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

+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
LED TO
UPDATED
PUBLISHED
FUNDING UNTIL 2005 [3 - CHECK!]
DEVELOPED
CHAIRED SURFcert
FOUNDING MEMBER
PART OF
LED TO THE CREATION OF
AVAILABLE SINCE 2016 [3]

LITERATURE (RELATING TO IR & EFFECTIVENESS)

2023 — The Impact of Organizational Structure and Technology Use on Collaborative Practices in CERTs: An Empirical Study (Riebe et al.)
SANS 2023 SOC survey (Crowley et. al)
SANS 2023 SOC survey (Crowley et. al)

2022 — ENISA CSIRT Maturity Framework - Updated and improved
Action Bias and the Two Most Dangerous Words in Cybersecurity IR: An Argument for More Measured IR (Dykstra et al.)
GCSCC SEI (CMU) CSIRTs: An Overview
How national CSIRTS operate: Personal Observations and Opinions from MyCERT (Kassim et al.)
BOOK CHAPTER Security Management Programs: Moving Towards Socio-Technical IR Learning (Østby & Kowalski)
Incident Response Practices Across National CSIRTs: Results from an Online Survey (Roziah et al.)
FIRST CSIRT Services Roles and CompetencieS

2021 — Stepping out of the shadow: CSIRTs in the cybersecurity ecosystem (van der Meulen)

2020 — FIRST PSIRT (Product Security Incident Response Team) Services Framework

2019 — ENISA Study on CSIRT landscape and IR capabilities in Europe 2025
FIRST CSIRT Services Framework Version 2.1.0
Trusting Infrastructure: The Emergence of Computer Security IR, 1989-2005 (Slayton & Clarke)

2018 — TREND MICRO A Historical Overview of Proactive IR Strategies and What They Mean to Enterprises
ENISA Reference Incident Classification Taxonomy
BOOK CHAPTER PUBLISHED (Choucri et al.)

2017 — FIRST Establishing a CSIRT (van der Heide)
SEI Create a CSIRT
Humans Are Dynamic - Our Tools Should Be Too (Sundaramurthy et al.)
Overview paper
Computer Security Incident Response Team Effectiveness: A Needs Assessment (Kleij et al.)

2016 — ENISA Task Force update for: Reference Incident Classification Taxonomy
Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations (Sundaramurthy et al.)
Improving Social Maturity of Cybersecurity Incident Response Teams (Tetrick et al.)
Improving CSIRT Skills, Dynamics and Effectiveness (Pfleeger)
Institutions for Cyber Security: International Responses and Data Sharing Initiatives (Choucri et al.)

2015 — 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
A Human Capital Model for Mitigating Security Analyst Burnout (Sundaramurthy et al.)

2014 — 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.)
An Anthropological Approach to Studying CSIRTs (Sundaramurthy et al.)
GCSCC Improving the Effectiveness of CSIRTs DRAFT (Bada et al.)
An Organizational Psychology Perspective to Examining CSIRTs (Chen at al.)
Institutional Foundations for Cyber Security: Current Responses and New Challenges (Choucri et al.)

2013 — ENISA CERT community: Recognition mechanisms and schemes (Dufková)
Cyber situation awareness and teamwork (Cooke et. al)

2012 — SEI Building an IM Body of Knowledge (Mundie & Reufel) CIMBOK
Incident Classification / Incident Taxonomy according to eCSIRT.net – adapted (S-tikvoort)
SANS Incident Handlers Handbook (Kral)

2011 — Never Waste a Crisis (Arkin & Adobe Systems)
Institutional Foundations for Cyber Security: Current Responses and New Challenges (Madnick et al.)

2010 — 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.)

2009 — Chronic Workload Problems In CSIRTs

Preserving a balanced CSIRT constituency

Persistent instabilities in the high-priority incident workload of CSIRTs (Wiik et al.)
Adapting the Ticket Request System to the Needs of CSIRT Teams (Kácha)
OTRS: streamlining CSIRT IM workflow (Kácha)
Developing a Community Cyber Security IR Capability (White & Granado)

2008 — CERT/CC (SEI) Creating and managing CSIRTS (Killcrece)
CERT/CC (SEI) FAQ: Collaboration Between the CERT Coordination Center and CSIRTs Worldwide
CERT/CC (SEI) IM Mission Diagnostic Method, Version 1.0 (Dorofee et al.)
Incident Response Probabilistic Cognitive Maps (Krichene & Boudriga)

