UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

Revisiting RFC2350 20 Years Later: A Hands-On Approach to Security Monitoring and Incident Response

Versão Pública

Diogo Bonfim Ribeiro Carou Cunha

Mestrado em Segurança Informática

Trabalho de Projeto orientado pelo
Professor Doutor Pedro Miguel Frazão Fernandes Ferreira
e pelo Mestre Artur Miguel Adriano Martins

2018

Resumo

Hoje em dia, o uso de diferentes tipos de informação encontra-se fundamentalmente associado aos principais processos de negócios de uma organização. Estes processos podem ser de vários tipos como por exemplo, a execução de diferentes aplicações, execução de comandos personalizados num computador remoto ou a instalação de complexas aplicações. Qualquer tipo de perturbação do correto comportamento destes processos pode resultar em perdas substanciais e de todo indesejadas para uma organização, sendo por isso que estas têm vindo a investir cada vez mais na segurança da sua informação.

Este tópico pode ser definido como a preservação da confidencialidade, integridade e disponibilidade da informação, sendo o seu principal objetivo, além de proteger essa informação de qualquer pessoa com intenções maliciosas, o de garantir que todos os incidentes de segurança que afetaram uma determinada organização no passado não voltem a acontecer no presente ou no futuro. Mais ainda, se por algum motivo estes acontecerem de novo, pelo menos devem ter um impacto muito menor na infraestrutura do que no passado. Estas premissas são normalmente atingidas através da implementação e monitorização de diversificados controlos de segurança, de uma forma geral posicionados em locais estratégicos da infraestrutura da organização, por forma a dar á equipa de segurança uma visão global daquilo que está a acontecer na infraestrutura a qualquer momento.

É comum quando se fala num Centro de Operações de Segurança (*SOC*), de se imaginar uma sala espaçosa e de última geração, composta por equipamentos topo de gama e repleta de engenheiros especializados, apesar de isso não constituir, naturalmente, um requisito. Um *SOC* é basicamente definido por aquilo que faz, podendo fornecer uma variedade de serviços a um vasto conjunto de clientes, desde a deteção e resposta a incidentes de segurança, a ações de sensibilização por forma a alertar para alguns dos riscos a que os utilizadores podem estar expostos diariamente, a identificação, quantificação e priorização de vulnerabilidades, entre outros.

No âmbito deste trabalho, e primeiro que tudo, foram identificados diversos problemas/desafios que existem atualmente no mundo da segurança da informação e que emergiram durante a fase de pesquisa e investigação que foi levada a cabo. Seguidamente, são apresentados e discutidos os pontos teóricos principais que devem servir de base á construção e posterior manutenção de um qualquer Centro de Operações de Segurança (*SOC*). Começando pela constituição da equipa responsável por levar a cabo as operações, são apresentados dois possíveis modelos de divisão de responsabilidades. De seguida, são enumeradas as diferentes fases de maturidade de um *SOC*, passando posteriormente pelos conceitos de *Logging*, onde são discutidos os conceitos de Logging proactivo e reativo,

Eventos, Alertas - sendo explicadas as 4 categorias de alertas com que a equipa de segurança irá ter de lidar, *SIEMs e Log Management* – onde é explicado no que consistem estas duas tecnologias e quais os seus propósitos, sendo depois feita uma comparação entre si. Seguidamente, é abordado o tema de resposta a incidentes de segurança, passando pela sua definição e respetivo ciclo de vida. Neste, são enumeradas e respetivamente explicadas todas as fases que o constituem, dando ênfase ás tarefas que o respetivo analista de segurança deve levar a cabo em cada delas.

Outro ponto central deste trabalho, é a revisão do *RFC2350*. Este documento especifica as boas práticas da comunidade, sendo o seu principal objetivo o de expressar as expectativas gerais da comunidade acerca das *equipas de resposta a incidentes de segurança* (*CSIRT's*). Uma vez que não é possível delinear um conjunto de requisitos que se possam aplicar a todas as equipas de segurança, é fornecida uma descrição de alguns tópicos e questões centrais, por forma a fornecer algum tipo de orientação. Todas as partes integrantes da *CSIRT* precisam e têm o direito de conhecer e compreender por completo todas as políticas e procedimentos que esta possui. Por forma a conseguir fazê-lo, a *CSIRT* deve fornecer um modelo de formulário formal e detalhado que contenha toda essa informação, e que possa ser consultado por toda a sua comunidade de clientes.

