrent announce request to bttracker.debian.org (130.239.18.173) on port 6969. This activity is flagged by two signatures, "ET P2P BitTorrent Announce" and "GPL P2P BitTorrent announce request," indicating P2P file sharing and a potential corporate privacy violation.

Logs 39-40: Internal host 192.168.10.128 requested and successfully downloaded a BitTorrent torrent file (debian-500-i386-CD-1.iso.torrent) from cdimage.debian.org (130.239.18.173). These alerts, "ET P2P Possible Torrent Download via HTTP Request" and "ET P2P BitTorrent - Torrent File Downloaded," confirm active BitTorrent usage and a potential corporate privacy violation.

Logs 41-43, 53, 54, 79: Internal host 192.168.10.128 is actively engaged in BitTorrent peer synchronization, DHT announce_peers requests, and BitTorrent protocol transfers with various external IP addresses and ports. These alerts signify ongoing peer-to-peer file sharing activities, consistently flagged as potential corporate privacy violations.

Logs 55-58: Internal host 192.168.10.124 is attempting to access SNMP services on 10.40.0.103 using the common "public" community string. This "GPL SNMP public access udp" alert indicates an attempted information leak or reconnaissance against an SNMP-enabled device.

Logs 59-60: Internal host 192.168.10.128 explicitly requested an executable file (mirc635.exe) via FTP from an external server (130.89.149.129), which then responded by sending a Windows executable over raw TCP. This sequence of "ET INFO .exe File requested over FTP" and "ET HUNTING PE EXE Download over raw TCP" indicates a successful download of an executable file onto the internal host.

Log 61: Internal host 192.168.3.35 requested a .bin file (cfg3.bin) via HTTP from kloretukap.net (188.124.5.107). This is detected as "ET MALWARE Zbot Generic URI/Header Struct .bin," indicating a potential Zbot malware download attempt.

Logs 62-63, 65-66, 68, 71, 75, 78: Multiple internal hosts (192.168.3.35, 192.168.3.25, 192.168.3.65) are making HTTP POST requests to external C2 servers (homesitetoo.com, pipiskin.hk, ishi-bati.com) for PHP files (stat1.php, index1.php, youyou.php). These repeated "ET MALWARE Zbot POST Request to C2" alerts indicate active command and control communication associated with Zbot malware from compromised internal hosts.

Logs 64, 79-80: Internal host 192.168.3.35 requested an executable file (/40.exe) via HTTP from solaruploader.com (188.124.9.56), which then delivered the file identified as application/x-msdownload. These alerts, including "ET MALWARE JS/Nemucod requesting EXE payload" and "ET MALWARE JS/Nemucod.M.gen downloading EXE payload," confirm the successful download of a Nemucod malware variant.

Logs 67: An external server (89.187.51.0) sent a Windows executable file (load.exe) to 192.168.3.25, identified as application/octet-stream. This "ET INFO PE EXE or DLL Windows file download HTTP" alert indicates the successful delivery of an executable file, likely malicious.

Logs 69-70: Internal host 192.168.3.65 made an HTTP GET request to ishi-bati.com (188.72.243.72) for a .bin file (kartos.bin). These alerts, "ET MALWARE Possible Zbot Activity Common Download Struct" and "ET MALWARE Zbot Generic URI/Header Struct .bin," suggest a Zbot malware download attempt.

Logs 72-74, 76-77: Internal host 192.168.3.65 is engaging in active malware downloading, requesting and receiving executables (krt.exe, ser.exe) from ishi-bati.com. The downloaded krt.exe (logs 74) is identified with multiple malicious characteristics, including

"IsDebuggerPresent" (anti-debugging) and "Packed Executable Download," strongly indicating a sophisticated malware payload.

Recommendations:

These logs indicate multiple active malware infections (Zbot, Nemucod, Tibs/Harnig) across several internal hosts (192.168.3.35, 192.168.3.25, 192.168.3.65), evidenced by suspicious HTTP requests, executable downloads (some disguised as HTML), and Command & Control (C2) communication.
Immediate remediation requires isolating the infected hosts to prevent further spread and conducting a thorough forensic analysis to eradicate the malware. Furthermore, block all identified malicious external IPs and domains at the network perimeter, and implement stronger endpoint security controls to prevent similar incidents.

Batched

Analyzing eve-2025-11-03-0114.json ....

Based on the provided Suricata log entries, here is the analysis:
Both log entries refer to the same network event, as indicated by identical timestamp, flow_id, src_ip, src_port, dest_ip, dest_port, proto, app_proto, payload_printable, and packet fields. This means two different Suricata rules fired on the same TFTP write request.

Log Entry 1 (Correlation for both entries):

Severity Rating:
High (Alert severity: 1 as indicated by the "ET TFTP Outbound TFTP Write Request" signature). This is the highest severity level in Suricata's 1-3 scale.

Mark this alert true positive, false positive, false negative, or true negative?
True Positive.
The alert correctly identifies a TFTP write request, which is an inherently insecure operation. While the activity might be legitimate within the network's operational context, it is a "Potential Corporate Privacy Violation" and "Potentially Bad Traffic" as per the alert categories. Therefore, the alert accurately detected a type of traffic that warrants security scrutiny, making it a true

positive detection of a potentially risky event. Further investigation is needed to determine if this specific instance is benign or malicious.

Explain what is happening in this log.
At 2013-04-27T09:07:59.452740+0000, an internal host with the IP address 192.168.0.1 initiated a TFTP (Trivial File Transfer Protocol) write request to another internal host, 192.168.0.13, on UDP port 69 (the standard TFTP port). The client (192.168.0.1) is attempting to transfer or "put" a file named rfc1350.txt onto the TFTP server running on 192.168.0.13.
Two Suricata rules were triggered by this single event:

ET TFTP Outbound TFTP Write Request (signature_id: 2008116): This rule detected an outbound TFTP write request originating from what Suricata considers HOME_NET. It categorized this as a "Potential Corporate Privacy Violation" and assigned a high severity (1).
GPL TFTP Put (signature_id: 2100518): This rule also detected a TFTP Put (write) operation, categorizing it as "Potentially Bad Traffic" with a medium severity (2). It additionally references CVE-1999-0183, which relates to vulnerabilities in TFTP servers.

Both alerts indicate that the traffic was allowed to proceed, meaning the file transfer was not blocked by Suricata. This activity is significant because TFTP is an unauthenticated protocol lacking encryption and robust access controls, making it a common vector for data exfiltration, malware distribution, or unauthorized configuration changes in compromised environments.

What remediation do you recommend for this log?
Immediate Actions (Investigation):

Identify Systems and Owners: Determine the identity and purpose of both 192.168.0.1 and 192.168.0.13 and their respective owners/administrators.
Verify Authorization: Confirm with the system owners or IT staff if this specific TFTP write operation (rfc1350.txt transfer) was expected, authorized, and part of a legitimate business process.
Check for Compromise: If unauthorized, investigate 192.168.0.1 for signs of compromise (e.g., malware, unauthorized user activity) and 192.168.0.13 for any running TFTP server that shouldn't be active or has improper permissions.
Analyze File Content: If the rfc1350.txt file was successfully written, retrieve and analyze its content to determine its nature (e.g., legitimate configuration file, malware, sensitive data).
Review TFTP Server Configuration: Inspect the TFTP server configuration on 192.168.0.13 to understand allowed directories, write permissions, and access controls.

Long-Term Remediation and Hardening:

Disable Unnecessary TFTP: If TFTP is not a required service on 192.168.0.13 or any other host, disable the TFTP server service and block UDP port 69 at relevant firewalls.
Secure Necessary TFTP: If TFTP is essential for specific functions (e.g., network device configuration, PXE boot):
Restrict Access: Configure the TFTP server to only accept connections from explicitly authorized IP addresses or subnets.
Limit Write Access: Configure the TFTP server to operate in read-only mode if write functionality is not needed. If writes are required, restrict them to a very specific, secure directory and only from authorized sources.
Implement Alternatives: Evaluate transitioning to more secure protocols that offer authentication, authorization, and encryption (e.g., SFTP, SCP, HTTPS) for file transfers.