2007 — CERT/CC (SEI) PODCAST The Real Secrets of IM (Losi et. al)

2006 — ENISA Step-by-step approach on how to set up a CSIRT (Bronk et al.)
CERT/CC (SEI) PODCAST CERT Lessons Learned: A Conversation with Rich Pethia, Director of CERT
Effectiveness of Proactive CSIRT Services (Wiik et al.)
On Incident Handling and Response: A state-of-the-art approach (Mitropoulos et al.)
Technical Infrastructure of a CSIRT (Penedo)

2005 — CERT/CC (SEI) IM (Killcrece)
Limits to Effectiveness in CSIRTS (Wiik et al.) 'Capability Trap'

2004 — FIRST CSIRT Case Classification: Ex for enterprise CSIRTS (Reid et al.)
CERT/CC (SEI) Defining IM Processes for CSIRTs: A Work in Progress (Alberts et. al)

Steps for Creating National CSIRTs (Killcrece)
SANS IM 101 Preparation and Initial Response (Dikerson)
An Exploratory Investigation of Factors Affecting CSIRT Performance (Lee & Lee)

2003 — CERT/CC (SEI) State of the Practice of CSIRTS (Killcrece et al.) CERT CSIRT DEVELOPMENT TEAM
CERT/CC (SEI) Organizational Models for CSIRTs (Killcrece et al.)
These are designed to go hand in hand
CERT/CC (SEI) Handbook for CSIRTs (West-Brown et al.)

2002 — SANS Incident Response in A Global Environment (Kelver)

2001 — SANS Computer Security Incident Team (Borodkin)

1999 — CERT/CC (SEI) International Infrastructure for Global Security Incident Response (West-Brown & Kossakowski)

1998 — A common langugae for computer security incidents (Howard & Longstaff)
SEI Handbook for CSIRTs (West-Brown et al.)

1997 — An Analysis Of Security Incidents On The Internet 1989 - 1995 (Howard)
SANS Computer Security Incident Handling, Step-by-Step. (Northcutt)

1996 — A computer emergency response team policy (Wood)

1995 — The DFN-CERT Project: The first 18 months (Kossakowski)

1994 — FIRST Forming an IR Team (Smith)
CERT IR & the Internet (NEED TO FIND)

1993 — RARE CERT Task Force: Guide to Setting up a CERT

1991 — Establishing a Computer Security IR Capability (Wack) CSIRC
Computer emergency response – an international problem (Pethia & Wyk)

1990 — BOOK Computers Under Attack (Denning)
BOOK Coping with the Threat of Computer Security Incidents: A Primer from Prevention Through Recovery (Brand)
Responding to computer security incidents: Guidelines for incident handling (Schultz et al.)
The Computer Fraud and Abuse Act of 1986 and the Computer Security Act of 1987: Impact on incident response efforts (Griffith)

1989 — K.R. Van Wyk joins CERT CC

KEY

ACRONYMNS
IM: INCIDENT MANAGEMENT
IR: INCIDENT RESPONSE
CERT: COMPUTER EMMERGENCY RESPONSE TEAM
CSIRT: COMPUTER SECURITY INCIDENT REPSONSE TEAM

SYMBOLS
STAR: CLASSED AS A KEY PAPER
GREYED OUT: SUPERCEEDED
DOTTED LINE: UPDATE OR CONCEQUENCE
SOID 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 REFERNCES
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 - review 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.futureoftech.org/cybersecurity/2-history-of-cybersecurity/
[7] https://blog.avast.com/history-of-cybersecurity-avast
[8]https://www.sentinelone.com/blog/short-history-of-edr/
[9]https://www.techtarget.com/searchsecurity/definition/SOAR

STANDARDS, LEGISLATION REGULATION FRAMEWORKS

POLICIES
STANDARDS/ CONTROLS
PROCEDURES

NIST SP 800-53 REV 5. (UPDATED TO INCL. MAPPING TO ISO 27001) — Security and Privacy Controls for Information Systems and Organizations — REV 4. — REV 3. — REV 2. — REV 1.

