Draft Computer Security Incident Handling Guide

LUCIANO KOLE

Computer Incident Response and Forensics Team Management "O'Reilly Media, Inc."
How did the Computer security incident management manager receive input to the development of a Computer security incident management improvement plan and the estimated completion dates/times of each activity? Does Computer security incident management appropriately measure and monitor risk? When was the Computer security incident management start date? How do we make it meaningful in connecting Computer security incident management with what users do day-to-day? How frequently do you track Computer security incident management measures? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Computer security incident management investments work better. This Computer security incident management All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Computer security incident management Self-Assessment. Featuring 693 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Computer security incident management improvements can be made. In using the questions you will be better able to: - diagnose Computer security incident management projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Computer security incident management and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Computer security incident management Scorecard, you will develop a clear picture of which Computer security incident management areas need attention. Your purchase includes access details to the Computer security incident management self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. Your exclusive instant access details can be found in your book.
Computer Security Incident Response Planning at Nuclear Facilities Packt Publishing Ltd
You will be breached—the only question is whether you'll be ready A cyber breach could cost your organization millions of dollars—in 2019, the average cost of a cyber breach for companies was $3.9M, a figure that is increasing 20-30% annually. But effective planning can lessen the impact and duration of an inevitable cyberattack. Cyber Breach Response That Actually Works provides a business-focused methodology that will allow you to address the aftermath of a cyber breach and reduce its impact to your enterprise. This book goes beyond step-by-step instructions for technical staff, focusing on big-picture planning and strategy that makes the most business impact. Inside, you’ll learn what drives cyber incident response and

how to build effective incident response capabilities. Expert author Andrew Gorecki delivers a vendor-agnostic approach based on his experience with Fortune 500 organizations. Understand the evolving threat landscape and learn how to address tactical and strategic challenges to build a comprehensive and cohesive cyber breach response program Discover how incident response fits within your overall information security program, including a look at risk management Build a capable incident response team and create an actionable incident response plan to prepare for cyberattacks and minimize their impact to your organization Effectively investigate small and large-scale incidents and recover faster by leveraging proven industry practices Navigate legal issues impacting incident response, including laws and regulations, criminal cases and civil litigation, and types of evidence and their admissibility in court In addition to its valuable breadth of discussion on incident response from a business strategy perspective, Cyber Breach Response That Actually Works offers information on key technology considerations to aid you in building an effective capability and accelerating investigations to ensure your organization can continue business operations during significant cyber events.

NIST Special Publication 800-61 Revision 1 Computer Security Incident Handling Guide Createspace Independent Publishing Platform

This book comes with access to a customizable word template that can be used in implementing an IT Security Incident Response Program in any organization. Most companies have requirements to document their incident response processes, but they lack the knowledge and experience to undertake such documentation efforts. That means businesses are faced to either outsource the work to expensive consultants or they ignore the requirement and hope they do not get in trouble for being non-compliant with a compliance requirement. In either situation, it is not a good place to be. The good news is that your CyberSecurityResource developed a viable incident response program, which is the "gold standard" for incident response programs. This document is capable of scaling for any sized company.The reality is that incidents do not care if your responders are or are not prepared and generally with incident response operations if you fail to plan you plan to fail. What matters most is appropriate leadership that is capable of directing response operations in an efficient and effective manner. This is where the Incident Response Program (IRP) is an invaluable resource for cybersecurity and business leaders to have a viable plan to respond to cybersecurity related incidents.The IRP is an editable Microsoft Word document, that contains the program-level documentation and process flows to establish a mature Incident Response Program. This product addresses the "how?" questions for how your company manages cybersecurity incident response. The IRP helps address the fundamental expectations when it comes to incident response requirements: Defines the hierarchical approach to handling incidents.Categorizes eleven different types of incidents and four different classifications of incident severity.Defines the phases of incident response operations, including deliverables expected for each phase.Defines the Incident Response Team (IRT) to enable a unified approach to incident response operations.Defines the scientific method approach to incident response operations.Provides guidance on forensics evidence acquisition

Security Planning and Disaster Recovery 5starcooks

Abstract: "This document provides guidance on forming and operating a computer security incident response team (CSIRT). In particular, it helps an organization to define and document the nature and scope of a computer security incident handling service, which is the core service of a CSIRT. The document explains the functions that make up the service; how those functions interrelate; and the tools, procedures, and roles necessary to implement the service. This document also describes how CSIRTs interact with other organizations and how to handle sensitive information. In addition, operational and technical issues are covered, such as equipment, security, and staffing considerations. This document is intended to provide a valuable resource to both newly forming teams and coexisting teams whose services, policies, and procedures are not clearly defined or documented. The primary audience for this document is managers who are responsible for the creation or operation of a CSIRT or an incident handling service. It can also be used as a reference for all CSIRT staff, higher level managers, and others who interact with a CSIRT."

