TO MATURITY AND BEYOND: THE HISTORY AND PRACTICE OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS

AUTHOR & LICENSOR:
EMMA WOODWARD

LITERATURE
(RELATING TO IR & EFFECTIVENESS)

STANDARDS, LEGISLATION REGULATION FRAMEWORKS

POLICIES
STANDARDS/ CONTROLS
PROCEDURES

TOOLS TECH TECHNIQUES

INSTITUTIONS ORGANISATIONS PIONEERS

MAJOR CYBER ATTACKS & EVENTS

+10 YEARS

2026 2025 2024 2023 2022 2021 2020 2019 2018 2017 2016 2015 2014 2013 2012 2011 2010 2009 2008 2007 2006 2005 2004 2003 2002 2001 2000 1999 1998 1997 1996 1995 1994 1993 1992 1991 1990 1989 1988 1987 1986 1985 1984 1983 1982 1981 1980

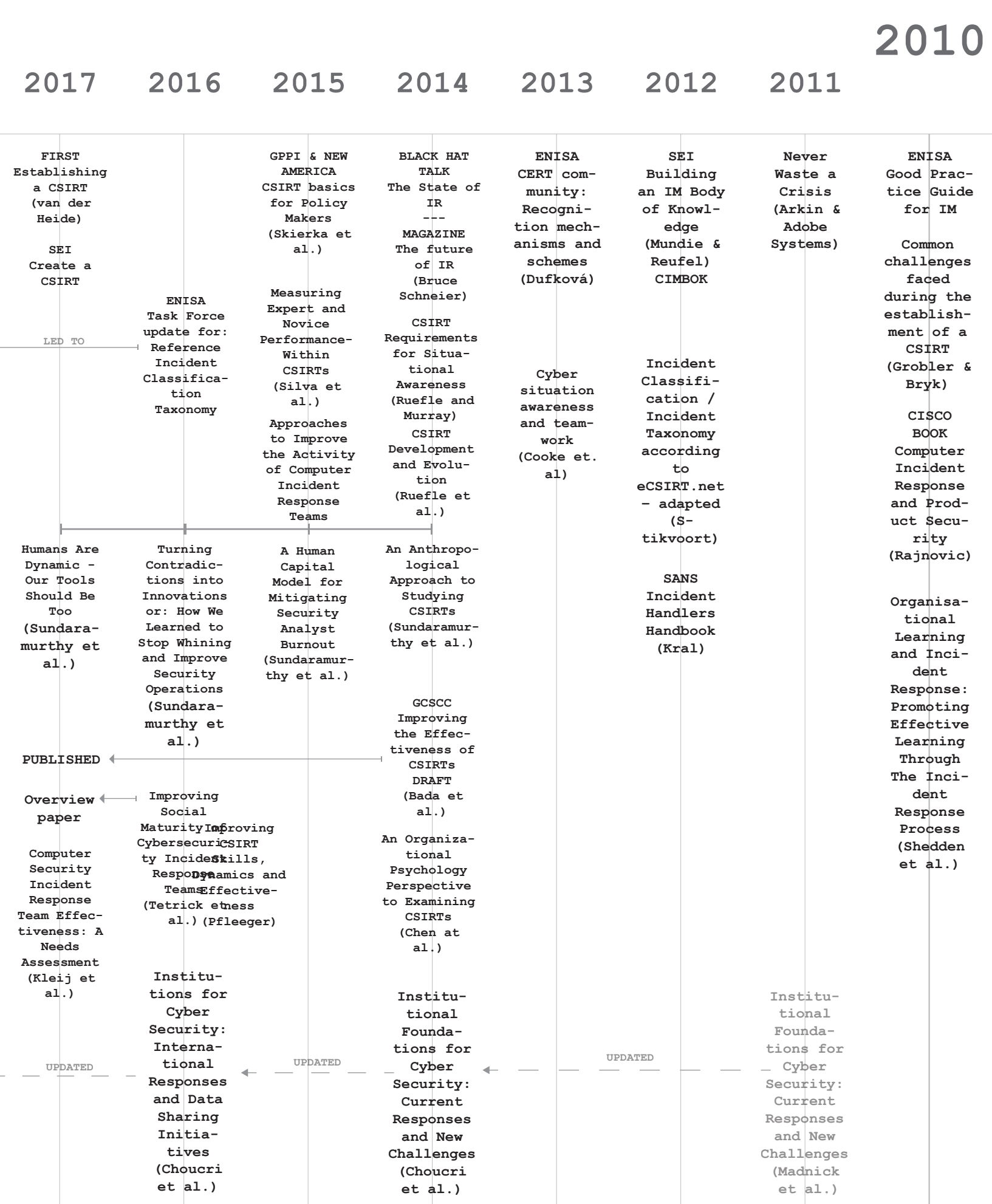
KEY

ACRONYMS
IM: INCIDENT MANAGEMENT
IR: INCIDENT RESPONSE
CERT: COMPUTER EMERGENCY RESPONSE TEAM
CSIRT: COMPUTER SECURITY INCIDENT RESPONSE TEAM