Network Segmentation: Isolate TFTP servers and clients into dedicated network segments or VLANs to limit the blast radius in case of compromise.
Policy Enforcement: Update internal security policies to restrict or prohibit the use of insecure protocols like TFTP, enforcing the use of secure alternatives where possible.
Enhanced Monitoring: Implement additional logging and monitoring for TFTP server access and file transfer activities on 192.168.0.13.

Analyzing eve-2025-11-03-0052.json ....

Here is the analysis of the provided Suricata log entries:

Log Entry 1 Analysis

```
{"timestamp":"2008-07-17T07:50:25.136169+0000","flow_id":303369210772878,"pcap_cnt":1,
"event_type":"alert","src_ip":"192.168.0.254","src_port":56162,"dest_ip":"192.168.0.254","dest
_port":3306,"proto":"TCP","pkt_src":"wire/pcap","community_id":"1:0HUQbshhYbATQXDHv/
ysOs0DlZA=","alert":{"action":"allowed","gid":1,"signature_id":2010937,"rev":3,"signature":"E
T SCAN Suspicious inbound to mySQL port 3306","category":"Potentially Bad
Traffic","severity":2,"metadata":{"confidence":["Medium"],"created_at":["2010_07_30"],"signat
ure_severity":["Informational"],"updated_at":["2019_07_26"]},"rule":"alert tcp
EXTERNALNETany−>EXTERNAL_NET any -> EXTERNALNETany−>HOME_NET 3306
(msg:\"ET SCAN Suspicious inbound to mySQL port 3306\"; flow:to_server; flags:S; threshold:
type limit, count 5, seconds 60, track by_src; classtype:bad-unknown; sid:2010937; rev:3;
```

metadata:created_at 2010_07_30, confidence Medium, signature_severity Informational,
updated_at
2019_07_26;)"},"direction":"to_server","payload_printable":"","stream":0,"packet":"AAAAAA
AAAAAAAAAACABFAAA8ZcNAAEAGUazAqAD+wKgA/ttiDOrM2LtNAAAAAKACgBi6
UQAAAgRADAQCCAoA8N6OAAAAAAEDAwY=","packet_info":{"linktype":1}}

Assign a severity rating to this log.
Medium. The Suricata rule assigns a severity: 2. While the metadata classifies it as "Informational," a "Suspicious scan" targeting a sensitive service like MySQL, especially when the source and destination are the same machine, is noteworthy. When correlated with the subsequent alerts in the same flow, it escalates to a higher concern.

Mark this alert true positive, false positive, false negative, or true negative?
True Positive. Given the progression of events in the correlated logs (initial scan followed by explicit SQL reconnaissance commands), this initial scan activity is indeed suspicious and appears to be part of a malicious or unauthorized sequence.

Explain what is happening in this log.
This log entry indicates that an application or process running on the host 192.168.0.254 is initiating a connection to a MySQL server, which is also running on the same host 192.168.0.254 on port 3306. The Suricata rule ET SCAN Suspicious inbound to mySQL port 3306 has fired because a threshold of SYN packets to the MySQL port was exceeded from the source 192.168.0.254. This suggests a port scan or reconnaissance activity aimed at the local MySQL service. This alert is the first event in a series of correlated activities within the same network flow (flow_id: 303369210772878).

What remediation do you recommend for this log?
Investigate the process on 192.168.0.254 that is generating these connections from source port 56162 to destination port 3306. Check for any unauthorized scripts, applications, or unusual user activity. Review system logs and MySQL server logs on 192.168.0.254 for further context, particularly for authentication attempts or related errors. Given the subsequent alerts, this is likely part of a larger incident requiring immediate attention.

Log Entry 2 Analysis

{"timestamp":"2008-07-17T07:52:04.419116+0000","flow_id":303369210772878,"event_type":
"alert","src_ip":"192.168.0.254","src_port":56162,"dest_ip":"192.168.0.254","dest_port":3306,"
proto":"TCP","pkt_src":"stream (flow
timeout)","community_id":"1:0HUQbshhYbATQXDHv/ysOs0DlZA=","alert":{"action":"allowe

d","gid":1,"signature_id":2062928,"rev":1,"signature":"ET HUNTING SQL Database Version Discovery","category":"Attempted User Privilege Gain","severity":1,"source":{"ip":"192.168.0.254","port":56162},"target":{"ip":"192.168.0.254","port":3306},"metadata":{"attack_target":["Server"],"confidence":["High"],"created_at":["2025_06_13"],"deployment":["Internal","Perimeter"],"performance_impact":["Significant"],"signature_severity":["Informational"],"updated_at":["2025_06_13"]},"rule":"alert tcp any any -> HOME_NET any (msg:\"ET HUNTING SQL Database Version Discovery\"; flow:established,to_server; content:\"select\"; nocase; content:\"version\"; fast_pattern; distance:0; pcre:\"/(?:[sS][eE][lL][eE][cC][tT]|[fF][rR][oO][mM])(?:\\s|\\x2520|[\\x2b\\x7c])+(?:v\\x24(?:version|instance)|\\x40{2}version|version\\x28\\x29)/\"; reference:url,portswigger.net/web-security/sql-injection/cheat-sheet; classtype:attempted-user; sid:2062928; rev:1; metadata:attack_target Server, created_at 2025_06_13, deployment Perimeter, deployment Internal, performance_impact Significant, confidence High, signature_severity Informational, updated_at 2025_06_13; target:dest_ip;)"},"app_proto":"failed","direction":"to_server","payload_printable":">...........!......................tfoerste....mUb....j.A#j..1^..!....select @@version_comment limit 1.....SELECT DATABASE().....test.....show databases.....show tables.....agent......create table foo (id BIGINT(10) UNSIGNED NOT NULL AUTO_INCREMENT PRIMARY KEY, animal VARCHAR(64) NOT NULL, name VARCHAR(64) NULL DEFAULT NULL) ENGINE = MYISAM7....insert into foo (animal, name) values (\"dog\", \"Goofy\"):....insert into foo (animal, name) values (\"cat\", \"Garfield\").....select * from foo'....delete from foo where name like '%oo%'.....delete from foo where id = 1.....select count(*) from foo.....select * from foo.....delete from foo.....drop table foo.....","stream":1,"packet":"RQAAKAAAABABveDwKgA/sCoAP7bYgzqzNi94gAAAABQAAoAr48AAA==","packet_info":{"linktype":1}}```

1. **Assign a severity rating to this log.** High. The Suricata rule assigns a `severity: 1`, indicating high importance. This alert is categorized as "Attempted User Privilege Gain" with "High" confidence. Given that specific SQL queries for version discovery (`select @@version_comment limit 1`, `SELECT DATABASE()`) are present and occurring locally on the host, this indicates a significant security event.2. **Mark this alert true positive, false positive, false negative, or true negative?**   True Positive. The `payload_printable` clearly contains SQL commands designed for database version discovery and enumeration (`select @@version_comment limit 1`, `SELECT DATABASE()`, `show databases`, `show tables`). This activity is a common initial step in SQL injection attacks or unauthorized database access, making the alert accurate.3. **Explain what is happening in this log.**   This log, occurring approximately two minutes after the suspicious scan (Log Entry 1) but within the same network flow, indicates that an entity on `192.168.0.254` is actively attempting to discover the version and structure of the local MySQL database (also on `192.168.0.254`). The `payload_printable` content shows a sequence of SQL commands including `select @@version_comment limit 1` and `SELECT DATABASE()`, which are typical