Handbook for Computer Security Incident Response Teams (CSIRTs). CreateSpace

Proactively implement a successful security and disaster recovery plan--before a security breach occurs. Including hands-on security checklists, design maps, and sample plans, this expert resource is crucial for keeping your network safe from any outside intrusions.

Cyber Breach Response That Actually Works Jones & Bartlett Learning

Computer security incident response has become an important component of information technology (IT) programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. Topics covered include organizing a computer security incident response capability, handling incidents from initial preparation through the post-incident lessons learned phase, and handling specific types of incidents.

Sans Inst

How companies can maintain computer security is the topic of this book, which shows how to create a Computer Security Incident Response Team, generally called a CSIRT.

Cybersecurity Incident Response Sams

Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

Establishing a computer security incident response capability Apress

This book will help IT and business operations managers who have been tasked with addressing security issues. It provides a solid understanding of security incident response and detailed guidance in the setting up and running of specialist incident management teams. Having an incident response plan is required for compliance with government regulations, industry standards such as PCI DSS, and certifications such as ISO 27001. This book will help organizations meet those compliance requirements.

Incident Handling and Response Createspace Independent Publishing Platform

The Department of Defense (DOD) depends on interconnected information systems and communications networks for critical combat and business operations. Many of these systems and networks are interconnected through the public telecommunications infrastructure, including the Internet, and they may be targeted by an increasing variety of cyber attacks. If successful, these attacks could result in the loss or corruption of critical data, damage to information systems, or disruption of military operations. To address such threats, DOD has established organizations, known as computer incident response capabilities, at various locations worldwide. These organizations engage in a range of activities associated with preventing, detecting, and responding to computer incidents.

Computer Forensics IOS Press

NIST SP 800-61 R 2 Aug 2012 Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. Why buy a book you can download for free? We print this so you don't have to. First you gotta find it and make sure it's the latest version, not always easy. Then you gotta print it using a network printer you share with 100 other people - and its outta paper - and the toner is low (take out the toner cartridge, shake it, then put it back). If it's just 10 pages, no problem, but if it's a 250-page book, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. An engineer that's paid $75 an hour has to do this himself (who has assistant's anymore?). If you are paid more than $10 an hour and use an ink jet printer, buying this book will save you money. It's much more cost-effective to just order the latest version from Amazon.com This material is published by 4th Watch Books. We publish tightly-bound, full-size books at 8 ½ by 11 inches, with glossy covers. 4th Watch Books is a Service Disabled Veteran Owned Small Business (SDVOSB) and is not affiliated with the National Institute of Standards and Technology. A full copy of all the pertinent cybersecurity standards is available on DVD-ROM in the CyberSecurity Standards Library disc which is available at Amazon.com. If you like the service we provide, please leave positive review on Amazon.com. Without positive feedback from the community, we will discontinue the service and y'all can go back to printing these books manually yourselves.

Computer Security Incident Handling Guide DIANE Publishing

As security professionals, our job is to reduce the level of risk to our organization from cyber security threats. However Incident prevention is never 100% achievable. So, the best option is to have a proper and efficient security Incident Management established in the organizationThis book provides a holistic approach for an efficient IT security Incident Management. Key topics includes,1) Attack vectors and counter measures 2) Detailed Security Incident handling framework explained in six phases._Preparation_Identification_Containment_Eradication_Recovery_Lessons Learned/Follow-up3) Building an Incident response plan and key elements for an efficient incident response.4) Building Play books.5) How to classify and prioritize incidents.6) Proactive Incident management.7) How to conduct a table-top exercise.8) How to write an RCA report /Incident Report.9) Briefly explained the future of Incident management. Also includes sample templates on playbook, table-top exercise, Incident Report, Guidebook.

Digital Forensics and Incident Response McGraw Hill Professional

Abstract: "When a computer security attack on an organization occurs, an intrusion is recognized, or some other kind of computer security incident occurs, it is critical for the organization to have a fast and effective means of responding. One method of addressing this need is to establish a formal incident response capability or a Computer Security Incident Response Team (CSIRT). When an incident occurs, the goal of the CSIRT is to control and minimize any damage, preserve evidence, provide quick and efficient recovery, prevent similar future events, and gain insight into threats against the organization. This handbook describes different organizational models for implementing incident handling capabilities, including each model's advantages and disadvantages and the kinds of incident management services that best fit with it. An earlier SEI publication, the Handbook for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-2003-HB-002), provided the baselines for establishing incident response capabilities. This new handbook builds on that coverage by enabling organizations to compare and evaluate CSIRT models. Based on this review they can then identify a model for implementation that addresses their needs and requirements."

