Important Logs and Files to Watch

/var/log/messages - /var/log/syslog (Debian)

- generic system activity, informational and non-critical system messages
- non-kernel boot errors, application-related service errors, system startup

/var/log/secure - /var/log/auth.log (Debian)

- authentication related events in Debian and Ubuntu server are logged here
- tracks sudo, SSH logins and other errors logged by system security services daemon
- investigate failed login attempts, brute-force attacks, etc
- successful logins and track activities of valid users

/var/log/wtmp - history of logins, use last command
/var/og/lastlog - recent user logins - use lastlog command
/var/log/faillog - failed login attempts
/var/log/btmp - failed login attempts, use lastb command
/var/log/setroubleshoot - track all the issues related to security context of files

/var/log/audit/audit.log

- audit daemon; use ausearch and aureport commands
- configuration changes, amount of failed system calls (syscalls), etc

Summary Report
==========
Range of time in logs: 12/07/2013 03:30:01.190 – 04/18/2014 15:00:01.378
Selected time for report: 12/07/2013 03:30:01 – 04/18/2014 15:00:01.378
Number of changes in configuration: 425
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 5
Number of terminals: 10
Number of host names: 0
Number of executables: 32
Number of files: 223
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 4190
Number of anomaly events: 3
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 3
Number of process IDs: 31405
Number of events: 116468

/var/log/maillog - /var/log/mail.log
- mail server related logs; postfix, smtpd, MailScanner, SpamAssassain etc
- trace the origin of an incoming email

/var/log/httpd/error_log - /var/log/httpd/access_log
- Apache server logging information
- logs the IP address and user ID of all clients that make connection requests

/var/log/mysql.log [mysqld.log in Debian]
- debug, failure and success messages related to the mysqld and mysqld_safe daemon
- starting, running, or stopping; info o client connections

/var/log/boot.log
- system initialization script, /etc/init.d/bootmisc.sh, sends all bootup messages here
- booting related information and messages logged during system startup process
- improper shutdown, unplanned reboots or booting failures.

/var/log/dmesg
- Kernel ring buffer messages, hardware device and driver info

/var/log/kern.log
- information logged by the kernel; kernel related errors and warnings

/var/log/daemon.log
- diagnosing issues created by daemons.

/var/log/yum.log
- track the installation of system components and software packages

/tmp - check for temp files from exploits that might have not been deleted
/etc/passwd - /etc/shadow - any suspicious user accounts added?
/etc/services - any suspicious services added? (i.e., backdoor)
crontab - /etc/init.d - It's good to detect any persistence

File Integrity Monitoring - a shortlist

Linux Networks. The most important files to monitor (or exclude)
Linux. Files to INCLUDE in FIM:
Root folder:
– monitor the permissions
Monitor the permissions, the access/modification time and the content of all files (except logs and cache files) in the following folders:
– /bin
– /sbin
– /usr/sbin
– /usr/bin.

– /usr/local/bin
– /usr/local/sbin
– /opt/bin
– /opt/sbin
– /lib
– /usr/lib
– /usr/local/lib
– /lib64
– /usr/lib64
– /root, /etc
Some Linux attacks try to gain privileges by modifying the configuration of your grub file, therefore it must be properly monitored /boot/grub/grub.conf

Linux. Files to EXCLUDE from FIM:
– Exclude log files (e.g. /var/log) – see Linux update below.
– Exclude cache files

Windows Networks. The most important files to monitor (or exclude)
Windows. Files to INCLUDE in FIM:

The following files in C:\:
– autoexec.bat
– boot.ini
– config.sys
– io.sys
– msdos.sys
– ntbootdd.sys
– ntdetect.sys
– ntldr
The following folders (no files and subfolders):
– C:\Documents and Settings
– C:\Users
– C:\System Volume Information
The following folders (including files and subfolders) in C:\:
– ProgramFiles
– ProgramFiles(x86)
All files and folders under C:\WINDOWS, and in particular the following folders (no files and subfolders):
– assembly
– CSC
– DEBUG
– security
– system32\NtmsData
– Temp

