Security Operations Center: il cuore della protezione dell'Informazione

Author : Andrea Boggio

Date : 26 giugno 2018

Non c'è sicurezza in questo mondo, ci sono solo opportunità

Douglas MacArthur

Cos'è un SOC ?

Il Security Operations Center (SOC) è un'entità organizzativa che si caratterizza, principalmente, per le capacità difensive in contrasto ad attività non autorizzate condotte contro gli *asset* oggetto di protezione. Tra le prerogative del SOC, usando come riferimento il *Cyber Security Framework* del NIST[1], rientrano capacità di identificazione (***Identify***), protezione (***Protect***), rilevazione (***Detect***), risposta (***Respond***) e recupero (***Recover***). Un SOC è composto da un gruppo di professionisti - analisti e architetti di sicurezza - organizzati per rilevare, analizzare, rispondere, fare rapporti e prevenire incidenti di cyber-security ed erogare servizi verso la propria ***constituency***, che consiste in un insieme di utenti, siti, *asset* IT, reti e organizzazioni. I *Managed Security Services Provider* (MSSP), operati da player di mercato, offrono servizi di sicurezza gestita tipici di un SOC ai propri clienti secondo una logica di esternalizzazione.

Uno dei principali **obiettivi di alto livello** del SOC è promuovere la ***Situational Awareness***[2] dell'organizzazione consolidando flussi di dati tramite aggregazione, associazione e contestualizzazione e presentazione di una visione olistica e costante della *security posture*. Altri obiettivi sono la riduzione del rischio e dei disservizi, il controllo e la prevenzione delle minacce cyber, la riduzione dei costi amministrativi, la capacità di investigare in maniera appropriata gli incidenti di sicurezza e il supporto nelle attività di audit e di *compliance* a leggi, norme, standard e *best practice* di settore.

Per raggiungere i propri obiettivi il SOC deve essere in grado di effettuare determinate azioni - organizzate in **domini funzionali** - che comprendono, come minimo, funzioni quali gestione dei log (collezione, conservazione e analisi), monitoraggio e correlazione degli eventi di sicurezza, gestione degli incidenti, identificazione e reazione alle minacce e attività di reporting.

L'azione del SOC è possibile tramite la combinazione di elementi quali **tecnologia**, **persone** e **processi**; è importante sottolineare che il termine stesso "SOC" non è inequivocabile ed è figlio delle evoluzioni del mercato della sicurezza delle informazioni. Esistono altre parole per identificare forme organizzative le cui funzioni, *capability* e obiettivi sono identici a quelli di un SOC, quali ad esempio i *Computer Emergency Response Team* (CERT) e i *Computer Security Incident Response Team* (CSIRT).

Il SOC utilizza numerose **tecnologie**, quali ad esempio sistemi di *Security Information Event Management* (SIEM), *Database Activity Monitoring* (DAM), *Intrusion Detection/Prevention System* (IDS/IPS), *Next-Generation Firewall*, *Malware Protection*, *Sandbox*, etc. Data la natura estremamente dinamica del panorama delle minacce cyber, è naturale per il SOC avvalersi costantemente delle tecnologie di sicurezza allo stato dell'arte, ampliando continuamente il novero delle capacità tecniche a disposizione e aggiornando di conseguenza le proprie capacità operative. Le **persone** sono il fattore centrale e distintivo del SOC e di solito esiste una struttura multilivello all'interno dell'organizzazione per svolgere azioni diverse e complementari. Ogni livello (*tier*) ha compiti e responsabilità ben identificate e si relaziona con gli altri secondo procedure chiare. La matrice degli skill delle persone che compongono un SOC comprende sia *hard skill* (conoscenza di protocolli di rete, tecnologie di sicurezza specifiche, sistemi e reti IT, etc) sia *soft skill* (capacità di operare sotto stress, attitudine alla comunicazione, capacità di gestire le relazioni con colleghi e clienti, etc). Per la natura specifica delle minacce che deve fronteggiare, il SOC è operativo 24 ore al giorno per tutto l'anno: gli attacchi informatici (automatici e manuali) sono sferrati continuamente e da qualsiasi parte del pianeta in modalità *follow-the-sun*. Al fine di garantire adeguati livelli di efficienza ed efficacia, il SOC opera secondo **processi** divisi in quattro categorie: di business, tecnologici, operativi e analitici.