NIST SP 800-61 V2 — Computer Security Incident Handling Guide(Cichonski et al.) — V1 — Initial Release

NIST CYBERSECURITY FRAMEWORK 2.0 — Risk management framework — Initial Release - V1.0

CYBER ESSENTIALS (CE) V3.1 — Security compliance certificate based on 5 pillars (CE+ 4rd party accreditation) — CYBER ESSENTIALS LAUNCHED

BS EN ISO/IEC 27001:2023 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements — BS EN ISO/IEC 27001:2013

BS EN ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls — ISO 17799 RENAMED TO ISO 27002 — 'A code of practice for information security'

BS ISO/IEC 27035-1:2023 — Information technology — Information security incident management — BS ISO/IEC 27035-1:2016 — BS ISO/IEC 27035-1:2011

EU ENFORCES GDPR — General data protection regulation

EU COMISSION NIS 2 DIRECTIVE — Directive on security of network and information systems (Critical National Infrastructure focus) — NIS 1

IETF RFC 7203 IODEF STANDARD EXT.FOR STRUCTURED CYBERSECURITY INFO — Incident Object Description Exchange & Exchange format(Danyliw et al.) — IETF RFC 5070 IODEF STANDARD (Danyliw et al.) — IETF RFC 3067 TERENA'S REQUIREMENTS (Arvidsson et al. incl. Cormack)

OCF SIM3 — Security IM Maturity Model (Stikvoort) — INITIAL RELEASE

FIRST TLP V2 — Traffic Light Protocol "set of designations to ensure sensitive information is shared with the appropriate audience" — FIRST TLP V1

Is this still considered/used?
PAS 555:2013 — Publically available specification

IETF RFC 2350 — Expectations for Computer Security IR (Brownlee & Guttman) — INITIAL RELEASE
Template for communication with constituencies

Computer Security Act of 1987

CFAA The Computer Fraud and Abuse Act of 1986 (US Legislation)

TOOLS TECH TECHNIQUES

"FOCUS ON RESPONSE" FOR PRODUCTS AND SERVICES [2]
"DETECTION WAS FORMALISED" FULL OF DETECTION PRODUCTS AND SERVICES [2]
"THE ERA OF PROTECTION" "FULL OF PRODUCTS TO PROTECT COMPUTERS & NETWORKS" [2]

CYBER DEFENSE CENTRE/CFC/CSOC [4] — NEXT GEN SOC [4] — SOC V3 [4] — SOC V2 [4] — NSOC/SOC V1 [4] — NOC - NETWORK OPERATIONS CENTRE [4]