Incident Response & Computer Forensics, 2nd Ed. Auerbach Pub

Computer Incident Response and Forensics Team Management provides security professionals with a complete handbook of computer incident response from the perspective of forensics team management. This unique approach teaches readers the concepts and principles they need to conduct a successful incident response investigation, ensuring that proven policies and procedures are established and followed by all team members. Leighton R. Johnson III describes the processes within an incident response event and shows the crucial importance of skillful forensics team management, including when and where the transition to forensics investigation should occur during an incident response event. The book also provides discussions of key incident response components. Provides readers with a complete handbook on computer incident response from the perspective of forensics team management Identify the key steps to completing a successful computer incident response investigation Defines the qualities necessary to become a successful forensics investigation team member, as well as the interpersonal relationship skills necessary for successful incident response and forensics investigation teams

Computer Security Incident Handling Guide Packt Publishing Ltd

This guide teaches security analysts to minimize information loss and system disruption using effective system monitoring and detection measures. The information here spans all phases of incident response, from pre-incident conditions and considerations to post-incident analysis. This book will deliver immediate solutions to a growing audience eager to secure its networks.

CIO's Guide to Security Incident Management McGraw Hill Professional

Successfully responding to modern cybersecurity threats requires a well-planned, organized, and tested incident management program based on a formal incident management framework. It must be comprised of technical and non-technical requirements and planning for all aspects of people,

process, and technology. This includes evolving considerations specific to the customer environment, threat landscape, regulatory requirements, and security controls. Only through a highly adaptive, iterative, informed, and continuously evolving full-lifecycle incident management program can responders and the companies they support be successful in combatting cyber threats. This book is the first in a series of volumes that explains in detail the full-lifecycle cybersecurity incident management program. It has been developed over two decades of security and response experience and honed across thousands of customer environments, incidents, and program development projects. It accommodates all regulatory and security requirements and is effective against all known and newly evolving cyber threats.

Organizational Models for Computer Security Incident Response Teams (CSIRTs) Pearson Education

Any good attacker will tell you that expensive security monitoring and prevention tools aren't enough to keep you secure. This practical book demonstrates a data-centric approach to distilling complex security monitoring, incident response, and threat analysis ideas into their most basic elements. You'll learn how to develop your own threat intelligence and incident detection strategy, rather than depend on security tools alone. Written by members of Cisco's Computer Security Incident Response Team, this book shows IT and information security professionals how to create an InfoSec playbook by developing strategy, technique, and architecture. Learn incident response fundamentals—and the importance of getting back to basics Understand threats you face and what you should be protecting Collect, mine, organize, and analyze as many relevant data sources as possible Build your own playbook of repeatable methods for security monitoring and response Learn how to put your plan into action and keep it running smoothly Select the right monitoring and detection tools for your environment Develop queries to help you sort through data and create valuable reports Know what actions to take during the incident response phase

Computer Security Incident Handling Guide John Wiley & Sons

Covers, Security Incident Handling FrameworkTypes of threats and it's countermeasuresBuilding an effective security incident handling policy and teamPrepare a Security Incident ReportThis book has four major sections, The first section gives an introduction on Security incident Handling and response frameworks. Also give a glimpse on Security forensics and Risk Management concepts. The second section explains different kinds of security threats and attacks that can result in potential security incident. Being familiarize with the attacks are very important for identifying and categorizing a security incident. The third section mentions the security controls and countermeasures to detect, prevent or/and to mitigate a threat. This includes the detection mechanisms, defense in depth, vulnerability management etc. The strategy and plan for building an efficient Security Incident Handing is comprehensively explained in the final section. The six phases of a security incident handling and response are explained step by step.

Incident Response with Threat Intelligence CRC Press

Hacker Techniques, Tools, and Incident Handling, Third Edition begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web. Written by subject matter experts, with numerous real-world examples, Hacker Techniques, Tools, and Incident Handling, Third Edition provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

Computer Incident Response and Product Security Packt Publishing Ltd

The number of cyber incidents reported by federal agencies increased in FY 2013 significantly over the prior 3 years. An effective response to a cyber incident is essential to minimize any damage that might be caused. The Department of Homeland Security (DHS) and the U.S. Computer Emergency Readiness Team (US-CERT) have a role in helping agencies detect, report, and respond to cyber incidents. This report reviewed the extent to which (1) federal agencies are effectively responding to cyber incidents and (2) DHS is providing cybersecurity incident assistance to agencies. The report found that 24 major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information). Tables and figures. This is a print on demand report.