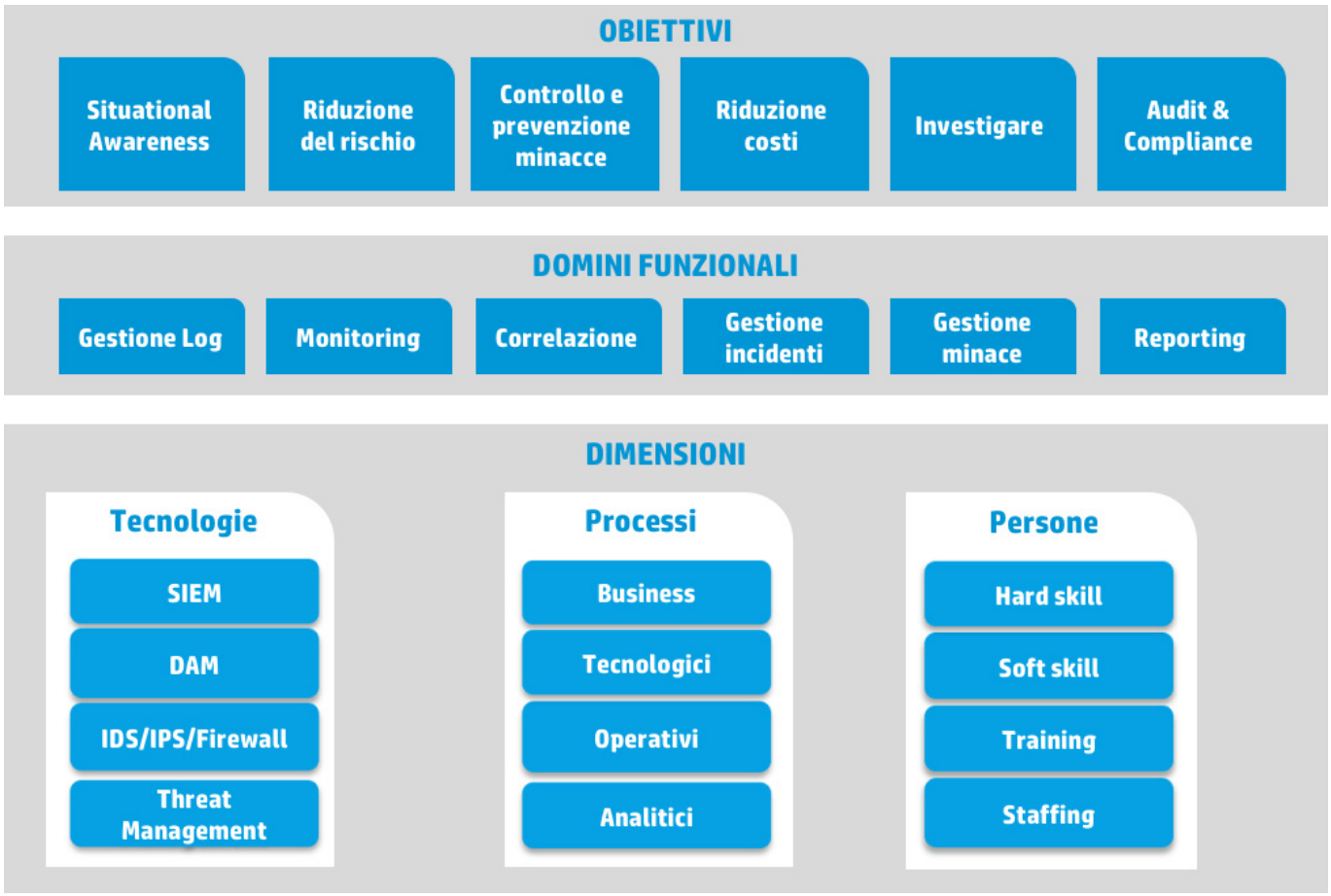

Figura 1 - Modello di SOC

Il SOC soddisfa le esigenze della propria *constituency* erogando un insieme di servizi, altrimenti noti come ***capability***, che possono essere raggruppate in cinque generazioni[3] e che verranno successivamente illustrate.