Windows. Files to EXCLUDE from FIM:

Folders in “C:\WINDOWS” listed below, which basically contain log files (the reason is explained below), cache files and other unimportant files:
– NtServicePackUninstall
– NtUninstall
– assembly
– CSC
– DEBUG
– HELP
– I386
– LogFiles
– Minidump
– Prefetch
– Shelliconcache
– SoftwareDistribution
– system32\Catroot
– system32\LogFiles
– system32\NtmsData
– system32\winevt\Logs
– System32\wdi\LogFiles
– system32\wbem
– Temp
– winsxs
– rescache
– serviceprofiles\networkservice\appdata\local\temp

Linux tools to:
httpie (like curl and wget)
tc
ngrep
tcpflow
mitmproxy (to see traffic on hosted SSL sessions)
p0f - see OS's of connected hosts
openvpn and wiregaurd
nc = netcat
socat
lsof
fuser
nftables - newer version of iptables
mtr (like traceroute?)
ethtool
sysctl
openssl
stunnel
iptraf nethogs iftop ntop

ab nload and iperf
ipcalc
nsenter (namespace enter- containers)

Cyber Kill Chain (classic)
1. Reconnaissance
2. Weaponization (choosing the exploit)
3. Delivery (send the exploit)
4. Exploitation (use the exploit on vulnerability)
5. Installation (of persistence on systems)
6. Command and Control (phoning back to attacker for further instructions)
7. Actions on Objectives (infiltrating other systems, increasing attack footprint)

Diamond Model (nodes to identify)
1. Adversary
2. Capability (tools operating on the vulnerabilities (on 'capacities')
3. Victim
4. Infrastructure (type 1 is owned by attacker, type 2 is not- like a hop or 3rd party)

Metafeatures include:
- Phase
- Result
- Direction of event-item
- Methodology (of capability nodes)
- Resources (that attackers have)

Threat Hunting Cycle
1. Hypothesis
2. Investigate
3. Uncover
4. Inform

Six Stages of Incident Response
1. Prepare
2. Identify
3. Contain
4. Eradicate
5. Recover
6. Lessons Learned

Mitigation
- Threat intelligence
- Email security
- DNS security
- Client security
- Web security
- Identity-based firewall roles/policies

- Intrusion Prevention
- Network Monitoring

CVSS 3.1 Metrics

[Forum of Incident Response and Security Teams (FIRST)]

- https://www.first.org/cvss/v3.1/specification-document

Base Metric Group

Exploitability Metrics

Attack Vector (AV) - Network (N), Adjacent (A), Local (L), Physical (P)
Attack Complexity (AC) - Low (L), High (H)
Privileges Required (PR) - None (N), Low (L), High (H)
User Interaction (UI) - None (N), Required (R)
Scope (S) - Unchanged (U), Changed (C)

Impact Metrics

Confidentiality (C) - None (N), Low (L), High (H)
Integrity (I) - None (N), Low (L), High (H)
Availability (A) - None (N), Low (L), High (H)

Temporal Metric Group

Exploit Code Maturity/ Exploitability (E) - Not Defined (X), High (H), Functional (F), Proof-of-Concept (P), Unproven (U)

Remediation Level (RL) - Not Defined (X), Unavailable (U), Workaround (W), Temporary Fix (T), Official Fix (O)

Report Confidence (RC) - Not Defined (X), Confirmed (C), Reasonable (R), Unknown (U)

Environmental Metric Group

(these refer to the specific system or systems, to over-ride Base Metrics to consider more specific context)

Security (CIA) Requirements (CR, IR, AR) - Not Defined (X), High (H), Medium (M), Low (L)

Modified Base Metrics (use same values as matching base metric above does)

Modified Attack Vector (MAV)
Modified Attack Complexity (MAC)
Modified Privileges Required (MPR)
Modified User Interaction (MUI)
Modified Scope (MS)
Modified Confidentiality (MC)
Modified Integrity (MI)
Modified Availability (MA)