Por fim, e ainda naquilo que diz respeito aos pontos teóricos, são apresentados dois documentos de duas entidades de referência (*SANS e MITRE*), ambos relacionados com a construção e manutenção de Centros de Operações de Segurança.

Finda a parte teórica, é então apresentada a contribuição deste trabalho, sendo esta constituída por um detalhado e completo guia que tem como principal propósito demonstrar como montar de forma correta e eficiente um Centro de Operações de Segurança, sendo primeiro enumeradas as diferentes tecnologias consideradas essenciais para o seu correto funcionamento *(SIEM, Log Management, Ticketing e CSIRT*), assim como onde estas e a *CSIRT* devem ser posicionadas dentro da infraestrutura da organização. Posto isto, são devidamente explicadas as diversas fases que constituem o seu processo de construção (Identificação de data sources, normalização de logs, identificação de eventos relevantes e implementação). De seguida, e após o centro estar montado e funcional, são enumeradas e debatidas diferentes formas de realizar uma cuidada e atenta monitorização da infraestrutura, através da definição de alarmes, da construção de dashboards e da aplicação de técnicas de *threat intelligence*.

Por fim, é abordado o tema de resposta a incidentes de segurança, sendo fornecido e devidamente explicado um *workflow* genérico de resposta a incidentes, o qual claramente explicita as diferentes interações que devem existir entre os diferentes membros da *CSIRT*, para cada uma das fases previamente identificadas aquando da definição do ciclo de vida de um incidente. São ainda enumeradas as diferentes categorias de incidente comumente utilizadas pela comunidade, assim como é apresentada e propriamente explicada uma plataforma de ticketing especialmente desenhada para o contexto de resposta a incidentes de segurança (*Request Tracker for Incident Response - RTIR),* sendo ainda explicado, de uma forma geral, a forma como esta funciona, sendo ainda fornecidos alguns screenshots da mesma.

Após a apresentação da solução, a mesma foi colocada em prática através da aplicação dos conceitos aqui apresentados a um caso de estudo para a construção de um Centro de Operações de Segurança para uma grande empresa nacional, por forma a produzir evidências práticas que permitissem demonstrar a eficiência da solução proposta. Após a

sua montagem, foram então levadas a cabo diversas tarefas de monitorização, nomeadamente a especificação de diferentes alarmes e a definição e criação de diferentes dashboards que permitissem á equipa de segurança conseguir visualizar aquilo que se encontra a acontecer na infraestrutura da empresa a qualquer momento.

Por fim, é abordado o conceito de resposta a incidentes de segurança, sendo apresentada e acompanhada de forma minuciosa a resposta a um incidente de segurança (Injeção de *Cross-Site-Scripting - XSS*), sendo evidenciadas todas as interações que o analista de segurança deve ter com a plataforma de ticketing aquando da passagem pelas diversas fases do ciclo de vida do incidente.

Em jeito de conclusão, é referido de que forma é que este trabalho vem resolver os problemas/ desafios que haviam sido identificados durante a fase de pesquisa e investigação, sendo inclusive especificada a parte da solução que vem resolver cada um dos diferentes pontos. Após algumas considerações finais, é levado a cabo um apanhado geral de todo o trabalho que foi desenvolvido, sendo posteriormente apresentadas algumas sugestões daquilo que poderá advir como trabalho futuro relativamente a este tema.

Palavras-chave: Centro, Operações, Segurança, RFC2350, Dados, Cibersegurança.