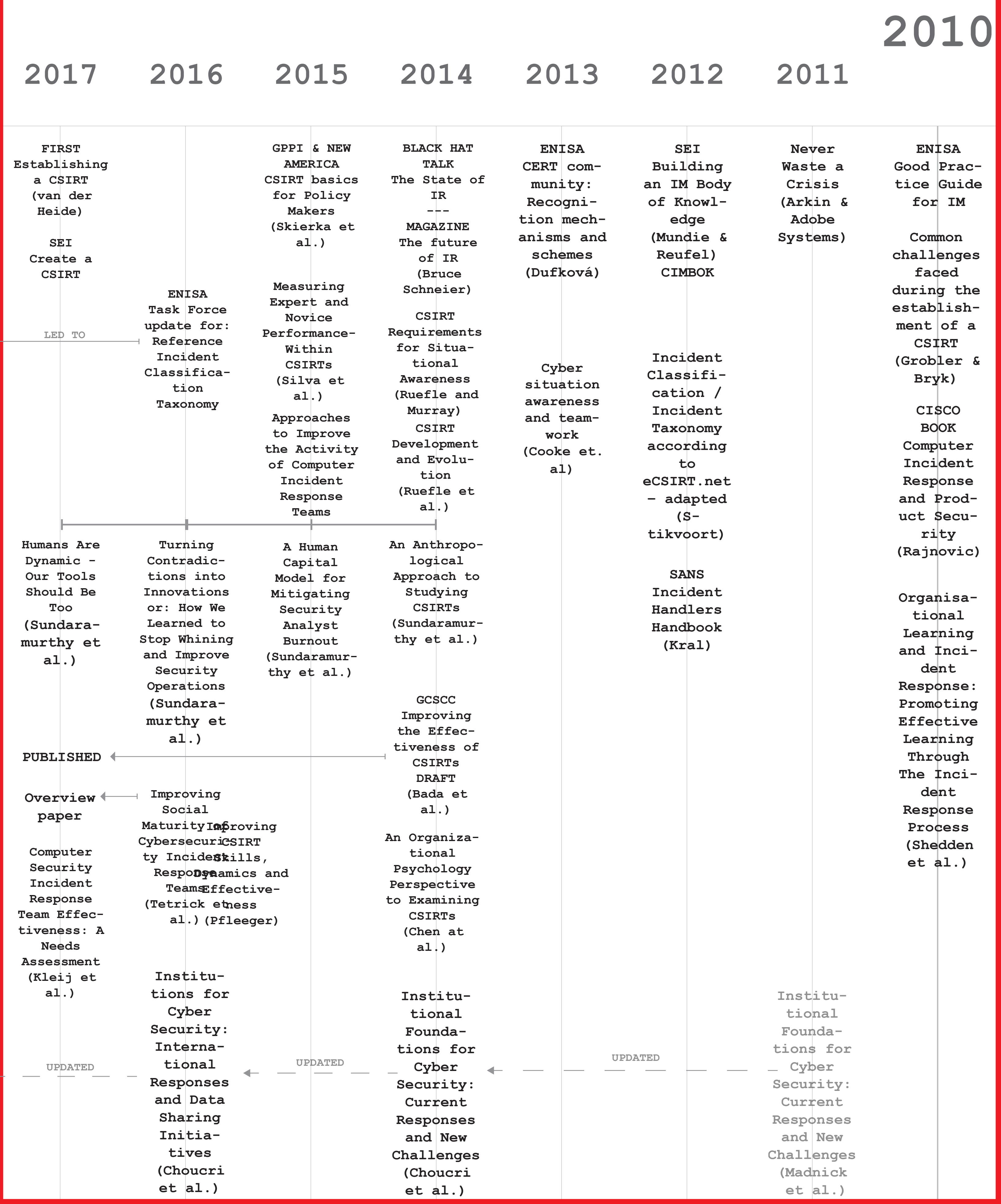
CHRONICLE MERGED WITH GOOGLE CLOUD
MICROSOFT AZURE SENTINEL RELEASED
XDR EXTENDED DETECTION & RESPONSE COINED BY N. ZUK Paolo Alto Networks CTO
CHRONICLE SECURITY FOUNDED
MITRE ATT&CK CREATED
"Blockchain" [5]
SOAR SECURITY ORCHESTRATION, AUTOMATION & RESPONSE NAME UPDATED BY GARTNER
SOAR SECURITY ANALYTICS & REPORTING COINED BY GARTNER
EDR ENDPOINT DETECTION & RESPONSE COINED BY N. ZUK Paolo Alto Networks CTO
Antivirus starts to use big data [6]
POPULARITY OF SMARTPHONES enables instant access to emails
AKA Next-gen firewalls
UTM UNIFIED THREAT MANAGEMENT gains popularity
EPP ENDPOINT PROTECTION PLATFORM COINED BY N. ZUK Paolo Alto Networks CTO
SIEM Secuirty Information and Event Management (Williams & Nicolett)
EMAIL GAINS UBIQUTOUS STATUS (WIKI)
"Frenzy over PKIs" [5]
"Email begins to proliferate" [6]
WEBMAIL + EMAIL CLIENTS
"Firewalls became the star product" [5]
CIA Triad first mentioned?
"Antivirus industry explodes" [6]
"Viruses took over the corporate imagination, and people got rich selling antivirus software" [5]
"Everyone talking about hackers (even if their numbers were tiny)" [5]
Virus-L Set up on Usenet [7]
K. Van Wyk "1st electronic forum devoted to antivirus security" [7]
COMMERCIAL ANTI VIRUS APPLIED TO NETWORK TECHNOLOGY [6]
Availability rose to prominence
Integrity formalised by US Air Force Study
1976 Confidentiality form``alised by US Air Force Study