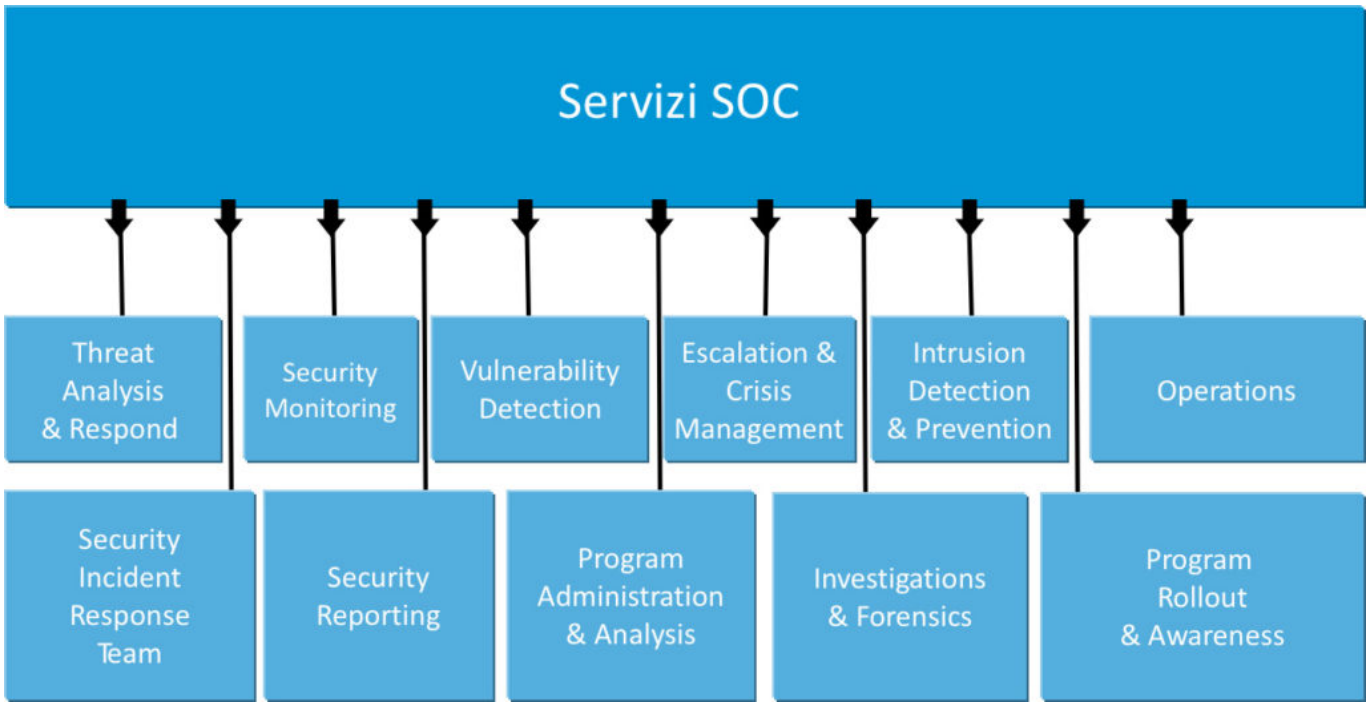

Figura 2 - Esempio di servizi SOC

Le dimensioni, l'ampiezza delle *capability* e del catalogo servizi, le competenze e la forma organizzativa dei SOC variano in funzione del valore che l'*asset* "informazione" riveste per la *constituency*.

