1.

Record Nr.	UNISA996211389403316
Titolo	String Processing and Information Retrieval: A South American Symposium, Santa Cruz de la Sierra, Bolivia, September 9-11, 1998
Pubbl/distr/stampa	[Place of publication not identified], : IEEE Computer Society Press, 1998
Disciplina	005
Soggetti	Text processing (Computer science) - Congresses Information storage and retrieval systems - Congresses Engineering & Applied Sciences Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph

2.

Record Nr.	UNINA9910555168603321
Autore	Anson Steve
Titolo	Applied incident response / / Steve Anson
Pubbl/distr/stampa	Indianapolis, Indiana : , : Wiley, , [2020] ©2020
ISBN	1-119-56031-4 1-119-56030-6 1-119-56028-4
Edizione	[1st edition]
Descrizione fisica	1 online resource (464 pages)
Disciplina	658.4038
Soggetti	Information technology - Management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

Sommario/riassunto

Incident response is critical for the active defense of any network, and incident responders need up-to-date, immediately applicable techniques with which to engage the adversary. Applied Incident Response details effective ways to respond to advanced attacks against local and remote network resources, providing proven response techniques and a framework through which to apply them. As a starting point for new incident handlers, or as a technical reference for hardened IR veterans, this book details the latest techniques for responding to threats against your network, including: Preparing your environment for effective incident response Leveraging MITRE ATT&CK and threat intelligence for active network defense Local and remote triage of systems using PowerShell, WMIC, and open-source tools Acquiring RAM and disk images locally and remotely Analyzing RAM with Volatility and Rekall Deep-dive forensic analysis of system drives using open-source or commercial tools Leveraging Security Onion and Elastic Stack for network security monitoring Techniques for log analysis and aggregating high-value logs Static and dynamic analysis of malware with YARA rules, FLARE VM, and Cuckoo Sandbox Detecting and responding to lateral movement techniques, including pass-the-hash, pass-the-ticket, Kerberoasting, malicious use of PowerShell, and many more Effective threat hunting techniques Adversary emulation with Atomic Red Team Improving preventive and detective controls