for reconnaissance. Furthermore, the payload contains much more aggressive commands like `show databases`, `show tables`, `create table foo`, `insert into foo`, `delete from foo`, and `drop table foo`, suggesting a clear intent for comprehensive database enumeration and manipulation, which could lead to data exfiltration, modification, or destruction.4. **What remediation do you recommend for this log?** This log, especially when correlated with the others, points to a likely compromise or malicious local activity on the host `192.168.0.254`. * **Isolate the host `192.168.0.254`** from the network immediately to prevent further compromise or lateral movement. * **Identify the process** on `192.168.0.254` that is originating these database queries. This could be done by examining active connections, process lists, or audit logs. * **Conduct a full forensic investigation** of the host `192.168.0.254` to determine the initial point of compromise, the extent of unauthorized access, and any persistence mechanisms installed. * **Review MySQL server logs** for details of the queries executed, the user accounts used, and any successful or failed authentication attempts related to this activity. * **Implement strong authentication and authorization policies** for MySQL users, adhering to the principle of least privilege. * **Patch and update** all software, especially the MySQL server and any applications that interact with it, to the latest versions to mitigate known vulnerabilities. * **Consider restoring the database** from a trusted backup if data integrity is suspected to be compromised.---### Log Entry 3 Analysis```json{"timestamp":"2008-07-17T07:52:04.419116+0000","flow_id":303369210772878,"event_type":"alert","src_ip":"192.168.0.254","src_port":56162,"dest_ip":"192.168.0.254","dest_port":3306,"proto":"TCP","pkt_src":"stream (flow timeout)","community_id":"1:0HUQbshhYbATQXDHv/ysOs0DlZA=","alert":{"action":"allowed","gid":1,"signature_id":2101776,"rev":5,"signature":"GPL SQL MYSQL show databases attempt","category":"Generic Protocol Command Decode","severity":3,"metadata":{"created_at":["2010_09_23"],"signature_severity":["Informational"],"updated_at":["2024_03_08"]},"rule":"alert tcp $EXTERNAL_NET any -> SQL_SERVERS 3306 (msg:\"GPL SQL MYSQL show databases attempt\"; flow:established,to_server; content:\"|0F 00 00 00 03|show databases\"; classtype:protocol-command-decode; sid:2101776; rev:5; metadata:created_at 2010_09_23, signature_severity Informational, updated_at 2024_03_08;)"},"app_proto":"failed","direction":"to_server","payload_printable":">...........!.......................tfoerste....mUb....j.A#j..1^..!....select @@version_comment limit 1.....SELECT DATABASE().....test.....show databases.....show tables.....agent......create table foo (id BIGINT(10) UNSIGNED NOT NULL AUTO_INCREMENT PRIMARY KEY, animal VARCHAR(64) NOT NULL, name VARCHAR(64) NULL DEFAULT NULL) ENGINE = MYISAM7....insert into foo (animal, name) values (\"dog\", \"Goofy\"):....insert into foo (animal, name) values (\"cat\", \"Garfield\").....select * from foo'....delete from foo where name like '%oo%'.....delete from foo where id = 1.....select count(*) from foo.....select * from foo.....delete from foo.....drop table foo.....","stream":1,"packet":"RQAAKAAAAABABveDwKgA/sCoAP7bYgzqzNi94gAAAABQAAoAr48AAA==","packet_info":{"linktype":1}}

Assign a severity rating to this log.

High. The Suricata rule assigns a severity: 3. While the rule's signature_severity is "Informational," an explicit show databases attempt, especially in conjunction with the "SQL Database Version Discovery" alert and originating locally after a suspicious scan, is a strong indicator of unauthorized reconnaissance for potential data access or privilege escalation. This makes it a high-severity event within the context of the overall incident.

Mark this alert true positive, false positive, false negative, or true negative?

True Positive. The payload_printable clearly includes the show databases command, which directly matches the rule's signature. This command is a well-known method for enumerating databases during reconnaissance phases of an attack.

Explain what is happening in this log.

This log entry occurred simultaneously with the "ET HUNTING SQL Database Version Discovery" alert (Log Entry 2) and within the same network flow. It indicates that an entity on 192.168.0.254 is attempting to list all available databases on the local MySQL server. The payload_printable contains show databases, confirming the attempt to enumerate the database schema. The presence of additional commands in the payload like show tables, create table, insert into, delete from, and drop table further emphasizes that this is not a benign activity but rather an aggressive attempt to understand and potentially manipulate the database contents. This activity, correlated with the preceding scan, strongly suggests a local attacker performing reconnaissance and active exploitation of the MySQL server.

What remediation do you recommend for this log?

The remediation for this alert is identical to Log Entry 2, as they represent concurrent alerts within the same malicious flow and signify a severe security event.

Immediately isolate 192.168.0.254 from all networks.

Identify and terminate the malicious process that is executing these SQL commands on 192.168.0.254.

Perform a comprehensive forensic analysis of 192.168.0.254 to ascertain the root cause of the compromise, search for any backdoors or persistent malware, and determine if data was accessed, modified, or exfiltrated.

Review MySQL server logs thoroughly for all executed commands, the user accounts involved, and any associated timestamps.

Restore the database from the most recent known-good backup, ensuring the backup is free from compromise.

Revoke unnecessary privileges from MySQL users and enforce strong, unique passwords.
Implement host-based intrusion detection/prevention systems (HIDS/HIPS) and file integrity monitoring on 192.168.0.254 to detect and prevent such local malicious activity in the future.

Analyzing eve-2025-11-03-0044.json ....

The two log entries provided are highly correlated, indicating continuous activity from the same source to the same destination with identical alert signatures. They describe two closely timed events where 10.10.10.49 is querying print attributes from 10.10.10.251 using the Internet Printing Protocol (IPP).

1. Severity Rating
The severity rating for these logs is Informational (Severity 3).

The alert.severity field is 3.
The alert.metadata.signature_severity is explicitly marked as "Informational".
The signature itself starts with "ET INFO", indicating an informational event from the Emerging Threats rule set.
The category is "Misc activity".

2. True Positive, False Positive, False Negative, or True Negative?
These alerts are True Positives (in terms of detection accuracy), likely representing benign activity.

Suricata has accurately identified outbound Internet Printing Protocol (IPP) requests to "Get-Printer-Attributes" based on the rule's criteria (HTTP POST, Content-Type: application/ipp, User-Agent: CUPS/1.3.4).
The payload_printable data in both logs confirms that 10.10.10.49 is making legitimate-looking IPP requests to query printer attributes (e.g., supported copies, document formats, job acceptance, printer state, job status) from 10.10.10.251 on port 631.
The signature is designed to inform about this specific type of network traffic rather than to flag inherently malicious behavior.

3. Explanation of What is Happening

An internal host, 10.10.10.49, is initiating communication with another internal host, 10.10.10.251, on TCP port 631, which is the standard port for the Internet Printing Protocol (IPP). This activity is identified as "ET INFO Internet Printing Protocol (IPP) Get-Printer-Attributes Outbound Request".
Specifically:

Source: 10.10.10.49 (client)
Destination: 10.10.10.251 (server/printer)
Protocol: TCP, utilizing HTTP over IPP (application/ipp)
User-Agent: "CUPS/1.3.4", indicating the Common Unix Printing System is in use.
Action: In the first log, 10.10.10.49 is querying 10.10.10.251 for general printer attributes like supported copies, document formats, and the printer's state. In the second log, 10.10.10.49 is querying for job-specific attributes such as job-id, requesting-user-name, job-media-sheets-completed, and job-state, along with printer state messages.
Correlation: Both logs represent distinct but very closely timed requests (within 1.2 seconds) from the same source to the same destination, likely part of an ongoing printer discovery or monitoring process by the CUPS client.