Dal punto di vista del mercato esistono diverse tipologie di SOC[4]:

Tipo di SOC	**Struttura dedicata**	**Team dedicato**	**Modalità**	**In house**	**Outsourced**
Virtuale	No	No (part time)	Reattivo	No	Si
Dedicato	Si	Si	Proattivo	Si	No
Distribuito	No	Si	Proattivo	Si	Si
Command	Si	Si	Proattivo focalizzato su Threat Intelligence	Si	Si
Multifunzione (SOC/NOC)	Si	Si (svolge operazioni di rete e di sicurezza)	Reattivo	Si	Si

Capability e livelli di maturità

Uno dei problemi legati alla valutazione dell'efficacia e dell'efficienza di un SOC nel perseguimento dei propri obiettivi è la possibilità di misurarne le *performance* (tramite appositi

indicatori prestazionali o KPI) e la qualità della *governance.* La misura della maturità delle *capability* è un metodo usato in molte aree, interne ed esterne al dominio IT, per determinare l'andamento dei processi e dei vari elementi all'interno di un'organizzazione. I risultati di tali *assessment* periodici evidenziano aree di forza e di debolezza, aiutando a indirizzare eventuali gap tramite interventi mirati e piani di rientro in accordo al paradigma del *continuous improvement*[5]. Un modello autorevole e universalmente riconosciuto è il *Capability Maturity Model Integration* (CMMI) della Carnegie Mellon University[6] , che identifica livelli di maturità crescenti e codificati in valori numerici (da 0, che indica l'assenza del processo, a 5, che indica l'esistenza di un processo ottimizzato). La misurazione dei livelli di maturità delle *capability* di un SOC avviene tramite scomposizione del dominio di analisi in diverse dimensioni di indagine; un ottimo riferimento è rappresentato da **SOC-CMM**[7], che fornisce sia una metodologia sia gli strumenti di lavoro per effettuare il *Maturity Assessment* misurando 5 ambiti di analisi (Business, Persone, Processi, Tecnologia, Servizi).