INSTITUTIONS ORGANISATIONS PIONEERS

EU CyCLONe LAUNCHED European Cyber Crises Liaison Organisation Network
TF-CSIRT COMES UNDER OCF
FIRST LAUNCHES Ethics-FIRST
NCSC FOUNDED — UK Govt. CSIRT — NCSC formed from CERT UK, Centre for cyber assessment (CCA) and CESG (infor security arm of GCHQ)
CERT UK FORMED
CERT UK ANNOUNCED
OCF Est. — Open CSIRT Foundation NOT FOR PROFIT — "an independent not-for-profit organisation with a mission we believe in - improving cyber resilience worldwide. formally speaking is a "stichting" under the law of The Netherlands"
CENTRE FOR CYBER ASSESSMENT (CCA)
CESG INFO SECURITY ARM OF GCHQ
EUROPOL EC3 Est. — Open CSIRT
EU GRANTS ENISA 7YR MANDATE w/expanded set of duties — "ENISA is a facilitator & Information knowledge broker" (Enisa 2013)
AFRICAN TEAMS JOIN FIRST
2nd FIRST ANNUAL MEETING IN N. HEMISPHERE (Singapore) [1]
ENISA EST. — European Union Agency for Cybersecurity — "Improve network & info security in EU"
Used TRANSITS material for training new staff of national CSIRTs[1]
Wyk joins private sector[1]
eCSIRT.net Funded by European Comission Kossakowski & Stikvoorts TI [1?]
US LAUNCHES National Cyber Security Division — 1st Task force dedicated to cybersecurity [6]
US-CERT Est.
TRANSITS TRAINING LAUNCHED Funded by European Comission — Training & socials to develop trusted relationships[CHECK REF]
APCERT Asia Pacific 1st conference
CERT/CC START TO LICENCE MATERIALS
TF-CSIRT LAUNCHED — TERENA Task Force of CSIRTs
TI SCHEME EST. — TRUSTED INTRODUCER SERVICE — "TERENA pay fees for education/research" [1]
G.Killcrece leads CERT CSIRT Dev team
Andrew Cormack Takes charge of British academic CERT JANET-CERT?
Shut down "too top down & confusion over function" [1]
GRIP WORKING GROUP — Guidelines and Recommendations for Incident Processing (Kossakowski & Fraser)
ISACS INTRODUCED (Information Sharing & Analysis Centres)
1st FIRST ANNUAL MEETING IN N. HEMISPHERE (Australia) [1]
FAILED PILOT: EURO-CERT "Basic Incident Response service" funded by TERENA[1]
ITDWG WORKING GROUP — Incident Taxonomy @TERENA
Kossakowski leaves DFN CERT for a private company[1]
"Raid commercialisation of organisations in IR"[1]
FIRST MEMBERS 39% Commercial 27% civilian /Govt. 25% Education
CERTCC-KR (Korea) Est.
1st FIRST ANNUAL MEETING IN EU (outside of US) [1]
IETF BOFS "Guidelines & Recomendations for incident processing" [1]
Kossakowski & Stikvoort start cooperation of CSIRTs
K.P. Kossakowski Helps est. German academic network DFN CERT
D. Stikvoort Helps est. Dutch academic network SURFnet
JPCERT (Japan) Est.
B. Fraser Ambassador joins CERT
M. West-Brown Manager of CERT/CC IR Team
UK join[1]
France join[1]
EICAR EST. — European Institute for Computer Antivirus Research [7]
"Primarily a Govt, research & Education network" [1]
FIRST EST. — Forum of IR & Security Teams
CERT SYSTEM EST. CERT CC + 10 OTHER CSIRTS [CHECK REF -1?]
CIAC EST. — Computer Incident Advisory Capability — "Advise people on computer incidents"
CERT CC & NIST run invitational workshops [1]
SANS EST. — SYSAdmin, Auditn Network & Security
G.Killcrece joins CERT CC
M. Zajicek joins SEI then CERT CC
"A reliable, trusted single point contact for computer emergency response" [1]
DIR R.Pethia
CERT/CC EST. — Computer Emmergency Response
'A SWAT team in cyberspace' (Fifthen & Fraser)
EST. BY DARPA Defence Advanced Research Projects Agency
SEI EST. — Software Engineeering Institute (Administered by CMU Carnegie Mellon University) FFRDC:
OSI PROTOCOLS
TERENA EST. — The Trans European Research & Education Networking Association
RARE Réseaux associés pour la recherche européenne
IETF EST. — Internet Engineering Task Force
DIGITAL REVOLUTION