This is a typical and expected behavior for a client attempting to interact with a network printer using IPP, especially within a CUPS environment.
4. Remediation Recommendations
Given that this is an informational alert for standard IPP communication, no immediate remediation for malicious activity is typically required.
However, the following actions can be considered:

Verification of Intent: Confirm that 10.10.10.49 is an authorized client and 10.10.10.251 is an authorized network printer or print server within the environment. If printing is not an expected function between these specific hosts, investigate the cause (e.g., misconfiguration, unauthorized device).
Network Segmentation: Ensure that printing services are appropriately segmented within the network. Printers and print servers should ideally be in a dedicated VLAN to control access and limit potential lateral movement in case of compromise.
Rule Tuning/Suppression: If these informational alerts are deemed legitimate and generate excessive noise without providing actionable security intelligence, consider suppressing Suricata sid:2056212 for traffic between these specific hosts or within the print server VLAN. This should only be done after verifying the legitimacy and expected nature of the traffic.
Logging and Monitoring: Continue to log and monitor IPP traffic, as while this specific activity is likely benign, IPP has been used in attack scenarios (e.g., PrintNightmare vulnerability). Anomalous IPP activity or a sudden increase in these types of informational alerts from unexpected sources could warrant further investigation.

Analyzing eve-2025-11-03-0022.json ....

Here is the analysis of the provided log entries:

Log Entry 1 Analysis
Log entry context: This log indicates a client initiating Spotify P2P traffic.

Severity Rating:

3 (Minor). The alert itself specifies severity: 3 and category: Not Suspicious Traffic. The metadata also lists signature_severity: Minor.

Mark this alert true positive, false positive, false negative, or true negative?

True Positive (Informational). The log accurately identifies traffic originating from 10.142.160.1 as the Spotify P2P client, matching the signature ET INFO Spotify P2P Client and payload content ("SpotUdp0"). While it's a true positive in terms of identification, it's categorized as "Not Suspicious Traffic," making it an informational alert rather than a malicious one, unless Spotify P2P usage is explicitly forbidden by policy.

Explain what is happening in this log:

An internal host with IP address 10.142.160.1 is initiating UDP communication on port 57621 to the broadcast address 10.142.160.255. Suricata detected this traffic as originating from the Spotify P2P client based on its signature, specifically identifying the unique "SpotUdp0" string in the payload. The alert is classified as "Not Suspicious Traffic," suggesting it's an informational alert indicating the presence and use of the Spotify P2P application on the network.

What remediation do you recommend for this log?

Policy Review: Determine if Spotify P2P client usage is allowed or restricted on the network. If it is permitted, document this type of traffic as normal.

Network Control: If Spotify P2P usage is not desired due to bandwidth concerns, security policy, or legal compliance, consider implementing firewall rules to block UDP traffic on port 57621 or deploy application-layer controls to specifically restrict Spotify P2P.
Asset Management: Verify that the host 10.142.160.1 is an authorized device to be running such applications and that its activity aligns with its intended purpose.

Log Entry 2 Analysis
Log entry context: This log indicates an HTTP DELETE attempt against an internal web server.

Severity Rating:

2 (High). The alert specifies severity: 2. The category is access to a potentially vulnerable web application, indicating a significant concern.

Mark this alert true positive, false positive, false negative, or true negative?

True Positive. The log accurately identifies an HTTP DELETE request. Whether this specific DELETE request is malicious or legitimate depends on the context of the application on 10.142.160.101. However, DELETE methods are often indicative of attempts to modify or remove data, and the rule's category "access to a potentially vulnerable web application" suggests it should be treated as a legitimate alert that requires investigation. Unless proven benign and authorized, it should be considered a true positive security event.

Explain what is happening in this log:

An internal client (source IP 10.142.160.1) is making an HTTP DELETE request to an internal web server (destination IP 10.142.160.101) on port 8091. The specific request targets /pools/default/buckets/default/docs/app. Suricata's rule GPL WEB_SERVER DELETE attempt triggered because an HTTP DELETE method was detected. This type of activity is often associated with attempts to exploit web server vulnerabilities or unauthorized content manipulation, especially if the server is not designed to handle such requests or lacks proper access controls.

What remediation do you recommend for this log?

Immediate Investigation: Determine the context and legitimacy of this DELETE request. Identify the user or process on 10.142.160.1 that initiated this action.
Server Configuration Review: Examine the web server (10.142.160.101) configuration to ascertain if HTTP DELETE methods are intentionally enabled and, if so, whether they are adequately protected by authentication and authorization mechanisms. If DELETE is not required for normal operation, disable it.
Access Control: Strengthen access controls on the web server to ensure that only authorized users or services can perform DELETE operations on specific resources.
Vulnerability Assessment: Conduct a vulnerability scan on 10.142.160.101 to identify any misconfigurations or vulnerabilities that could be exploited by HTTP DELETE requests.
Monitor for Further Activity: Keep a close watch on both 10.142.160.1 and 10.142.160.101 for any subsequent suspicious activity.

Log Entry 3 Analysis
Log entry context: This log indicates another HTTP DELETE attempt against the same internal web server.

Severity Rating:

2 (High). The alert specifies severity: 2, matching the previous DELETE attempt.

Mark this alert true positive, false positive, false negative, or true negative?

True Positive. Similar to Log Entry 2, this is a true positive. The repetition of DELETE attempts, even on different paths, strengthens the indication that this activity is either exploratory (e.g., by an attacker mapping resources) or unauthorized, requiring immediate investigation.

Explain what is happening in this log:

This log shows a second, closely timed HTTP DELETE request originating from the same internal client (10.142.160.1) to the same internal web server (10.142.160.101) on port 8091. This time, the request targets /pools/default/buckets/default/docs/apple. This is another instance of the GPL WEB_SERVER DELETE attempt signature being triggered. The repeated attempts suggest either an authorized user performing multiple deletion actions or an attacker probing the server for deletable resources.

What remediation do you recommend for this log?

The remediation steps are identical to Log Entry 2, but the occurrence of multiple DELETE attempts in close succession (15:25:42 and 15:25:44) elevates the urgency of the investigation.
Expedited Investigation: Prioritize the investigation into the source (10.142.160.1) and destination (10.142.160.101) to determine if these DELETE requests are part of legitimate administrative activity or malicious probing.
Blocking/Quarantining: If the activity is confirmed to be unauthorized, consider temporarily isolating 10.142.160.1 or blocking its access to 10.142.160.101 until the root cause is identified and mitigated.
System Hardening: If the web server is vulnerable, apply necessary patches or reconfigure it to disallow unauthorized DELETE requests.

Correlations Between Logs

Logs 2 and 3 are highly correlated:

They originate from the same source IP (10.142.160.1) and target the same destination IP (10.142.160.101) and port (8091).
Both logs share the same flow_id (1674331865711969) and community_id, indicating they are part of the same TCP flow/connection.
They were triggered by the exact same Suricata signature (GPL WEB_SERVER DELETE attempt, signature_id: 2101603) and occurred within seconds of each other (15:25:42 and 15:25:44).
The payloads show two distinct HTTP DELETE requests targeting different paths (/docs/app and /docs/apple), suggesting either an authorized user performing multiple deletions or an attacker actively probing the web application's DELETE functionality. This pattern warrants a more urgent investigation than a single occurrence.

Log 1 is not correlated with Logs 2 and 3:

Log 1 involves a different source IP, a broadcast destination, a different protocol (UDP vs. TCP), different ports, and a completely different alert signature ("ET INFO Spotify P2P Client" vs. "GPL WEB_SERVER DELETE attempt"). It represents an entirely separate and unrelated network event.

Analyzing eve-2025-11-02-2252.json ....

Here is the analysis of the provided Suricata log entry:

1. Severity Rating

Severity: 1 (High)
Explanation: The log explicitly states "severity":1 within the alert object. While the metadata indicates a signature_severity of "Informational", the numerical severity of 1 typically represents the highest level in Suricata's scale (1-3), aligning with the alert's category of "Potential Corporate Privacy Violation".

2. Mark this alert true positive, false positive, false negative, or true negative?

Classification: True Positive (with policy context)
Explanation: The alert is a True Positive in the sense that Suricata accurately detected traffic containing the "iTunes" string in the User-Agent header as per the ET INFO iTunes User Agent signature. The payload_printable clearly shows User-Agent: iTunes/10.6. Whether this specific activity constitutes an actual "violation" or requires intervention depends entirely on the organization's specific acceptable use policy regarding software and network traffic. If iTunes usage, particularly for internal communication on corporate networks, is prohibited or restricted, then this is a true positive policy violation. If it is permitted, then while the detection is accurate, the alert might be considered noise in terms of requiring security action.