Qualitative Severity Rating Scale

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9

High 7.0-8.9
Critical 9.0-10.0

(Optional: only intended to help organizations properly assess/prioritize their vulnerability management)

A vector string takes the form of (e.g.) CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L
Calculators to automatically calculate numeric scores for the metric groups are available here:

- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- https://www.first.org/cvss/calculator/3.1

Make CIA aggregate scores, then determine the minimum required security controls
To get the aggregate scores,
- classify information types into levels of CIA based on the organization or industry
- incorporate stakeholder input into CIA determinations
- assess the aggregate score of CIA

For each in C,I, and A: Value of Info * Threat Value = Total Risk
Total sum risk for C + I + A = Aggregate CIA

CIA Attribute	Value of Info		Threat Value		Total Risk
Confidentiality	7	*	10	=	70
Integrity	3	*	5	=	15
Availability	8	*	5	=	40

= Aggregate CIA (sum total risks) score of 125

Another way of using the CIA aggregate: Collectively assess 3 servers.

Attribute:	C	I	A
Manufacturing		L	M	L
Research	H	L	M
Sales/ PR	M	H	H

In this method, the aggregate score is said to be high in all 3 attributes, which is the aggregate.

Exposure factor * Asset Value = SLE, ALE = SLE * ARO

Likelihood- Annualized Rate of Occurrence (ARO)
Single Loss Expectancy (SLE)
Laptop stolen = $1000
Add in purchasing cost of replacement process, hours lost
Annual Loss Expectancy ALE = ARO x SLE
Seven laptops a year x $1000 = $7000
Also non-monetary loss: quantitative vs qualitative
How many man hours were spent resolving the issue?
How much money was lost by diverting labor to doing forensics

CBA - cost benefit analysis - ROI and TCO

ROI return on investment = (gain from investment / money spend on investment) * 100

IPS example:

Cost = $1,000

Gain = $5,000 (benefits minus costs, "cost-based analysis" focus on profitability)

ROI = (5,000 / 1,000) * 100 = 500% (benefits minus costs, then divided by cost, *100 to convert to %)

ROI is achieved after the year containing the $ covering the original cost is over

TCO = Purchase + (Operating + Training + Maintenance costs - Salvage value)

Other acronyms you may see: Net Present Value (NPV), Internal Rate of Return (IRR), Equity Value Analysis (EVA)

ROI = [net benefit year1 / (1+discount rate) + net benefit year2 / (1+discount rate) + net benefit
year3/ (1+discount rate)] / initial cost

Review Existing Security

Consistent reviews ensure increasing ROI and overall security.

Conduct yearly (at minimum) reviews of all systems and policies.

Perform vulnerability assessments internally or by contract. Use penetration testing for a more intense approach.

Full internal audits review both the systems and the processes behind those systems.

General attributes of enterprise security solutions to evaluate:

Evaluating the effectiveness and ROI of a solution can be an involved, complex process.

Performance
Availability
Capability
Latency (delay)
Scalability
Usability
Maintainability
Recoverability

After-Action Report

What actions did you take?
Is this the optimal solution?
Are there more capable solutions?
How well did the security teams react?
How would you respond differently in the future?
Should the security policy change in light of your answers?

Guidelines for Analyzing Scenarios to Secure the Enterprise

Create a separate security baseline for each system.

Use relevant and effective metrics for measuring configurations in a baseline.

Routinely conduct benchmarks on systems to see if they align with the security baseline.

Prototype and test multiple solutions before implementing them.

Request that a vendor demonstrate a live environment test.

Determine the return on investment and total cost of ownership of each solution to ensure they meet cost-benefit requirements.

Collate information from various sources to see high-level trends in security.

Exercise critical thinking and skepticism before trusting unverified information.

Review the effectiveness of existing security controls.

Perform vulnerability assessments, penetration tests, and full internal audits.