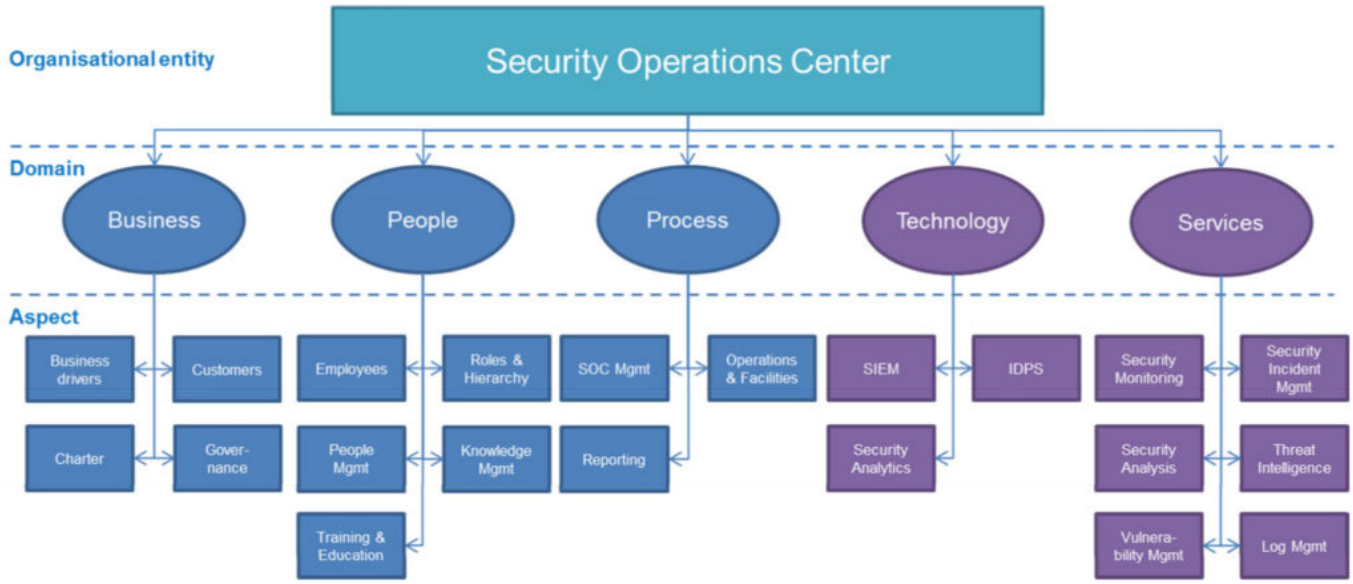

Figura 3 - Modello SOC-CMM

Storia dei SOC

La breve storia dei SOC che segue è tratta dal *Business White Paper "5G/SOC: SOC Generations"* rilasciato da Hewlett Packard Enterprise ed è un tentativo di correlare i principali eventi storici di sicurezza alle forme che i vari SOC hanno adottato nel corso del tempo.

SOC di prima generazione – Dagli anni 70 al 1995

I SOC di prima generazione si sono sviluppati per quasi 25 anni e sono nati insieme a Internet. Durante questo periodo le connessioni Internet non erano ubiquitarie come lo sono oggi e molti business non erano nemmeno connessi alla rete. Gli attacchi erano tipicamente programmi seccanti che comportavano un impatto minimo sulla capacità delle varie organizzazioni di

erogare i propri servizi *core*. Verso la fine di questa generazione, ambienti governativi e militari iniziarono a stabilire i *Computer Emergency Response Team* (CERT) ponendo le fondamenta di ciò che oggi chiamiamo Security Operations Center. Inoltre, cominciano ad apparire tecnologie di sicurezza quali gli anti-virus e gli Intrusion Detection System (IDS).

- 1972 Introduzione del primo modem full duplex a veocità di 1.200 baud per second
- 1974 Sviluppo della tecnologia Ethernet
- 1979 Kevin Mitnick - tramite *social engineering* – ottiene accesso a sistemi DEC[8]
- 1981 Lo SmartModem Hayes (14.4kbs) diventa popolare nel circuito delle BBS
- 1983 Esce il film “War Games”
- 1986 Negli Stati Uniti, il *Computer Fraud and Abuse Act and the Electronic Communications Privacy Act* rende l’accesso informatico non autorizzato un reato
- 1987 *Christmas Tree Exec*, primo software auto-replicante, si diffonde in maniera dirompente[9]
- 1987 Viene creato il tool *tcpdump*
- 1987 McAfee & Associates crea il primo software antivirus[10]
- 1992 Viene lanciato sul mercato DEC SEAL, primo firewall commerciale[11]
- 1993 Viene rilasciato Windows 3.11 con funzionalità di rete *peer to peer*
- 1993 USAF crea il *67th Air Intelligence Wing* (AFCERT) foclizzato sulla *Cyber Intelligence*
- 1995 Wheelgroup lancia il primo Intrusion Detection System: *NetRanger***[12]**

SOC di seconda generazione – 1996 – 2001: Esplosione del malware e sviluppo degli IDS

I SOC di seconda generazione sono nati verso la fine del ventesimo secolo. Questa generazione ha visto la nascita dei *Managed Security Service Provider* (MSSP) e l’introduzione di risorse preziose per la sicurezza delle informazioni quali la mailing list di *Packet Storm*, il *SANS Institute Internet Storm Center* e il database delle *Common Vulnerabilities and Exposure* (CVE). La propagazione di *worm* e virus inizia ad avere un impatto crescente e piattaforme di tipo SIEM (*Security Information Event Management*) come ArcSight e netForensics si affacciano sul mercato.