3. Explain what is happening in this log
This log indicates that an internal host, 192.168.3.107, initiated an HTTP (specifically, an OPTIONS * RTSP/1.0 request) TCP connection from source port 51594 to another internal host, 192.168.3.123, on destination port 5000.
Suricata's "ET INFO iTunes User Agent" signature (SID 2002878) was triggered because the User-Agent field in the HTTP request contained "iTunes/10.6". This signature is categorized as a

"Potential Corporate Privacy Violation" and is designed to flag the presence of iTunes application traffic, which might be a concern depending on organizational policies. The traffic flow was allowed. Port 5000 is commonly associated with Apple's AirPlay or remote control services, further supporting the presence of Apple device communication.
4. What remediation do you recommend for this log?
The recommended remediation steps depend on the organization's specific policies regarding software usage and network traffic:

Policy Review and Enforcement:

Clarify Policy: Determine if iTunes usage, particularly internal network communication or streaming (like AirPlay), is permitted, restricted, or prohibited on the corporate network. The alert's category "Potential Corporate Privacy Violation" suggests a policy concern.
User Education: If iTunes usage is not permitted, educate users on acceptable software and network usage policies.

Contextual Investigation:

Identify Hosts: Investigate the devices 192.168.3.107 and 192.168.3.123. Understand their roles in the network and if iTunes or Apple device communication is expected or necessary for their functions. For example, if these are BYOD devices or devices in a specific lab network, the usage might be acceptable.
Traffic Purpose: Analyze the full context of the traffic flow to understand the exact purpose of this iTunes communication (e.g., AirPlay, file sharing, remote control).

Network Controls (if policy violation):

Firewall Rules: If iTunes traffic is to be blocked, implement firewall rules to prevent communication on specific ports (like 5000 for AirPlay) or based on application signatures, if available on your firewall.
Suricata Action: If the policy dictates blocking, consider changing the Suricata rule's action from alert to drop for this specific signature, if it is universally considered a violation.

Alert Tuning (if legitimate):

Suppress or Tune: If iTunes usage is legitimate and aligns with policy, consider suppressing this specific alert for internal traffic or tuning the rule to only alert on traffic crossing the network perimeter (i.e., to/from the internet), thereby reducing alert fatigue for benign internal activity.

Analyzing eve-2025-11-03-0112.json ....

Here is the analysis of the provided Suricata log entry:

Severity Rating:

1 (Informational). The alert.severity field is set to 1, and the alert.metadata.signature_severity is "Informational".

True positive, false positive, false negative, or true negative?

Based solely on the information provided in this log entry, it is not possible to definitively determine if this is a true positive, false positive, false negative, or true negative. Further investigation into the network environment, the role of the involved IPs, and organizational policies is required.

Explain what is happening in this log:

On 2013-05-01T12:24:11.972852+0000, a device with the IP address 192.168.0.253 (source port 50618) initiated a UDP connection to the IP address 192.168.0.10 on destination port 69.
Suricata identified this traffic as Trivial File Transfer Protocol (TFTP) and generated an alert with the signature "ET TFTP Outbound TFTP Read Request".
The alert is categorized as a "Potential Corporate Privacy Violation."
The payload_printable field indicates that 192.168.0.253 is attempting to read a file named "rfc1350.txt" using the TFTP protocol.
The Suricata engine allowed this connection ("action":"allowed").

What remediation do you recommend for this log?

Investigate Involved Hosts: Immediately investigate 192.168.0.253 to determine why it is initiating an outbound TFTP read request. Confirm if this is an authorized action for its role. Also, investigate 192.168.0.10 to ascertain if it is a legitimate TFTP server within the network or an unauthorized host.
Evaluate TFTP Necessity: TFTP is an insecure protocol often used for legitimate purposes like network device booting but is also commonly exploited for data exfiltration or unauthorized file transfers due to its lack of authentication and encryption. Determine if TFTP is a necessary protocol in the environment.
Block or Restrict TFTP: If TFTP is not required, disable the TFTP service on 192.168.0.10 and implement firewall rules to block UDP port 69 traffic, especially outbound, at network perimeters and internal segment boundaries.
Implement Secure Alternatives: If file transfer is necessary, enforce the use of secure protocols such as SFTP (SSH File Transfer Protocol) or SCP (Secure Copy Protocol) instead of TFTP.
Review Security Policies: Review and update corporate security policies regarding allowed file transfer protocols and data handling to prevent potential corporate privacy violations.

Analyzing eve-2025-11-03-0013.json ....

Here's an analysis of the provided Suricata log entry:

1. Severity Rating
Informational (Severity 3)
The log explicitly states "severity": 3 and metadata.signature_severity": ["Informational"]. This indicates a low-severity alert, typically used to log legitimate or routine network activity that might be worth monitoring but isn't immediately indicative of malicious activity.
2. Alert Classification
Requires further investigation, potentially a True Positive or Expected Behavior.
This alert signifies access to the "IPC"shareviaNETBIOSSMB.IPC" share via NETBIOS SMB. IPC"shareviaNETBIOSSMB.IPC is a legitimate administrative share on Windows systems used for interprocess communication, remote administration, and network browsing.

True Positive: If 192.168.29.1 is not an authorized administrative system or user, or if 192.168.29.133 should not be exposing SMB on port 139, then this access could indicate unauthorized reconnaissance, an attempt to exploit vulnerabilities, or lateral movement.

Expected Behavior: If 192.168.29.1 is a legitimate administrative workstation, a network scanner, or a backup system performing routine tasks against 192.168.29.133, then this alert might represent normal, expected network traffic.

Without additional context regarding the network topology, expected traffic patterns, and the roles of these specific IPs, a definitive classification is not possible. However, due to its "Informational" nature, it's more likely to be expected behavior if both systems are Windows machines in a typical network, but still warrants review.

3. Explanation of What is Happening

A TCP connection was initiated from the source IP 192.168.29.1 (source port 1107) to the destination IP 192.168.29.133 (destination port 139). Port 139 is associated with the NETBIOS Session Service, which is used for File and Printer Sharing (SMB) over NetBIOS over TCP/IP. Suricata detected this activity and triggered an "Informational" alert with the signature "GPL NETBIOS SMB IPCshareaccess".The‘appproto‘is‘smb‘,andthe‘flowbits‘‘smb.tree.connect.ipc‘confirmsthattheactivityrelatestoanSMBTreeConnectrequesttotheIPC share access". The `app_proto` is `smb`, and the `flowbits` `smb.tree.connect.ipc` confirms that the activity relates to an SMB Tree Connect request to the IPCshareaccess".The‘appproto‘is‘smb‘,andthe‘flowbits‘‘smb.tree.connect.ipc‘confirmsthattheactivityrelatestoanSMBTreeConnectrequesttotheIPC share. The payload_printable further corroborates this, showing a connection attempt to \\*SMBSERVER\IPC$.

The action was "allowed," meaning this connection was observed and permitted to proceed by Suricata. In essence, 192.168.29.1 is attempting to access the administrative IPC share on `192.168.29.133` using the SMB protocol over NetBIOS.### 4. Remediation Recommendations1. **Contextual Analysis:** * Determine the role of `192.168.29.1` and `192.168.29.133` within the network. * Verify if `192.168.29.1` is an authorized system or user account for accessing administrative shares on `192.168.29.133`. * If `192.168.29.133` is not a server or workstation that should be offering SMB services, investigate why it is doing so.2. **Disable Legacy SMB/NetBIOS (Port 139):** * Port 139 is associated with older implementations of SMB (SMBv1/NetBIOS over TCP/IP). Modern Windows systems primarily use port 445 for SMB. If not explicitly required for legacy systems, disable NetBIOS over TCP/IP on `192.168.29.133` to prevent exposure on port 139.3. **Network Segmentation and Access Control:** * Implement network segmentation to restrict SMB/IPC access only to authorized administrative subnets or systems.

