

BRASÍLIA / BRASIL



MARCELO CAIADO, M.Sc.

CISSP, GCFA, GCIH, GSLC, CCO, CCPA, CHFI, CTIA, CCFC, CRC



REALIZAÇÃO:















28 a 31 de Agosto/2023 BRASÍLIA/ BRASIL

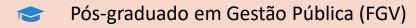
Aviso Legal

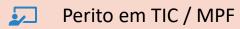
Todas as opiniões apresentadas aqui são exclusivas do orador, apenas para fins ilustrativos, e são pessoais e não representam as de pessoas, instituições ou organizações com as quais o apresentador possa estar associado em capacidade profissional ou pessoal, a menos que explicitamente declarado. Quaisquer opiniões ou pontos de vista não são recomendações técnicas e nem jurídicas, e não têm a intenção de difamar qualquer religião, grupo étnico, clube, organização, empresa ou indivíduo.

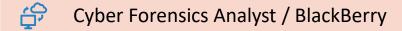


Sobre









Professor (INSPER, IDESP, IPOG e WB)

Coautor dos livros Cyber Risk e Técnicas Avançadas de Investigação

Idealizador e mantenedor do http://dfir.com.br/



BRASÍLIA / BRASIL

Crime organizado



Falta de segurança cibernética

Ransomware

Elevados retornos

Riscos menores



2009.2.27 DEFENSE CHIEF LIFTS BAY OF PICTURES OF COFFINS: IN A REVERSAL OF POLICY, THE PEATAGON WILL ALLOW THE PRESS TO PHOTOGRAPH THE FLAG-DRAPED COFFINS OF AMERICA IS.2.27 U.S., PAKISTAN AND AFGHANISTAN TO HOLD REGULAR TALKS: THE PLAN WAS ANNOUNCED AFTER THREE DAYS OF MEETINGS, WHICH TOUCHED ON SENSITIVE ISSUES LIKE AMERICAN AIRSYRI IVE AT A JEWISH COMMUNITY CENTER IN CARACAS, BUT NOBODY WAS HURT IN THE BLAST. ZODS & 27 WORLD BRIEFING. THE AMERICAS: VENEZUELA: ATTACK ON JEWISH CENTER: ASSAILANTS SE TOWN OF MALAKAL KILLED AT LEAST 14 CIVILIANS AND SCORES OF F... ZODB 2.27 IRAQ HANDS DEATH PENALTY TO 28 CULTISTS FOR ATTACKS: A MESSIANIC SHITE PRINGE GROUP HAS TAKEN S EARLY AS 1.5 MILLION YEARS AGO AN ANCESTRAL SPECIES HAD ALREADY EVOLVED THE FEET AND WALKING GRIT OF MODERN HUMANS. ZOOS. 2. 27 MALBORK JOURNAL: FACING GERMAN SUFFERIA N A TURKISH AIRLINES JET CRASH-LANDED DU MEDNESDAY WERE FOUR AMERICANS AND FIVE TURKS, DUTCH OFFICIALS SAID. 2019.2.27 U.S. WILL GIVE DAEDA SUSPECT A CIVILIAN TRIAL: THE CH JOLVED THE FEET AND WALKING GAIT OF MODERN HUMANS. ZODS. 2.27 WORLD GRIEFING. THE AMERICAS: VEREZUELA: ATTACK ON JEWISH CENTER: ASSAILANTS THREW AN EXPLOSIVE AT A JEWIS E IT HARDER FOR IRAQ TO PAY FOR SERVICES AND COULD AFFECT U.S. PLANS FOR MITHORAWAL, 2009.2. 27 DEFENSE CHIEF LIFTS BAN DII FICTURES OF COFFINS: IN A REVERSAL OF POLICY, THE PRO-SHARIF DEMONSTRATIONS SPREAD ACROSS PUNJAB: THOUSANDS OF SUPPORTERS OF THE OPPOSITION LEADER NAMAZ SHARIF PROTESTED THE SUPPLEME COURT ?? DNOR MONEY INTO HIS PERSONAL BANK ACCOU... ZDOS.Z.Z? IRAQ HANDS DEATH PENALTY TO ZA CULTISTS FOR ATTACKS: A MESSIANIC SHITE FRINGE GROUP HAS TAKEN AIM AT SHITE PILORIMS A LP. GUARDSMEN IN THE WEST BANK ARE TRAIDING TO ENFORCE LAW AND ORDER. 