SYMBOLS
SOLID LINES: CASSED AS A KEY PAPER
GREYED OUT: SUPERCEDED
SOLID LINE: UPDATE OR CONSEQUENCE
SOLID LINE WITH CIRCLE ENDS: LINKED 2 WAYS
SOLID LINE WITH ARROW: LINKED 1 WAY
SOLID LINE WITH FLAT ENDS: THEME
NB: ANYTHING THAT ISN'T A PAPER IS DETAILED

COMMON REFERENCES
THESE HAVE BEEN NUMBERED FOR EASE OF READ ON THE MAP BECAUSE OF THEIR FREQUENT USE

[1] Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989-2005 (Slayton & Clarke)
[2]Bruce Schneir - The future of IR (not complete)
[3]TREND MICRO - overview of viruses and IR (not complete)
[4]Evolution Of Security Operations Center
[5]Security Engineering: A guide to building dependable distributed systems
[6]https://www.futurefast.org/cybersecurity/2-history-of-cybersecurity/
[7] https://blog.rsisec.com/history-of-cybersecurity-4vsat
[8]https://www.sentinelone.com/blog/short-history-of-ddos/
[9]https://www.techtarget.com/searchsecurity/definition/ZOAA


2017
2016
2015
2014
2013
2012
2011
2010
FIRST Establishing a CSIRT (van der Heide)
SEI Create a CSIRT
LED TO
ENISA Task Force update for: Reference Incident Classification Taxonomy
GPPI & NEW AMERICA CSIRT basics for Policy Makers (Skierka et al.)
Measuring Expert and Novice Performance-Within CSIRTs (Silva et al.)
Approaches to Improve the Activity of Computer Incident Response Teams
BLACK HAT TALK The State of IR

MAGAZINE The future of IR (Bruce Schneier)
CSIRT Requirements for Situational Awareness (Ruefle and Murray)
CSIRT Development and Evolution (Ruefle et al.)
ENISA CERT community: Recognition mechanisms and schemes (Dufková)
Cyber situation awareness and teamwork (Cooke et. al)
SEI Building an IM Body of Knowledge (Mundie & Reufel) CIMBOK
Incident Classification / Incident Taxonomy according to eCSIRT.net - adapted (Stikvoort)
SANS Incident Handlers Handbook (Kral)
Never Waste a Crisis (Arkin & Adobe Systems)
ENISA Good Practice Guide for IM
Common challenges faced during the establishment of a CSIRT (Grobler & Bryk)
CISCO BOOK Computer Incident Response and Product Security (Rajnovic)
Organisational Learning and Incident Response: Promoting Effective Learning Through The Incident Response Process (Shedden et al.)
Humans Are Dynamic - Our Tools Should Be Too (Sundaramurthy et al.)
Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations (Sundaramurthy et al.)
A Human Capital Model for Mitigating Security Analyst Burnout (Sundaramurthy et al.)
An Anthropological Approach to Studying CSIRTs (Sundaramurthy et al.)
PUBLISHED
GCSCC Improving the Effectiveness of CSIRTs DRAFT (Bada et al.)
Overview paper
Improving Social Maturity in Cybersecurity Incident Response Teams (Tetrick et al.)
Improving CSIRT Skills, Dynamics and Effectiveness (Pfleeger)
An Organizational Psychology Perspective to Examining CSIRTs (Chen at al.)
Computer Security Incident Response Team Effectiveness: A Needs Assessment (Kleij et al.)
UPDATED
Institutions for Cyber Security: International Responses and Data Sharing Initiatives (Choucri et al.)
UPDATED
Institutional Foundations for Cyber Security: Current Responses and New Challenges (Choucri et al.)
UPDATED
Institutional Foundations for Cyber Security: Current Responses and New Challenges (Madnick et al.)