    *   Use firewall rules to block inbound connections to ports 139 and 445 on systems that do not require SMB services, especially from EXTERNAL_NET.

Least Privilege Principle:

Ensure that any accounts or services accessing the IPCshareoperatewiththeabsoluteminimumnecessaryprivileges.5.**EndpointSecurityMonitoring:* **Increasemonitoringon‘192.168.29.133‘foranysubsequentsuspiciousactivityfollowingthisIPC share operate with the absolute minimum necessary privileges.5. **Endpoint Security Monitoring:**   *   Increase monitoring on `192.168.29.133` for any subsequent suspicious activity following this IPCshareoperatewiththeabsoluteminimumnecessaryprivileges.5.**EndpointSecurityMonitoring:* **Increasemonitoringon‘192.168.29.133‘foranysubsequentsuspiciousactivityfollowingthisIPC connection, such as unusual process creation, privilege escalation attempts, or data exfiltration, especially if the access was unauthorized.

Vulnerability Management:

Regularly patch and update 192.168.29.133 to mitigate known SMB vulnerabilities.
Perform vulnerability scans on 192.168.29.133 to identify any open shares or misconfigurations.

Suricata Rule Tuning (if deemed False Positive):

If this activity is confirmed as legitimate and expected behavior, and if the alert volume becomes excessive, consider suppressing or adjusting the Suricata rule for sid:2100537 for 192.168.29.1 to 192.168.29.133 connections to reduce noise. However, it's generally good practice to log such activity for auditing purposes.

Analyzing eve.json ....

Here is a structured analysis of the provided Suricata logs:

Event 1: ET DYN_DNS External IP Lookup

Severity Rating: Informational (Severity 2, signature_severity Informational)
True/False Positive/Negative: True Positive.
Explanation: The internal host 192.168.1.101 initiated a DNS query for checkip.dyndns.org to the external DNS server 65.32.5.111 on UDP port 53. This domain is commonly used by Dynamic DNS clients to determine their external IP address. While not inherently malicious, it can be indicative of non-standard software running on a host or reconnaissance activity.

Remediation:
Investigate Host 192.168.1.101: Determine why this host is performing an external IP lookup. Check for installed Dynamic DNS clients or unusual applications.
Policy Review: Assess if Dynamic DNS usage is permitted within the network. If not, enforce a policy to prevent its use.
Network Segmentation: Restrict external DNS lookups to authorized servers only.

Event 2: ET MALWARE Tibs/Harnig Downloader Activity (Multiple HTTP GET/Response flows)

Correlated Logs: Logs 2-4, 9-10 (Flow ID: 481342585854820, Community ID: 1:Ft80dpGFXumwOYf1j9RoSSms/nE=)
Correlated Logs: Logs 5-7, 8-9 (Flow ID: 481217962379606, Community ID: 1:uwBhqugg/eCYPXa3nGBcQpan2W4=)
Correlated Logs: Logs 11-13 (Flow ID: 305066164919106, Community ID: 1:wkLYTVOpikuiqt+Owxkbx7gM21A=)
Correlated Logs: Logs 14-17 (Flow ID: 530544451590907, Community ID: 1:g9fY7CwDf1eRIm+6TK2GiWWQlFs=) - This flow specifically mentions "Win32/Harnig.gen-P Reporting"
Correlated Logs: Logs 18-19 (Flow ID: 295383930134986, Community ID: 1:4D5LgKfmA0PW7MK5fxmR+yn9jUE=)

Severity Rating: High (Highest severity in these correlated events is 1 - Major)
True/False Positive/Negative: True Positive.
Explanation: Multiple internal hosts on the 192.168.3.0/24 subnet (specifically 192.168.3.35) are attempting to download or report to a known malware domain acxerox.com (IP 195.2.253.92) over HTTP (port 80).
The src_ip 192.168.3.35 makes multiple HTTP GET requests to PHP files (e.g., /tdfpmmn/hohhveswgc.php, /tdfpmmn/hnkppz.php, /tdfpmmn/wtqanbo.php, /tdfpmmn/bhanx.php, /tbuhrblyis/flvfbp.php) on acxerox.com.
These requests use a suspicious User-Agent (Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)ver49) and are detected as "Possible Trojan Downloader" and "Tibs/Harnig Downloader Activity".
Crucially, at least two of these requests (Flow IDs 481342585854820 and 481217962379606) result in the server 195.2.253.92 sending back an executable file (identified by "MZ" and "PE"

headers in the payload) while claiming the content type is text/html. This is a classic method for disguising malware downloads.

One flow (ID 530544451590907) is specifically tagged as "TrojanDownloader Win32/Harnig.gen-P Reporting", indicating the malware is communicating back to its command and control (C2) server.

The overall pattern strongly indicates that a system on 192.168.3.35 is infected with or attempting to download the Tibs/Harnig malware.

Remediation:

Isolate 192.168.3.35: Immediately disconnect 192.168.3.35 from the network to prevent further infection or lateral movement.

Malware Analysis & Eradication: Perform a full forensic analysis on 192.168.3.35 to confirm the malware, determine its capabilities, and eradicate it. This likely requires a full system re-image.

Block External IPs/Domains: Block access to 195.2.253.92 (acxerox.com) at the perimeter firewall/proxy.

Endpoint Security Review: Ensure all endpoints have up-to-date antivirus/EDR solutions and conduct a full scan of the 192.168.3.0/24 subnet.

User Training: Reinforce security awareness training on avoiding suspicious links and downloads.

Event 3: ET INFO Observed UA-CPU Header

Severity Rating: Informational (Severity 3, signature_severity Informational)

True/False Positive/Negative: True Positive (potential reconnaissance).

Explanation: The internal host 192.168.3.35 made an HTTP POST request to go-thailand-now.com (IP 96.0.203.90) on port 80. The request included a UA-CPU: x86 header. This header can be used for reconnaissance to fingerprint the architecture of the client system. It's often associated with older browser versions or specific applications, but its presence might also be indicative of enumeration attempts or unusual client behavior.

Remediation:

Investigate Host 192.168.3.35: Correlate this activity with other events from this host. Given the Zbot/Nemucod activity (Event 9), this could be a pre-infection reconnaissance step or a side effect of malware attempting to gather system information.

Policy Enforcement: Review HTTP traffic policies. If UA-CPU headers are not expected from legitimate applications, consider blocking them or raising a higher alert if seen in conjunction with other suspicious activity.

Reputation Check: Check the reputation of go-thailand-now.com (96.0.203.90) for any known malicious associations.

Event 4: GPL NETBIOS SMB-DS IPC$ unicode share access (Internal Reconnaissance / Lateral Movement)

Correlated Logs: Logs 21-24, 30-31, 40-41, 45-48, 50-51, 55-61, 64-65 (Multiple flows accessing 192.168.10.101 on port 445)
Correlated Logs: Logs 42-44, 49, 62, 66 (Multiple flows accessing 192.168.10.102 on port 139)

Severity Rating: Medium (Severity 3, signature_severity Informational, but context makes it higher)
True/False Positive/Negative: True Positive.
Explanation: Multiple internal hosts on the 192.168.10.0/24 network are attempting to access the IPC$ share on 192.168.10.101 and 192.168.10.102 via SMB (ports 445 and 139).
IPC$ is a null session share used for interprocess communication and is often targeted during internal reconnaissance and lateral movement phases of an attack.
The source IPs include 192.168.10.127, 192.168.10.128, 192.168.10.129, 192.168.10.125, 192.168.10.126, and 192.168.10.123.
The payload confirms attempts to access \\SKYNET.EXAMPLE.COM\IPC$ and \\192.168.10.102\IPC$.
The sheer volume of these alerts from different sources to different internal destinations suggests widespread internal scanning or an attempt by malware to spread.