MAJOR CYBER ATTACKS & EVENTS

LOG4j
COVID-19 HOME WORKING INCREASES
Cira. 6.8 IoT devices PP around globe [6]
SOLARWINDS
NOTPETYA
Lateral movement through a system
ETERNAL BLUE LEAKED BY SHADOW BROKERS
WANNACRY RANSOMWARE [3]
BOARABBIT RANSOMWARE [3]
MIRAI BOTNET [3]
PETYA [3]
GERMAN STEEL MILL ATTACK
POS MALWARE POINT-OF-SALE [3]
SONY PICTURES BREACH [3]
EXPLOIT KITS [3]
BLACKHOLE 2.0 RANSOMWARE [3]
INDUSTRY 4.0
STUXNET 1st Weaponised Malware Attack [6]
TOR BROWSER RELEASED
CONFLICKER (AKA DOWNAD) [3]
KOOBFACE WORM [3]
iPHONE LAUNCHED A computer in every pocket
STORM WORM [3]
LEAP (AKA OOMPA LOOMPA) [3]
MYDOOM VIRUS [3]
DOS ATTACKS: SQL SLAMMER BLASTER WORM [3]
TOR RELEASED
INDUSTRIAL IIoT
EMERGENCE OF CLOUD TECH
CodeRed Fileless worm,buffer overflow attack, trad. antivirus failed [6]
DARK WEB BORN - FREENET
1ST IOT FRIDGES
I LOVE YOU VIRUS Infects 50 million computers [6]
MELISSA VIRUS "entered the user's computer via a Word document and then emailed copies of itself to the first 50 email addresses in Microsoft Outlook. causes $80 million of damage" [7]
SQL INJECTION VULNERABILITY 1ST DOCUMENTED (Jeff Forristal)
CIH VIRUS DRIVE OVERWRITING [3]
MICHAEL ANGELO VIRUS [3]
POLYMORPHIC VIRUSES "code that mutates while keeping the original algorithm intact to avoid detection" [7]
DISC KILLER VIRUS "PC Today releases edition w/ free disc that accidentally contained the virus" [7]
WORMS AGAINST NUCLEAR KILLERS Suspected to have come from Australian Uni [1]
AIDS TROJAN [3]
MORRIS WORM "Before Morris unleashed this worm, the internet was a small town where people thought little of leaving their doors unlocked. Internet Security was seen as mostly a theoretical problem, and software vendors treated security flaws as a low priority" (Lee 2013)
LINKS TO ANTIVIRUS DEVELOPMENT [6]
VIENNA VIRUS [6]
CASCADE VIRUS INFECTED .COM [3]
LEIGH VIRUS COMMAND .COM [3]
INTRO OF THE ETHERNET
1989 INTERNET BORN



2017

FIRST Establishing a CSIRT (van der Heide)

SEI Create a CSIRT

Humans Are Dynamic - Our Tools Should Be Too (Sundaramurthy et al.)

PUBLISHED

Overview paper

Computer Security Incident Response Team Effectiveness: A Needs Assessment (Kleij et al.)

2016

ENISA Task Force update for: Reference Incident Classification Taxonomy

Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations (Sundaramurthy et al.)

Improving Social Maturity of Cybersecurity Incident Response Teams (Tetrick et al.)

Improving CSIRT Skills, Dynamics and Effectiveness (Pfleeger)

Institutions for Cyber Security: International Responses and Data Sharing Initiatives (Choucri et al.)

2015

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

A Human Capital Model for Mitigating Security Analyst Burnout (Sundaramurthy et al.)

2014

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.)

An Anthropological Approach to Studying CSIRTs (Sundaramurthy et al.)

GCSCC Improving the Effectiveness of CSIRTs DRAFT (Bada et al.)

An Organizational Psychology Perspective to Examining CSIRTs (Chen at al.)

Institutional Foundations for Cyber Security: Current Responses and New Challenges (Choucri et al.)

2013

ENISA CERT community: Recognition mechanisms and schemes (Dufková)

Cyber situation awareness and teamwork (Cooke et. al)

2012

SEI Building an IM Body of Knowledge (Mundie & Reufel) CIMBOK

Incident Classification / Incident Taxonomy according to eCSIRT.net – adapted (S-tikvoort)

SANS Incident Handlers Handbook (Kral)

2011

Never Waste a Crisis (Arkin & Adobe Systems)

Institutional Foundations for Cyber Security: Current Responses and New Challenges (Madnick et al.)

2010

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.)