2009.2.27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT THE APOLOGY BY A BISHOP WHO HAS DE LIFTS BAN ON PICTURES OF COFFINS: IN A REVERSAL OF POLICY, THE PENTAGON WILL ALLOW THE PRESS TO PHOTOSRAFH THE FLAG-ORAPED COFFINS OF AMERICA 2008.2.27 U.S., PAKISTAN AN HE SCOPE OF THE AMER... 2009.2.27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT THE APOLOGY BY A BISHOP WHO HAS DENIED THE SCOPE OF THE HOLDCAUST WAS NOT SUFFICIE TRALIA 2009. 2. 27 IN SOUTHEAST ASIA, THE UNEMPLOYED RETURN HOME: AS A MEETING OF THE ASSOCIATION OF SOUTHEAST ASIAN NATIONS EEGINS. THE REGION IS EXPECTING AN EXODUS OF NO S APOLOGIZED FOR REMARKS IN WHICH HE DENIED THE ... ZODS. Z. ZY WORLD SRIEFING - AFRICA : SUDAN : 14 CIVILIANS DIE DURING FIGHTING : THO DAYS OF CLASHES BETWEEN LOCAL GOVERNMENT ZODS, Z. ZY CHINA SAYS U.S. DISTORTS FACTS IN REPORT ON RIGHTS: THE STATE DEPARTMENT SEES. ZODS, Z. ZY IRAQ WITHORAWAL FLAN GAINS G. D. F. SUPPORT: PRESIDENT DEAM I IS TO ALL MORE THAN \$11 MILLION OF INTERNATIONAL DONOR MONEY INTO HIS PERSONAL BANK ACCOU... 2008.2.27 WORLD BRIEFING EUROPE: THE NETHERLANDS: VICTIMS: THE NINE PEOPLE WHO DIED SRI LANKA FEDITOR ACCUSED IN ATTACK: THE POLICE ARRESTED THE EDITOR OF A TAMIL-LANGUAGE NEWSPAPER DURING A FUNERAL IN COLUMNO, THE CAPITAL, ACCUSING HIM OF AIDING A REGEL I NETHERLANDS: VICTIMS: THE NINE PEOPLE WHO DIED WHEN A TURKISH AIRCINES JET CRASH-LANDED ON WEDNESDAY WERE FOUR AMERICANS AND FIVE TURKS, DUTCH OFFICIALS SAID. 2009.2.2 USTRALIAN BUSHFIRES: FIREFIGHTERS CONTAINED EIGHT NEW BUSHFIRES IN AUSTRALIA 2009.2.27 FIREFIGHTERS CONTAIN NEW BUSHFIRES: FIREFIGHTERS CONTAINED EIGHT NEW BU FOUND IN BANGLADESH: POLICE COMBING THROUGH THE HEADQUARTERS OF MUTINOUS BORDER GUARDS HERE FOUND A MASS GRAVE ON FRIDAY CONTAINING AROUND 20 BODIES. AN OFFICIAL SAID. VARIF DEMONSTRATIONS SPREAD ACROSS PUNJAR: THOUSANDS OF SUPPORTERS OF THE OPPOSITION LEADER NAMAZ SHARIF PROTESTED THE SUPREME COURT 2009.2.27 U.S. WILL GIVE DAEGA SU BAKILI MULUZI WAS ARRESTED AND CHARGED WITH SIPHONING MORE THAN \$11 MILLION OF INTERNATIONAL CONCR MONEY INTO HIS PERSONAL BANK ACCOU... 2000. 2.27 WORLD BRIEFING ASIA: 5 YS OF MEETINGS, WHICH TOUCHED ON SENSITIVE ISSUES LIKE AMERICAN AIRSTRIKES IN PARISTAN, AND THE SCOPE OF THE AMER... ZODS. 2. 