Remediation:
Investigate Source Hosts: Examine 192.168.10.127, .128, .129, .125, .126, .123, .120, .124 for signs of compromise, such as unusual processes, elevated privileges, or other malware indicators.
Review SMB Configurations:
Restrict IPC$ access to only necessary administrative accounts and services.
Ensure SMB signing is enforced.
Disable SMBv1 if not required.

Implement Principle of Least Privilege: Ensure users and systems only have access to resources strictly necessary for their function.

Network Segmentation: Isolate the affected subnet or critical servers to prevent further spread.
Endpoint Protection: Verify that all endpoints have robust and updated endpoint detection and response (EDR) or antivirus solutions.

Event 5: ET SCAN UPnP SUBSCRIBE Inbound - Possible CallStranger Scan (CVE-2020-12695)

Correlated Logs: Logs 26-29, 32-39, 54, 55, 63 (Multiple flows targeting 192.168.10.100 on port 2869)
Log 26 (Flow ID: 1401764261451487, Community ID: 1:FBE91p0WI+uaQT4Khcg55KayZfo=)
Log 27 (Flow ID: 1406694338058063, Community ID: 1:CLNClc/4PZ8wTZBhAnx9EOHe6bw=)
Log 28 (Flow ID: 1163776129073327, Community ID: 1:iLbvSaKYHiW3TzEYLDq35TO0Dd0=)
Log 29 (Flow ID: 1164033897785577, Community ID: 1:/I9R4vb94Abhfke8ERJZmAjAosI=)
Log 32 (Flow ID: 1167966912149491, Community ID: 1:foX+Fn45m7WDcV5KWk7uzAQK928=)
Log 33 (Flow ID: 1174286489664693, Community ID: 1:zabl8175AF8oYagJS1l0EkEKtkM=)
Log 34 (Flow ID: 1211712193001300, Community ID: 1:4BEsXS2BiOAwMQpAkPAYddPiDng=)
Log 35 (Flow ID: 1220810896298958, Community ID: 1:XF7U3hmMjHI6XpbnNEO/WsTy4N4=)
Log 36 (Flow ID: 1280148338896096, Community ID: 1:E7EAUYFIOceFnchD668uCmCdJlg=)
Log 37 (Flow ID: 1321613593265656, Community ID: 1:F+C0NSFZA/mlELZcj3z3K7A7kes=)
Log 38 (Flow ID: 1397017323705798, Community ID: 1:IQSpgiPBviGznb0buyHTQR3Vpwo=)
Log 39 (Flow ID: 1147423958119385, Community ID: 1:LDvEGXBtDKbGsSI3yLwICK+ECzg=)
Log 54 (Flow ID: 68251242533865, Community ID: 1:S4/v+ODKC95ac7s8VUAj6p8jx1s=)
Log 55 (Flow ID: 74552118209180, Community ID: 1:M/QR8Al5kKZgV2W9JJ1pNt1/G+U=)
Log 63 (Flow ID: 1510624556734864, Community ID: 1:Rx9k0vf8G3j4v6iRbPWfhcrY6G8=)
Log 64 (Flow ID: 1526670520544754, Community ID: 1:aaTmOgiL9VMBGhJB1uCcj8cjpxY=)

Severity Rating: Medium (Severity 2, signature_severity Informational)

True/False Positive/Negative: True Positive.
Explanation: Multiple internal hosts on the 192.168.10.0/24 subnet (192.168.10.125, 192.168.10.124, 192.168.10.127, 192.168.10.128) are sending UPnP SUBSCRIBE requests to 192.168.10.100 on port 2869. These requests contain Callback: headers pointing back to the initiating IPs, which is characteristic of attempts to exploit the CallStranger vulnerability (CVE-2020-12695). This indicates internal reconnaissance or an attempt to use 192.168.10.100 as a relay for further attacks.
Remediation:
Investigate Source Hosts: Examine 192.168.10.125, .124, .127, .128 for compromise, as they are initiating the scan.
Patch 192.168.10.100: Ensure 192.168.10.100 is patched against CVE-2020-12695.
Disable UPnP: If UPnP is not required, disable it on 192.168.10.100 and other internal devices to reduce the attack surface.
Network Segmentation: Restrict UPnP traffic to only authorized segments or devices, and block inbound UPnP SUBSCRIBE requests from untrusted sources.

Event 6: ET P2P BitTorrent Activity

Correlated Logs: Logs 25, 32-48, 51, 90, 93 (All from 192.168.10.128)

Severity Rating: Medium (Highest severity is 1 - Informational, but policy violation makes it Medium)
True/False Positive/Negative: True Positive.
Explanation: The internal host 192.168.10.128 is actively engaged in BitTorrent peer-to-peer (P2P) file sharing activities.
It initiated a uTorrent client request to update.dna.bittorrent.com (64.127.109.133) (Log 25).
It made DHT ping requests to 72.20.34.145 (Log 26).
It attempted to download a torrent file (debian-500-i386-CD-1.iso.torrent) from cdimage.debian.org (130.239.18.173) (Logs 31-32), followed by announce requests to bttracker.debian.org (130.239.18.173) on port 6969 (Logs 33-34).
It's synchronizing with multiple BitTorrent peers on various external IPs and ports (77.204.217.77:5869, 219.90.186.1:44398, 72.83.129.122:34737, 70.38.54.39:28364, 140.211.166.44:8081, 200.223.236.53:51275, 96.36.117.14:27830, 83.191.116.166:6890) (Logs 35-40, 42-45, 48, 90, 93).
It's also performing BitTorrent transfers with peers (77.243.184.65:6881, 193.47.150.10:6882) (Logs 41, 46-47).

The "flow timeout" alerts (Logs 90, 93) simply indicate the end of some of these BitTorrent peer sync/transfer flows.
While some torrent activity might be legitimate (like downloading Linux ISOs as seen here), unauthorized P2P traffic often carries legal, security (malware), and bandwidth implications for organizations.

Remediation:
Policy Enforcement: Review and enforce the organizational policy regarding P2P file sharing. If not allowed, investigate the user of 192.168.10.128.
Bandwidth Management: If P2P traffic is a bandwidth concern, implement QoS or traffic shaping to limit its impact.
Block P2P Traffic: Configure perimeter firewalls to block common BitTorrent ports and protocols if P2P is prohibited. Consider deep packet inspection to identify and block P2P disguised as other protocols.
Security Assessment: P2P networks are often vectors for malware. Perform a security assessment on 192.168.10.128 for any additional compromises.

Event 7: FTP .exe File Request and PE EXE Download

Correlated Logs: Log 52 (request), Log 53 (download response, different flow_id but same src/dest and near-simultaneous)

Severity Rating: High (Severity 3 for "ET INFO .exe File requested over FTP", but the actual download of a PE executable over raw TCP is critical).
True/False Positive/Negative: True Positive.
Explanation: The internal host 192.168.10.128 requested to download an executable file named mirc635.exe via FTP from 130.89.149.129 on port 21 (Log 52). Immediately after, there's a log indicating a PE (Portable Executable) file download from 130.89.149.129 to 192.168.10.128 over a high ephemeral TCP port (1638). This strongly suggests the requested executable file was delivered and is now residing on the internal host. Downloading executables over unencrypted FTP is a significant security risk and a common malware delivery vector.
Remediation:
Isolate 192.168.10.128: Immediately disconnect 192.168.10.128 from the network.
Malware Analysis & Eradication: Conduct a full forensic investigation on 192.168.10.128 to determine if mirc635.exe is malicious, what it does, and how to eradicate it.

Block External IPs/Domains: Block 130.89.149.129 at the perimeter.
FTP Policy Review: Enforce strict policies against downloading executables over FTP. Consider blocking FTP outbound or requiring SFTP/FTPS for legitimate transfers.
User Education: Remind users about the dangers of downloading software from untrusted sources.