- 1996 *Managed Security Service Provider* iniziano a offrire servizi di gestione Firewall e IDS[13]
- 1998 Viene creato SNORT[14]
- 1999 Mitre crea il *repository* CVE[15]
- 1999 SANS crea il precursore dell’Internet Storm Center
- 1999 Viene lanciata la mailing list PacketStorm
- 1999 Il virus “*Happy99*” colpisce Outlook Express, il worm “*Melissa*” attacca Microsoft Word
- 2000 Diffusione del virus “*ILOVEYOU*” (LoveBug)
- 2001 Il *worm* “*Sadmind*” attacca Sun Solaris[16], i *worm*“*Code Red*” e “*Code Red II*” attaccano MS IIS, si diffonde il *worm* “*Nimda*”
- 2001 I prodotti SIEM (Security Information Event Management) sono introdotti sul mercato

SOC di terza generazione – 2002 – 2005: Botnet, Cybercrime, Intrusion Prevention, Compliance

La terza generazione dei SOC è esistita tra il 2002 e il 2005. Botnet controllate centralmente e requisiti di *compliance* proliferano e molte grandi aziende costituiscono i propri SOC.

- 2002 Il *Sarbanes Oxley Act* prescrive controlli di sicurezza IT e introduce responsabilità individuali per le figure apicali all'interno delle organizzazioni
- 2003 Si diffondo i worm "*SQL Slammer*", "*Blaster*", "*Nachi*", "*Sobig*" e "*Sober*"
- 2003 HD Moore crea il *framework Metasploit***[17]**
- 2003 Viene creato lo US-CERT[18]
- 2003 La legge della California SB 1386 obbliga la notifica al consumatore nel caso in cui le proprie informazioni personali (PII) siano rivelate a terze parti: è considerata la prima legge che obbliga a notificare il *data breach*
- 2004 Viene formato il *PCI council*
- 2004 Si diffondo i *worm* "*Bagle*" e "*MyDoom*"
- 2004 Primo attacco rilevato tramite l'utilizzo di *entry* di tipo *wildcard* sul DNS[19]
- 2004 Primo *malware* per piattaforme mobile ("*Cabir*", scritto per Symbian OS)
- 2004 Operazione *Titan Rain* (attacco cinese contro sistemi governativi e militari degli Stati Uniti)[20]
- 2005 Diffusione del *worm* "*Zotob*"

SOC di quarta generazione - 2006 – 2012: Cyberwar, Hacktivisim, APT, data exfiltration

I SOC di quarta generazione coprono un periodo che va dal 2006 al 2012 circa. I temi principali sono relativi all'Hacktivism, alle minacce interne (*insider threat*), all'ingresso nell'arena degli Stati Nazione e al furto di proprietà intellettuale.

- 2007 *Zeus* Trojan/Botnet
- 2007 Data breach della TJX[21]
- 2007 La Russia attacca l'Estonia nella prima *cyberwar* pubblicamente conosciuta[22]
- 2007 Il gruppo Anonymous guadagna le prime attenzioni mediatiche
- 2008 Diffusione del *worm Conficker* e delle relative Botnet
- 2008 Data breach della Hannaford Bros[23]
- 2009-2010 *Operazione Aurora* – attacchi Cinesi contro aziende quali Google, Adobe Systems, Juniper Networks, Yahoo, Symantec, Northrop Grumman, Morgan Stanley e Dow Chemical[24]
- 2010-2011 WikiLeaks pubblica il Baghdad Air Strike video e numerosi dispacci diplomatici[25]
- 2010 Il *trojan Stuxnet* attacca sistemi SCADA Iraniani[26]
- 2011 Data breach subito da RSA[27]

SOC di quinta generazione – 2012 – oggi: Automazione, Analytics, Big Data, Information Sharing, Machine Learning, Threat Management & Intelligence, Predictive Analysis

I SOC di quinta generazione sono ancora in evoluzione. Il panorama delle minacce cyber si sta evolvendo ad un ritmo senza precedenti e i mercati chiedono e offrono prodotti e servizi sempre

più avanzati. I SOC di quinta generazione riconoscono il cambiamento del panorama delle minacce e approcciano la sfida in maniera olistica: addestrando gli analisti in ambiti quali *counter-intelligence* di sicurezza, sorveglianza, psicologia criminale e pensiero analitico. Gli sforzi di standardizzazione e conformità hanno facilitato l'adozione diffusa di prodotti e pratiche di sicurezza.