27 FIREFIGHTERS CONTAIN NEW AUSTRALIAN BUSHFIRE IRIERING THE AMERICAS: VENEZUELA: ATTACK ON JEWISH CENTER: ASSAILANTS THREW AN EXPLOSIVE AT A JEWISH COMMUNITY CENTER IN CARACAS. BUT NOBODY WAS HURT IN THE ELAST. U.S. DISTORTS FACTS IN REPORT ON RIGHTS: THE STATE DEPARTMENT SEES. 2009, 2.27 MASS GRAVE FOUND IN BANGLACESH: POLICE COMBING THROUGH THE HEADQUARTERS OF MUTINOUS BORDE RIEFING UNITED NATIONS: IRANIAN REBUKES U.S. COUNTERPART: A PASSING REMARK FROM THE NEW AMERICAN AMERICAN AMERICAN TO THE UNITED NATIONS. SUSAN RICE, PROMPTED A REBUKE FROM HE HEADQUARTERS OF MUTINDUS BORDER GUARDS HERE FOUND A MASS GRAVE ON FRIDAY CONTAINING AROUND 30 EDDIES. AN OFFICIAL SAID. 2009.2.27 WORLD BRIEFING. EUROPE | THE WI GRAVE IN POLAND HAS REVEALED THAT AN UNDERSTANDING OF CIVILIAN SUFFERING IN FORMER SERMAN TERRITORIES IS STARTING... 2009. Z. 27 WORLD BRIEFING ASIA: SKI LANKA: EDITOR ACCU A MASS GRAVE ON FRIDAY CONTAINING AROUND 30 BODIES. AN OFFICIAL SAID. 2009.2.27 CHINA FAILS TO HALT SALE OF LODTED RELICS AT PARIS AUCTION! TWO BRONZE HEADS ORIGINALLY LOD ALYSTS SAY ETHNIC DIVISIONS ARE ESCALATING INTO A CRISIS THAT COULD PUT THE DAYTON ACCORDS OF 1995. WHICH EXDED A SAVAGE WAR THAT KILLED MORE THAN 1... 2000. RS CONTAIN NEW AUSTRALIAN BUSHFIRES: FIREFIGHTERS CONTAINED BIGHT NEW BUSHFIRES IN AUSTRALIA 2009. 2.27 U.S., PAKISTAN AND AFGHARISTAN TO HOLD REGULAR TALKS! THE PLAN WA DUNCED AFTER THREE DAYS OF MEETINGS, WHICH TOUCHED ON SENSITIVE ISSUES LIKE AMERICAN AIRSTRIKES IN PAKISTAN. AND THE SCOPE OF THE AMER... 2009, 2.27 DEBT TESTS CANADIAN ME HISSIDNS AFTER FIERCE PROTESTS AND A FAILED LEGAL CHALLENG... 2009, 2.27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT THE APOLOGY BY A BISHOP WHO HAS DENIED THE SC ESS TO PHOTOGRAPH THE FLAG-DRAPED COFFINS OF AMERICA 2009, 2.27 U.S. HELPS PALESTINIANS BUILD FORCE FOR SECURITY: WITH AMERICAN HELP. GUARDSMEN IN THE WEST BANK ARE TRAIN IANCIAL CRISIS AND FALLING DIL PRICES WILL MAKE IT HARDER FOR IRAO TO PAY FOR SERVICES AND COULD AFFECT U.S. PLANS FOR WITHDRAWAL. 2009, 2. 27 MORLO BRIGGING ACING BANKRUPTCY. ZDD9.2.27 CHINA SAYS U.S. DISTORTS FACTS IN REPORT ON RIGHTS! THE STATE DEPARTMENT SEES ZDD9.2.27 PRO SHARE DEMONSTRATIONS SERBAD ACROSS PURJABL T. NEWSPAPER DURING A FUNERAL IN COLOMBO. THE CAPITAL. ACCUSING HIM OF AIDING A REBEL AIR ATTACK THERE... ZDD9.2.27 IRAQ HANDS DEATH PENALTY TO ZD CULTISTS FOR ATTACKS! A MES I MULUZI WAS ARRESTED AND CHARGED WITH SIPHONING MORE THAN \$11 MILLION OF INTERNATIONAL DONOR MONEY INTO HIS PERSONAL BANK ACCOU... 2009.2.27 PALESTINIAN RIVALS ANNOUNCE
A CIVILIAN TRIAL. THE CHARGES WOULD MOVE THE CASE OF THE ONLY ENEMY COMBATANT TO BE HELD ON U.S. SOIL. ALI SALEH KAHLAH AL-MARRI. INTO A CIVILIAN CRIMINAL COURT. 2009.2.27