Abstract

Nowadays, with the amount of information being produced and exchanged at any given moment, data security has become a central discussion topic, with companies spending more money than ever trying to protect their own resources. Also, with the rise of Cyber Criminality, new ways of infiltrating or simply disturbing businesses through their Information Technology (IT) systems (for example, by exhausting their resources) are discovered almost on a daily basis. This requires a sophisticated defense strategy from these companies, which is based on the aggregation of several dedicated operational security functions into a single security department - a Security Operation Center (SOC). A SOC's main goal is to detect, analyze, respond to, report on and prevent any sort of security incident. In order to do that, they need not only to be properly assembled and configured, but they need to have a vast array of sophisticated detection and prevention technologies, a virtual sea of Cyber Intelligence reporting information and immediate access to a set of talented IT professionals ready to mitigate any incoming security incident.

In order to achieve this, this work will first identify the different problems/challenges that were identified during the research phase, and then give a detailed background on some of the major theoretical concepts behind SOCs as well as revisit the RFC2350's main concepts, which is the standard for Computer Security Incident Response Teams (CSIRTs), it will also provide a detailed guide on how to properly assemble and maintain a Security Operations Center, and then show how to perform a variety of security monitoring and incident response tasks.

After this, the proposed solution will be put into practice and will be used to build a brand new SOC for a major Portuguese company. Once the assembling process has finished, some security monitoring tasks will then be performed (definition of different alarms and creation of several dashboards). Then, the incident response lifecycle will be meticulously reviewed, in a response to a real security incident (*Cross-Site-Scripting - XSS* Injection). A special emphasis will be put in the different interactions the security analyst should engage with the ticketing platform in use.

Lastly, some considerations on how this work solves the problems/ issues that were previously identified is given, and some considerations on possible future work are provided.

Keywords: Security, Operation, Center, Data, RFC2350, Cybersecurity

Acknowledgments

First of all, I would to thank my family for giving me the opportunity to get where I am now and for supporting me in my life, especially in the times where I most needed them.

I would also like to thank my friends, who not only provided me with great moments throughout times, but also helped me to keep focused on what was essential, and greatly contributed for my personal improvement as a person on a daily basis.

Finally, a special thanks to my advisors Prof. Doc. Pedro Miguel Frazão Fernandes Ferreira for his tolerance, patience and guidance in this last year, and Artur Miguel Adriano Martins for always being able to make up the time to meet up, for giving me his valuable advice and for allowing me to work in a company like LAYER8.

To my grandmother Maria do Carmo

Contents

List of Figures

List of Tables

” Research is to see what everybody else has seen, and to think what nobody else has thought.”

- Albert Szent-Gyorgyi

Chapter 1

Introduction

1.1 Context

With the extensive use of information, data security has become a central discussion topic nowadays. In order for an organization to be able to effectively secure their information, it would need to monitor its own resources. However, this monitoring cannot be done for each device distinctly, otherwise the amount of time and men power it would take to achieve this would just be unbearable. The solution is to continuously gather, aggregate and correlate information from various sources into a central machine (or cluster of machines). This, along with a team of information security experts and analysts, a Security Operations Center (SOC), opens the possibility to effectively monitor the organization's assets, in order to prevent security incidents as well as unwanted threats from occurring within the organization's infrastructure.

With an efficiently assembled *SOC*, an organization is not only able to better detect, investigate and respond to incoming security incidents, but it is also better prepared to build awareness regarding information security issues as well as prioritizing the deployment of enterprise resources to address those. However, and most due to the lack of structured procedures and specialized personal by the respective organizations, this does not always happen in practice, and these *SOCs* will eventually fall short on keeping adversaries out of the enterprise.

Bearing this in mind, and with the standard for Computer Security and Incident Response (*RFC2350*) [16] as a literary reference, this work will not only provide a guide on how to carry out efficient security monitoring activities, a well-structured and effective incident response plan and a plan for architecting, assembling and monitoring a *SOC*, but it will also apply all these concepts to a major Portuguese company, in order to demonstrate the advantages of this solution.

1.2 Problem Statement

These days, every *SOC* should have at its disposal all the necessary tools in order to build a competent defense infrastructure for what it aims to protect. Since the floor is so weighted against the defenders, it is of extreme importance that the security team who's responsible for monitoring and protecting these resources really knows what it is doing.

