

Incident Responder Toolkit Requirements

Hardware Requirements			
Sr. No.	Resource	Required	Remarks/Comments/ Specification
1	Latest processor	<input type="checkbox"/>	
2	Adequate RAM	<input type="checkbox"/>	
4	Large-capacity HDD drives	<input type="checkbox"/>	
5	SCSI card and controller	<input type="checkbox"/>	
6	SCSI connectors and HDMI cables	<input type="checkbox"/>	
7	Parallel-to-SCSI adapters and active terminators	<input type="checkbox"/>	
8	Motherboard which supports SCSI, USB/2, FireWire, slot for LAN/WAN card	<input type="checkbox"/>	
9	Latest laptop hard drive connectors	<input type="checkbox"/>	
10	Graphics cards	<input type="checkbox"/>	
11	AGP	<input type="checkbox"/>	
12	Monitor	<input type="checkbox"/>	
13	Keyboard	<input type="checkbox"/>	
14	Mouse	<input type="checkbox"/>	
15	USB	<input type="checkbox"/>	
16	Power-extension cords	<input type="checkbox"/>	
17	Uninterruptible power supply (UPS)	<input type="checkbox"/>	
18	Category (CAT) 5	<input type="checkbox"/>	
19	Network devices	<input type="checkbox"/>	
20	Permanent marker for labeling evidence	<input type="checkbox"/>	
21	Operating manuals for all your hardware	<input type="checkbox"/>	
22	Digital camera	<input type="checkbox"/>	

23	Scanner and printer	<input type="checkbox"/>	
24	External storage for evidence	<input type="checkbox"/>	

Software Requirements			
Sr. No.	Resource	Required	Remarks/Comments/Specification
1	Windows 10/11 operating systems	<input type="checkbox"/>	
2	Windows Server 2016/2019/2022 operating systems	<input type="checkbox"/>	
3	Linux operating systems	<input type="checkbox"/>	
4	Unix operating systems	<input type="checkbox"/>	
5	macOS operating systems	<input type="checkbox"/>	
6	Drivers for all the hardware	<input type="checkbox"/>	
7	Forensics software	<input type="checkbox"/>	
8	Imaging tools	<input type="checkbox"/>	
9	Programming language applications	<input type="checkbox"/>	
10	Graphics tools	<input type="checkbox"/>	
11	Specialized viewers	<input type="checkbox"/>	
12	Hashing tools	<input type="checkbox"/>	
13	File recovery programs	<input type="checkbox"/>	
14	Encryption decoding software	<input type="checkbox"/>	
15	Password cracking software	<input type="checkbox"/>	
16	Anti-virus software	<input type="checkbox"/>	
17	Vulnerability assessment tools	<input type="checkbox"/>	
18	Network scanning tools	<input type="checkbox"/>	
19	Network sniffing tools	<input type="checkbox"/>	
20	Protocol analyzers	<input type="checkbox"/>	
21	Reverse engineering tools	<input type="checkbox"/>	

22	Malware analysis tools	<input type="checkbox"/>	
23	Web application proxies	<input type="checkbox"/>	
24	Intelligence sharing tools	<input type="checkbox"/>	
25	Database requirement	<input type="checkbox"/>	
26	Miscellaneous software	<input type="checkbox"/>	
27	Spare servers	<input type="checkbox"/>	
28	Spare virtualized equipment		

Communication and Facilities Requirements

Sr. No.	Resource	Required	Remarks/Comments/ Specification
1	Contact information (Phone numbers, email addresses, and public encryption keys for the required software)	<input type="checkbox"/>	
2	On-call information	<input type="checkbox"/>	
3	Incident reporting mechanisms (Online forms, numbers, contact numbers, instant messaging service)	<input type="checkbox"/>	
4	Issue tracking system	<input type="checkbox"/>	
5	Smartphones	<input type="checkbox"/>	
6	Encryption software	<input type="checkbox"/>	
7	War room	<input type="checkbox"/>	
8	Secure storage facility	<input type="checkbox"/>	

Incident Analysis and Mitigation Resources Requirements

Sr. No.	Resource	Required	Remarks/Comments/ Specification
1	Port lists	<input type="checkbox"/>	
2	Incident documentation	<input type="checkbox"/>	

3	Network diagrams and lists of assets	<input type="checkbox"/>	
4	Current baselines	<input type="checkbox"/>	
5	Cryptographic hashes of critical files	<input type="checkbox"/>	
6	Incident mitigation tools	<input type="checkbox"/>	