S. DUTCH OFFICIALS SAID. 2009.2.27 MASS GRAVE FOUND IN BANGLAGESH! POLICE COMBING THROUGH THE HEADQUARTERS OF MUTINOUS BORDER GUARDS HERE FOUND A MASS GRAVE ON FRIDAY. COPE OF THE HOLDCAUST WAS NOT SUFFICIENT. Z009. Z. Z7 IN SOUTHEAST ASIA. THE UNEMPLOYED RETURN HOME: AS A MEETING OF THE ASSOCIATION OF SOUTHEAST ASIAN NATIONS BEGINS. " NITY CENTER IN CARACAS, BUT NORDDY WAS HURT IN THE BLAST. 2009 2 27 DEST TESTS CANADIAN MEDIA COMPANY: CANNEST GLOBAL COMMUNICATIONS MAY SOON BE NEARING DEFAULT ON I RT. A COLDMBIAN POLITICIAN, IS DEPICTED AS SELFISH AND HAUGHTY IN A MEMOIR BY FELLOW HOSTAGES HELD WITH HER. 2009. 2.27 VATICAN SAYS BISHOP FELL SHOP IF MODERN HUMANS, 2009 2 27 IRAO HANDS DEATH PENALTY TO 20 CULTISTS FOR ATTACKS: A MESSIANIC SHITE FRINGE GROUP HAS TAKEN AIM AT SHITE PILGRIMS AND FOUGHT AMERICAN AND IF 39.2.27 BISHOP OFFERS APOLOGY FOR HOLOCAUST REMARKS: BISHOP RICHARD WILLIAMSON, WHOSE RECENT REHABILITATION BY POPE BENEDICT 2 27 FIREFIGHTERS CONTAIN NEW AUSTRALIAN EUSHFIRES I FIREFIGHTERS CONTAINED EIGHT NEW BUSHFIRES IN AUSTRALIA 2005.2.27 CHINA FAILS TO HALT SALE OF LODTED RELICS AT PARIS AU SU. ZODG Z Z7 U.S. PAKISTAN AND AFGHANISTAN TO HOLD REGULAR TALKS: THE PLAN WAS ANNOUNCED AFTER THREE DAYS OF MEETINGS. WHICH TOUCHED ON SENSITIVE ISSUES LIKE AMERICAL IDNS RISE IN FRAGILE BOSNIA AS COUNTRY: ANALYSTS SAY ETHNIC DIVISIONS ARE ESCALATING INTO A CRISIS THAT COULD PUT THE DAYTON ACCORDS OF 1995, WHICH ENDED A SAVAGE WAR THAT DISMEN IN THE WEST BANK ARE TRAINING TO ENFORCE LAW AND ORDER. 2008, 2. 27 VATICAN SAYS BISHOP FELL SHORT: THE VATICAN SAID THAT THE APOLOGY BY A BISHOP WHO HAS DENIED THE HER, ZODBIZIZY WORLD BRIEFING AFRICA: MALAWIT FORMER PRESIDENT IS ARRESTED. FORMER PRESIDENT BAKKLI MULUZI WAS ARRESTED AND CHARGED WITH SIPHONING MORE THAN \$11 MILLION MILAN MILLITINOVIC. WAS ACQUITTED. 2009.2.27 IRAD WITHORAWAL PLAN GAINS S. D.P. SUPPORT: PRESIDENT DEAMA IS TO ANNOUNCE THAT HE WOULD PULL COMEAT FORCES OUT BY AUGUST 20 IS DEPICTED AS SELFISH AND HAUGHTY IN A MEMOIR BY FELLOW HOSTAGES HELD WITH HER. 2008.2.27 MALBORK JOURNAL: FACING GERMAN SUFFERING, AND NOT LOCKING AWAY: THE DISCOVER DS: VICTIMS: THE NINE PEOPLE WHO DIED WHEN A TURKISH AIRLINES JET CRASH-LANDED ON WEDNESDAY WERE FOUR AMERICANS AND FIVE TURKS, DUTCH OFFICIALS SAID. 2008.2.27 PRO-SHARII RI. INTO A CIVILIAN CRIMINAL COURT. 2009. 2.27 DEBT TESTS CANADIAN MEDIA COMPANY: CANWEST GLEBAL COMMUNICATIONS MAY SOON BE NEARING DEFAULT ON ITS CRUSHING DEET LOAD AND P ERN FOOT IN PREHUMANS: FOSSIL FOOTPRINTS SHOW THAT AS EARLY AS 1.5 MILLION YEARS AGO AN ANCESTRAL SPECIES HAD ALREADY EVOLUED THE FEET AND WALKING GAIT OF MODERN HUMANS THE FORMER SERE PRESIDENT, MILAN MILUTINOVIC, WAS ACQUITTED. 2009.2.27 PRINTS SHOW A MEDERN FOOT IN PREHUMANS: FOSSIL FOOTPRINTS SHOW THAT AS CARLY AS 1.5 MILLION VEARS. TO A CIVILIAN CRIMINAL COURT, 2009.2.27 MASS GRAVE FOUND IN BANSLADESH: POLICE COMBINS THROUGH THE HEADQUARTERS OF MUTICOUS BORDER SURROS HERE FOUND A MASS GRAVE DU FR .. 2008.2.27 DEBT TESTS CANADIAN MEDIA COMPANY: CANWEST GLOBAL COMMUNICATIONS MAY SOON BE NEARING DEFAULT ON ITS CRUSHING DEBT LOAD AND POSSIELY FACING BANKRUPTCY. 201





