Critical Log Review Checklist for Security Incidents

General Approach

1. Identify which log sources and automated tools you can use during the analysis.
2. Copy log records to a single location where you will be able to review them.
3. Minimize "noise" by removing routine, repetitive log entries from view after confirming that they are benign.
4. Determine whether you can rely on logs' time stamps; consider time zone differences.
5. Focus on recent changes, failures, errors, status changes, access and administration events, and other events unusual for your environment.
6. Go backwards in time from now to reconstruct actions after and before the incident.
7. Correlate activities across different logs to get a comprehensive picture.
8. Develop theories about what occurred; explore logs to confirm or disprove them.

Potential Security Log Sources

- Server and workstation operating system logs
- Application logs (e.g., web server, database server)
- Security tool logs (e.g., anti-virus, change detection, intrusion detection/prevention system)
- Outbound proxy logs and end-user application logs
- Remember to consider other, non-log sources for security events.

Typical Log Locations

- Linux OS and core applications: /var/log
- Windows OS and core applications: Windows Event Log (Security, System, Application)
- Network devices: usually logged via Syslog; some use proprietary locations and formats

What to Look for on **Linux**

Successful user login	"Accepted password","Accepted publickey", "session opened"
Failed user login	"authentication failure","failed password"
User log-off	"session closed"
User account change or deletion	"password changed","new user", "delete user"
Sudo actions	"sudo: … COMMAND=…""FAILED su"
Service failure	"failed" or "failure"

What to Look for on **Windows**

Event IDs are listed below for Windows 2000/XP. For Vista/7 security event ID, add 4096 to the event ID.

Most of the events below are in the Security log; many are only logged on the domain controller.

User logon/logoff events	Successful logon 528, 540; failed logon 529-537, 539; logoff 538, 551, etc
User account changes	Created 624; enabled 626; changed 642; disabled 629; deleted 630
Password changes	To self: 628; to others: 627
Service started or stopped	7035, 7036, etc.
Object access denied (if auditing enabled)	560, 567, etc

What to Look for on **Network Devices**

Look at both inbound and outbound activities.

Examples below show log excerpts from Cisco ASA logs; other devices have similar functionality.

Traffic allowed on firewall	“Built … connection”,“access-list … permitted”
Traffic blocked on firewall	“access-list … denied”,“deny inbound”, “Deny … by”
Bytes transferred (large files?)	“Teardown TCP connection … duration … bytes …”
Bandwidth and protocol usage	“limit … exceeded”,“CPU utilization”
Detected attack activity	“attack from”
User account changes	“user added”,“user deleted”, “User priv level changed”
Administrator access	“AAA user …”,“User … locked out”, “login failed”

What to Look for on **Web Servers**

Excessive access attempts to non-existent files	
Code (SQL, HTML) seen as part of the URL	
Access to extensions you have not implemented	
Web service stopped/started/failed messages	
Access to “risky” pages that accept user input	
Look at logs on all servers in the load balancer pool	
Error code 200 on files that are not yours	
Failed user authentication	Error code 401, 403
Invalid request	Error code 400
Internal server error	Error code 500

Source: Created by Dr. Anton Chuvakin and Lenny Zeltser.
https://zeltser.com/security-incident-log-review-checklist/