Event 8: GPL SNMP public access udp

Correlated Logs: Logs 49, 50, 52-56 (Flow ID: 199515906894090, Community ID: 1:T+HR2e17IlUBn2D69p7hUpVpR7M=)

Severity Rating: Medium (Severity 2, signature_severity Informational)
True/False Positive/Negative: True Positive.
Explanation: The internal host 192.168.10.124 is sending SNMP requests to the internal host 10.40.0.103 on UDP port 161 using the default "public" community string. This indicates an attempted information leak or reconnaissance activity, as the "public" community string is a well-known default that, if not changed, allows unauthorized access to device information.
Remediation:
Investigate Host 192.168.10.124: Determine why this host is attempting SNMP public access. This could be legitimate network management gone awry or another sign of compromise.
Harden SNMP on 10.40.0.103:
Change the default "public" community string to a strong, unique value.
Restrict SNMP access to authorized management stations only.
Consider upgrading to SNMPv3 for encryption and stronger authentication.

Network Monitoring: Continuously monitor for SNMP traffic, especially from unauthorized sources or using default community strings.

Event 9: ET MALWARE Zbot/Nemucod Activity (Multiple Malware C2 and Download flows)

Correlated Logs:

Log 67 (Flow ID: 570940483672378, Community ID: 1:vwc0PeVb/6U7zwlDUjPeLVh735Y=) from 192.168.3.35

Logs 68-69 (Flow ID: 571534755435097, 571570802661464, Community ID: 1:dKt6u6TboGRndwDLOc6De5dosSk= and 1:+HYQ85hZjwxyr5RDpX2YVtZX0xM=) from 192.168.3.35

Logs 70, 91-92 (Flow ID: 573331368821902, Community ID: 1:Gvl+u10F5yAYdeDl0qkTITyEcOs=) from 192.168.3.35

Logs 71-72, 74 (Flow ID: 999435280049551, 999473087043808, 1001587535219783, Community IDs: 1:9EVHSgrQ4iWfzfiAoSrJgrJX+kE= and 1:IjG25LlW8rSExpR+KvbHJzmHRkU= and 1:lOnLDTJapdQ50BHVZ/vOBy1nODk=) from 192.168.3.25

Log 73 (Flow ID: 1000416191746471, Community ID: 1:SiaqMLAd+aV4HE8ja2BOrmr+p38=) to 192.168.3.25

Logs 75-76 (Flow ID: 1067078209022816, Community ID: 1:NeV3XZmJ3MAZ/fGhZpIhR6Y8pf4=) from 192.168.3.65

Logs 77-78 (Flow ID: 957286489509897, Community ID: 1:6RmOegRK+BqWakqwKUOxon2LXS8=) from 192.168.3.65

Logs 79-83 (Flow ID: 957259452902610, Community ID: 1:rb4USHg48EB2+ogYLkfG7+sGdpM=) from/to 192.168.3.65

Logs 84-88 (Flow ID: 969484395522672, Community ID: 1:uTHPHEyy+iPSz7YuF3uDCNI7Igs=) from/to 192.168.3.65

Log 89 (Flow ID: 894493780268853, Community ID: 1:EvNwLrZrrclYwlS4c67yNLgcmmU=) from 192.168.3.65

Severity Rating: Critical (Highest severity is 1 - Major, indicating trojan/C2 activity, multiple executable downloads, and anti-debugging techniques.)

True/False Positive/Negative: True Positive.

Explanation: Multiple internal hosts (192.168.3.35, 192.168.3.25, 192.168.3.65) are exhibiting extensive malware activity consistent with Zbot and Nemucod trojan downloaders. 192.168.3.35 is making HTTP GET requests for .bin files (/cfg3.bin) from kloretukap.net (188.124.5.107) and HTTP POST requests to .php files (/back11/stat1.php) on homesitetoo.com (188.124.5.100), which are recognized as Zbot C2 activity. It's also requesting .exe payloads (e.g., /40.exe) from solaruploader.com (188.124.9.56), identified as Nemucod activity. The 40.exe file is successfully downloaded and confirmed as a Windows executable and a Nemucod payload.

192.168.3.25 is making HTTP POST requests to .php files (/index1.php) on pipiskin.hk (89.187.51.0), identified as Zbot C2 activity. An executable file (load.exe) is subsequently downloaded to 192.168.3.25 from 89.187.51.0.

192.168.3.65 is making HTTP GET requests for .bin files (/kartos/kartos.bin) and HTTP POST requests to .php files (/kartos/youyou.php) on ishi-bati.com (188.72.243.72), identified as Zbot C2 activity. It then requests krt.exe and ser.exe from ishi-bati.com and www.hostme.name (also 188.72.243.72). Both krt.exe and ser.exe are confirmed as Windows executables, with krt.exe specifically containing anti-debugging techniques (IsDebuggerPresent) and being a packed executable, which are strong indicators of malicious intent.

The consistent pattern across multiple internal hosts (C2 communication -> executable download, often with obfuscation or anti-analysis features) indicates a widespread infection.

Remediation:

Immediate Isolation: Isolate all affected hosts (192.168.3.35, 192.168.3.25, 192.168.3.65) from the network immediately.

Threat Hunting & Forensics:

Conduct deep forensic analysis on all infected machines to understand the extent of the compromise, data exfiltration, and any other malicious activities.

Identify the initial infection vector (e.g., phishing, drive-by download, vulnerable service).

Look for persistence mechanisms and additional payloads.

Eradication: Re-image or restore affected systems from known good backups. Standard malware removal might not be sufficient for sophisticated threats.

Block C2 Infrastructure: Block all identified malicious domains (kloretukap.net, homesitetoo.com, solaruploader.com, pipiskin.hk, ishi-bati.com, www.hostme.name) and IP addresses (188.124.5.107, 188.124.5.100, 188.124.9.56, 89.187.51.0, 188.72.243.72) at the perimeter firewall and proxy servers.

Endpoint Security Enhancement: Review and enhance endpoint detection capabilities, ensuring behavior-based detection and sandboxing are active.

Email & Web Filtering: Improve email and web filtering to prevent similar malware delivery.

User Awareness: Conduct urgent security awareness training on identifying and reporting suspicious emails or websites.

Network-wide Scan: Perform a network-wide scan for Zbot/Nemucod indicators of compromise (IOCs) to identify any other potentially infected systems.

Summary of Correlated Activity:
The logs show a highly active network environment with several critical security incidents occurring concurrently:

Widespread Internal Reconnaissance/Lateral Movement: Multiple internal hosts are scanning other internal hosts using SMB IPC$ access and UPnP SUBSCRIBE requests. This could be legitimate system administration, but given the other malware alerts, it's highly suspicious and indicative of an attacker attempting to map the internal network or spread.

Active Malware Infections: At least three internal hosts (192.168.3.35, 192.168.3.25, 192.168.3.65) are heavily compromised with Zbot/Nemucod malware, engaging in C2 communication and downloading malicious executables. This is the most critical finding.

Unauthorized P2P Activity: An internal host (192.168.10.128) is actively using BitTorrent, downloading torrent files, and communicating with many external peers. While not directly malware, this is a policy violation and a common vector for malware.

Insecure File Transfer of Executable: The same P2P-active host (192.168.10.128) is also downloading an executable over unencrypted FTP, a clear security risk.

SNMP Reconnaissance: An internal host (192.168.10.124) is attempting to access another internal host (10.40.0.103) via SNMP with a default community string, indicating potential vulnerability exploitation or reconnaissance.

DNS Reconnaissance: An internal host (192.168.1.101) is performing external IP lookups, potentially identifying systems running dynamic DNS.

These events paint a picture of a network under significant attack or already extensively compromised, with several internal systems actively engaged in malicious activities. The immediate priority should be isolating infected hosts and thoroughly investigating the extent of the breach.

```
'\n    display(to_markdown("## Severity"))\n
display(to_markdown(analysis_data[\'severity\']))\n\n    display(to_markdown("## Type"))\n
display(to_markdown(analysis_data[\'alert_type\']))\n\n    display(to_markdown("## Summary
of events"))\n    display(to_markdown(analysis_data[\'summary_of_events\']))\n\n
display(to_markdown("## Recommendations:"))\n
display(to_markdown(analysis_data[\'recommendations\']))'
```