Use judgment to solve difficult problems that do not have a best solution.

Reverse engineer systems to analyze their behavior, when possible.

Write an after-action report and detail any lessons learned from an incident.

Think of questions to ask that pertain to improving your security.

Analyze security solution attributes to ensure they meet business needs.

Automate best practice implementation through scripts.

Should the security policy change in light of your answers?

When you first perform a risk assessment, you need to know exactly what you are assessing. Organizational assets can include firewalls, servers, and other computers and devices. These need to be identified first before you can identify vulnerabilities and threats. Last on the list when assessing risk is to identify potential monetary impact, which can be done in a qualitative or quantitative manner.

Assessment Types - Quantitative View

Business Impact Analysis (BIA) - examine risk for every resource and every threat

Likelihood - how likely is the threat to occur?

What's the impact to the organization if a particular threat happens?

Quantify- assign a dollar value (SLE) - hard to do without a historical reference

In these cases do qualitative- take elements and represent graphically by green, red, yellow

When dealing with dollars, risk assessments should be based upon a quantitative measurement of risk, impact, and asset value.

"The main objective of risk management in an organization is to reduce risk to a level the organization will accept"

"An RPO (recovery point objective) defines acceptable data loss."

Risk Avoidance

Stop risky activity (block BitTorrent on corporate network)

Transfer risk - buy insurance - RISK TRANSFERENCE
Business decision to take the risk
Decrease risk level - mitigate with security solutions
Deterrence- warnings, dogs, security fences

SRTM Security Requirements Traceability Matrix - Clear CIA Attributes

Security Requirement	Source of Requirement	Verification Method
Full system recovery in 24 hours	Business continuity plan	Perform a full backup restore on bare hardware in under 24 hours, then test it.
High website availability	Network security policy	Solve with redundancy; Simulate a DoS condition without it taking web servers offline.
Confidential storage of customer info	Legal compliance policy	Perform penetration test on customer information databases with no significant findings.

Each needs a "who's responsibility?" column for traceability part - accountability

Risk Response Techniques: Transfer, Mitigate, Avoid, Accept

Risk Management Processes
Exemptions, Deterrence, inherent risk (port "x" must be open), residual risk (can't be patched, etc)

Business Documents that Support Security Initiatives
Statement of applicability (SOA) what controls are put in place and why we are doing it
Business impact analysis (BIA) works with the business continuity plan
Service-level agreement (SLA)
Memorandum of understanding (MOU) - he says this isn't legally binding.
Operating-level agreement (OLA) a subdoc of the MOU that specifies interdepartmental ties to responsibility
Non-disclosure agreement (NDA)
Business partnership agreement (BPA)
Interoperability agreement (IA) partnership (see section on mergers) part of the BPA (below)
Interconnection security agreement (ISA) - sort of the same for security of data and infrastructure

More Linux refresher stuff
hostname
hostnamectl set-hostname hostx.example.com
timedatectl set-time
mandb - run after installing new software to update man database
who command refers to /var/run/utemp
apropos the same as man -k

pidof and pgrep to list PID of a process
While pgrep merely prints a list of matching processes, pkill will send the specified

signal (or SIGTERM by default) to the processes. The common options and semantics between pgrep and pkill comes in handy when you want to be careful and first review the list matching processes with pgrep, then proceed to kill them with pkill. pgrep and pkill are provided by the the procps package, which also provides other /proc file system utilities, such as ps, top, free, uptime among others.

User crontab files are in /var/spool/cron

rpm2cpio dumps files out of an RPM package

RHEL GPG signature store is /etc/pki/rpm-gpg

gpk-prefs command to set up automatic SW updates

2 tools for especially for editing shadow password files- vipw and vigr
2 tools for checking shadow password file consistency pwck and grpck
2 tools to create and update shadow/gshadow files - pwconv grpconv
(shadow and gshadow)
shadow- is the name of the backup of the shadow file
su with the dash (su -) will process the user's startup files) whereas without a '-' it wont