28 a 31 de Agosto/2023 BRASÍLIA/ BRASIL

Prevenir



Conscientização de usuários

Segurança de rede e de dispositivos

Estratégia de resiliência cibernética



BRASÍLIA / BRASIL



Prevenir – Conscientização de Usuários



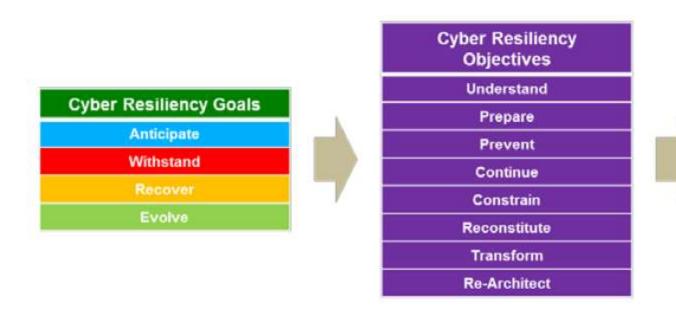
28 a 31 de Agosto/2023 BRASÍLIA/ BRASIL

Prevenir – Segurança de Rede e de Dispositivos





BRASÍLIA/



Cyber Resiliency **Techniques** Adaptive Response **Analytic Monitoring Coordinated Defense** Deception Diversity **Dynamic Positioning Dynamic Representation** Non-Persistence **Privilege Restriction** Realignment Redundancy Segmentation **Substantiated Integrity** Unpredictability

Figure 2. Cyber Resiliency Engineering Framework





Investigar



Executar ferramentas de triagem

Executar análise de causa raiz

Seguir o dinheiro



Investigar – Ferramentas de Triagem e *Hunting*













Investigar – Ferramentas de Triagem e *Hunting*













Investigar – Causa Raiz



sepinf-inc/IPED

IPED Digital Forensic Tool. It is an open source software that can be used to process and analyze digital evidence,...