- 2012 Attacco contro Foxconn, Linkedin subisce il furto di 6.5 milioni di credenziali
- 2012 Saudi Aramco subisce per mesi un attacco cyber tramite malware *Shamoon*, che distrugge 35.000 computer della compagnia[28]
- 2013 Edward Snowden divulga i programmi di sorveglianza di massa delle maggiori intelligence occidentali[29]
- 2014 Data Leak ai danni della Sony[30]
- 2017 Attacco del *ransomware Wannacry***[31]**
- 2017 Attacco cyber di *Petya***[32]** e data breach alla Equifax[33]

Conclusione

I rapporti sociali di produzione attuali si fondano su un fattore determinante: l'Informazione. La *Digital Transformation* espone l'Informazione a rischi direttamente proporzionali alla dinamica di crescente centralità delle ICT ed è sempre più urgente attivare adeguate capacità di difesa contro attacchi e minacce. Il SOC è l'eccellenza operativa di tali capacità e i servizi che lo caratterizzano rappresentano la frontiera mobile entro cui proteggere l'Informazione nelle dimensioni di sicurezza che le sono proprie: **Riservatezza, Integrità** e **Disponibilità**.

NOTE

- [1] https://www.nist.gov/cyberframework
- [2] https://it.wikipedia.org/wiki/Situational_awareness
- [3] https://www.slideshare.net/slideshow/embed_code/key/3pM9UIQoZSwEVb https://community.softwaregrp.com/t5/Security-Operations-Thought/5G-SOC-Generations-pdf/ta-p/1587382
- [4] https://www.gartner.com/newsroom/id/3815169
- [5] https://en.wikipedia.org/wiki/Continual_improvement_process
- [6] https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration
- [7] https://www.soc-cmm.com
- [8] http://passwordresearch.com/stories/story47.html
- [9] https://it.wikipedia.org/wiki/Christmas_Tree_EXEC
- [10] https://en.wikipedia.org/wiki/John_McAfee
- [11] https://www.darkreading.com/who-invented-the-firewall/d/d-id/1129238
- [12] https://en.wikipedia.org/wiki/WheelGroup
- [13] https://en.wikipedia.org/wiki/Managed_security_service
- [14] https://en.wikipedia.org/wiki/Snort_(software)
- [15] https://cve.mitre.org
- [16] https://en.wikipedia.org/wiki/Sadmind
- [17] https://en.wikipedia.org/wiki/Metasploit_Project

- [18] https://www.us-cert.gov
- [19] https://tools.ietf.org/html/rfc3833
- [20] https://en.wikipedia.org/wiki/Titan_Rain
- [21] https://www.computerworld.com/article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html
- [22] https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
- [23] https://www.networkworld.com/article/2284998/lan-wan/details-emerging-on-hannaford-data-breach.html
- [24] https://en.wikipedia.org/wiki/Operation_Aurora
- [25] https://wikileaks.org
- [26] https://en.wikipedia.org/wiki/Stuxnet
- [27] https://www.theregister.co.uk/2011/04/04/rsa_hack_howdunnit/
- [28] https://en.wikipedia.org/wiki/Shamoon
- [29] https://it.wikipedia.org/wiki/Edward_Snowden
- [30] https://en.wikipedia.org/wiki/Sony_Pictures_hack
- [31] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- [32] https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine
- [33] https://en.wikipedia.org/wiki/Equifax#May.E2.80.93July_2017_security_breach

A cura di: **Andrea Boggio**