1. Record Nr. UNINA9910830854003321

Autore	Lee Martin (Computer security expert)
Titolo	Cyber threat intelligence / / Martin Lee
Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, Inc., , [2023] ©2023
ISBN	9781119861751 1-119-86177-2 1-119-86175-6
Descrizione fisica	1 online resource (307 pages)
Disciplina	005.8/7
Soggetti	Cyber intelligence (Computer security) Cyberspace operations (Military science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Preface -- About the Author -- Abbreviations -- Endorsements for Martin Lee's Book -- Chapter 1 Introduction -- 1.1 Definitions -- 1.1.1 Intelligence -- 1.1.2 Cyber Threat -- 1.1.3 Cyber Threat Intelligence -- 1.2 History of Threat Intelligence -- 1.2.1 Antiquity -- 1.2.2 Ancient Rome -- 1.2.3 Medieval and Renaissance Age -- 1.2.4 Industrial Age -- 1.2.5 World War I -- 1.2.6 World War II -- 1.2.7 Post War Intelligence -- 1.2.8 Cyber Threat Intelligence -- 1.2.9 Emergence of Private Sector Intelligence Sharing -- 1.3 Utility of Threat Intelligence -- 1.3.1 Developing Cyber Threat Intelligence -- Summary -- References -- Chapter 2 Threat Environment -- 2.1 Threat -- 2.1.1 Threat Classification -- 2.2 Risk and Vulnerability -- 2.2.1 Human Vulnerabilities -- 2.2.1.1 Example - Business Email Compromise -- 2.2.2 Configuration Vulnerabilities -- 2.2.2.1 Example - Misconfiguration of Cloud Storage -- 2.2.3 Software Vulnerabilities -- 2.2.3.1 Example - Log4j Vulnerabilities -- 2.3 Threat Actors -- 2.3.1 Example - Operation Payback -- 2.3.2 Example - Stuxnet -- 2.3.3 Tracking Threat Actors -- 2.4 TTPs - Tactics, Techniques, and Procedures -- 2.5 Victimology -- 2.5.1 Diamond Model -- 2.6 Threat Landscape -- 2.6.1 Example - Ransomware -- 2.7 Attack Vectors, Vulnerabilities, and Exploits -- 2.7.1 Email Attack

Vectors -- 2.7.2 Web-Based Attacks -- 2.7.3 Network Service Attacks -- 2.7.4 Supply Chain Attacks -- 2.8 The Kill Chain -- 2.9 Untargeted versus Targeted Attacks -- 2.10 Persistence -- 2.11 Thinking Like a Threat Actor -- Summary -- References -- Chapter 3 Applying Intelligence -- 3.1 Planning Intelligence Gathering -- 3.1.1 The Intelligence Programme -- 3.1.2 Principles of Intelligence -- 3.1.3 Intelligence Metrics -- 3.2 The Intelligence Cycle -- 3.2.1 Planning, Requirements, and Direction.
3.2.2 Collection -- 3.2.3 Analysis and Processing -- 3.2.4 Production -- 3.2.5 Dissemination -- 3.2.6 Review -- 3.3 Situational Awareness -- 3.3.1 Example - 2013 Target Breach -- 3.4 Goal Oriented Security and Threat Modelling -- 3.5 Strategic, Operational, and Tactical Intelligence -- 3.5.1 Strategic Intelligence -- 3.5.1.1 Example - Lazarus Group -- 3.5.2 Operational Intelligence -- 3.5.2.1 Example - SamSam -- 3.5.3 Tactical Intelligence -- 3.5.3.1 Example - WannaCry -- 3.5.4 Sources of Intelligence Reports -- 3.5.4.1 Example - Shamoon -- 3.6 Incident Preparedness and Response -- 3.6.1 Preparation and Practice -- Summary -- References -- Chapter 4 Collecting Intelligence -- 4.1 Hierarchy of Evidence -- 4.1.1 Example - Smoking Tobacco Risk -- 4.2 Understanding Intelligence -- 4.2.1 Expressing Credibility -- 4.2.2 Expressing Confidence -- 4.2.3 Understanding Errors -- 4.2.3.1 Example - the WannaCry Email -- 4.2.3.2 Example - the Olympic Destroyer False Flags -- 4.3 Third Party Intelligence Reports -- 4.3.1 Tactical and Operational Reports -- 4.3.1.1 Example - Heartbleed -- 4.3.2 Strategic Threat Reports -- 4.4 Internal Incident Reports -- 4.5 Root Cause Analysis -- 4.6 Active Intelligence Gathering -- 4.6.1 Example - the Nightingale Floor -- 4.6.2 Example - the Macron Leaks -- Summary -- References -- Chapter 5 Generating Intelligence -- 5.1 The Intelligence Cycle in Practice -- 5.1.1 See it, Sense it, Share it, Use it -- 5.1.2 F3EAD Cycle -- 5.1.3 D3A Process -- 5.1.4 Applying the Intelligence Cycle -- 5.1.4.1 Planning and Requirements -- 5.1.4.2 Collection, Analysis, and Processing -- 5.1.4.3 Production and Dissemination -- 5.1.4.4 Feedback and Improvement -- 5.1.4.5 The Intelligence Cycle in Reverse -- 5.2 Sources of Data -- 5.3 Searching Data -- 5.4 Threat Hunting -- 5.4.1 Models of Threat Hunting -- 5.4.2 Analysing Data.
5.4.3 Entity Behaviour Analytics -- 5.5 Transforming Data into Intelligence -- 5.5.1 Structured Geospatial Analytical Method -- 5.5.2 Analysis of Competing Hypotheses -- 5.5.3 Poor Practices -- 5.6 Sharing Intelligence -- 5.6.1 Machine Readable Intelligence -- 5.7 Measuring the Effectiveness of Generated Intelligence -- Summary -- References -- Chapter 6 Attribution -- 6.1 Holding Perpetrators to Account -- 6.1.1 Punishment -- 6.1.2 Legal Frameworks -- 6.1.3 Cyber Crime Legislation -- 6.1.4 International Law -- 6.1.5 Crime and Punishment -- 6.2 Standards of Proof -- 6.2.1 Forensic Evidence -- 6.3 Mechanisms of Attribution -- 6.3.1 Attack Attributes -- 6.3.1.1 Attacker TTPs -- 6.3.1.2 Example - HAFNIUM -- 6.3.1.3 Attacker Infrastructure -- 6.3.1.4 Victimology -- 6.3.1.5 Malicious Code -- 6.3.2 Asserting Attribution -- 6.4 Anti-Attribution Techniques -- 6.4.1 Infrastructure -- 6.4.2 Malicious Tools -- 6.4.3 False Attribution -- 6.4.4 Chains of Attribution -- 6.5 Third Party Attribution -- 6.6 Using Attribution -- Summary -- References -- Chapter 7 Professionalism -- 7.1 Notions of Professionalism -- 7.1.1 Professional Ethics -- 7.2 Developing a New Profession -- 7.2.1 Professional Education -- 7.2.2 Professional Behaviour and Ethics -- 7.2.2.1 Professionalism in Medicine -- 7.2.2.2 Professionalism in Accountancy -- 7.2.2.3 Professionalism in Engineering -- 7.2.3 Certifications and Codes of Ethics -- 7.3 Behaving Ethically -- 7.3.1 The Five Philosophical