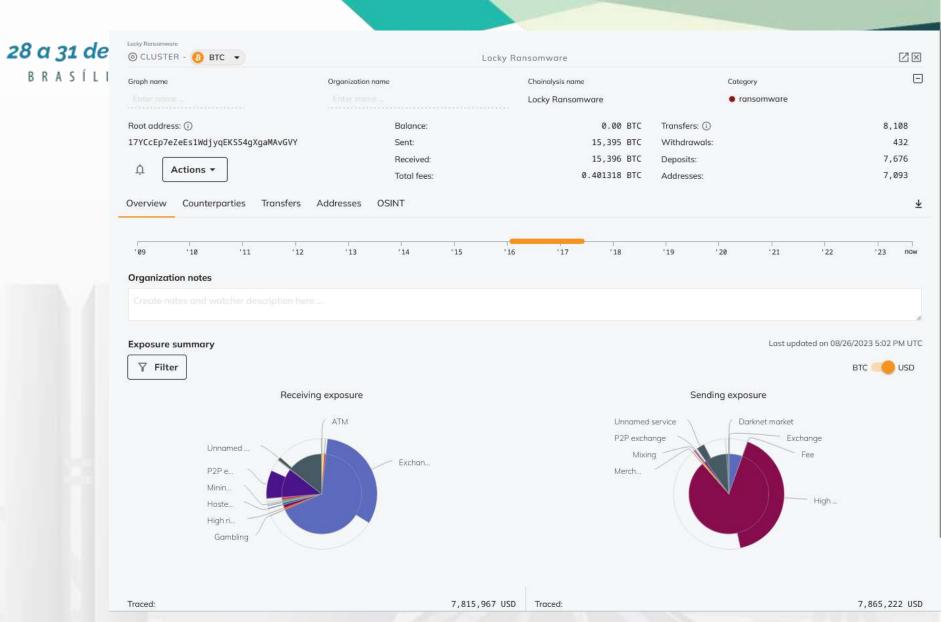








Investigar Siga o Dinheiro





28 a 31 de Agosto / 2023 B R A S Í L I A / B R A S I L

Restaurar



Empregar planos de recuperação de curto e longo prazos

Usar ferramentas antivírus e antimalware

Prevenir ataques futuros



BRASÍLIA / BRASIL

Restaurar – Planos de Recuperação





BRASÍLIA / BRASIL

Restaurar – Ferramentas





Restaurar – Prevenir Ataques Futuros

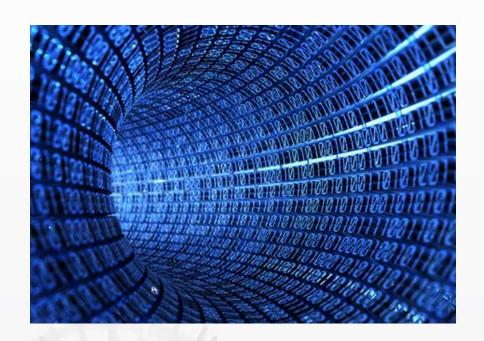




28 a 31 de Agosto/2023 BRASÍLIA/ BRASIL

Referências

- Mitre ATT&CK: https://attack.mitre.org
- IPED: https://github.com/sepinf-inc/IPED
- CERT.br: https://cartilha.cert.br/ransomware/
- Ransomware Database: https://www.ransom-db.com
- Velociraptor: https://github.com/Velocidex/velociraptor
- SANS Digital Forensics: https://digital-forensics.sans.org
- Stop Ransomware: https://www.cisa.gov/stopransomware
- Eric Zimmerman's Tools (Kape): https://ericzimmerman.github.io
- Mitre Cyber Resiliency: https://www.mitre.org/sites/default/files/publications/13-4047.pdf
- NIST Tips & Tactics Ransomware: https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST Ransomware Tips and Tactics Infographic.pdf





"O ransomware é um grande negócio, possibilitado por redes inseguras que permitem aos criminosos obter acesso às redes, em primeiro lugar, e por criptomoedas que permitem pagamentos que os governos não podem interditar. O ransomware tornou-se o modelo de negócio do crime cibernético mais lucrativo e, até resolvermos esses dois problemas, isso não vai mudar."

Bruce Schneier, maio de 2021

Contato

https://www.linkedin.com/in/caiado

http://dfir.com.br/about

WWW.INTERFORENSICS.COM













@InterForensics