SOCs are becoming more and more common among organizations nowadays, so, in this work, besides providing a guide on how to assemble an efficient Security Operations Center and then perform different security monitoring and incident response activities, some fundamental challenges that most *SOC* teams frequently encounter will be enumerated and then addressed and mitigated within the proposed solution. These were divided into three different categories (People, Processes and Technology) and are listed below:

Technology:

t1. SIEMs are not mature enough to feed the ticketing system.

t2. All relevant events are spread out through the infrastructure and no one knows where the security logs are (these are usually fragmented through the security equipment).

t3. There's no central point to where the logs can be sent.

Processes:

p1. There's no central point to perform detection and investigation tasks in an incident response context.

p2. Incident response is performed in an ad-hoc manner depending on the technology.

p3. The ticketing systems don't reflect a formal and structured incident response plan.

People:

pp1. The SOC is seen as an IT helpdesk.

pp2. The SOC manager doesn't have formal evidence to justify within the administration board the need to invest in information security - Budgeting problem.

pp3. There is no cross-company structure that allows the SOC team to reduce the impact of an incident in a timely manner.

1.3 Thesis outline

This thesis is divided into five main chapters. A summary follows:

- Chapter 2 - Background - In this chapter, relevant existing work as well as theoretical content will be presented, in order to provide a better understanding of the concepts and issues being discussed in this work.
- Chapter 3 - Solution Design - This third chapter is where the actual solution will be presented. First, some guidance on how to build a Security Operations Center will be given, and then some possible ways of performing security monitoring (definition of different Alarms and the creation of several relevant dashboards) and incident response tasks (incident response workflows) will be presented.
- Chapter 4 – Case Study - In this fourth chapter, the previously presented solution will be applied to a major Portuguese company. Then, the obtained results will be discussed.
- Chapter 5 - Conclusion & Future Work - In this chapter, the results from the previous phases are evaluated and conclusions about this work will be presented, and some thoughts on possible future work will be given.

Chapter 2

Background

"If all you have is a hammer, everything looks like a nail."

- Abraham Maslow

In this chapter, theoretical concepts as well as relevant existing work will be presented, in order to not only provide a clear understanding of the subjects being discussed in this work, but also to show what has already been done in this field of study.

First, some detail regarding Security Operations Centers (SOC's) will be given: the main requirements for its proper assembly, the SOC's different phases, some insights on Events and Alerts, log management (which is an essential part of the SOC) and incidents (incident lifecycle and ticketing platforms). Then, the RFC2350 [6] which expresses the general Internet community's expectations for Computer Security Incident Response Teams (CSIRTs) will be revisited and resumed, and, at last, existing approaches from some major companies to Security Operations Centers will be presented.

2.1 Information security

Nowadays, the usage of information is fundamentally associated to an organization's core business processes. These can vary from executing a standard desktop application, to running custom commands on a remote machine, or to deploying web applications on an international scale. The disturbance of the correct behavior and functionality of these processes can then result in substantial and undesired losses for an organization, which is why these tend to lean towards investing in Information Security.

This trendy topic can be defined as the preservation of Confidentiality, Integrity and Availability of information, and its main goal besides protecting this information from anyone with malicious intentions, is to ensure that any security incidents that might have affected a certain organization in the past, do not happen again in the present or the future. More so, if they do happen again, at least they should have a much smaller impact on the infrastructure than before.

This is usually accomplished by the implementation and monitoring of different security controls, which are usually positioned in strategic places of the organization's infrastructure, in order to give the security team a global vision of what's going on at any given time.

2.2 Security operations center

When people picture a Security Operations Center, they usually visualize a state of the art spacious room, with large screens and plenty of specialized engineers. While this can be the case, this is not at all a requirement since a *SOC* is basically defined by what it does. According to [1], [2], [3], [4], [5] and [6] "it is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.".

A *SOC* can provide a variety of services to a set of costumers, from incident detection and response to other related amenities such as security awareness training (sensibilize users for some of the risks they might be exposed to on a daily basis) and vulnerability assessment (identification, quantification and prioritization of existing vulnerabilities). Each SOC costumer is commonly referred to as a constituency, which according to [1], it can be defined as "a restricted circle of users, sites, assets, networks and organizations".

Over the years, many different terms have been used to refer to these teams of cybersecurity experts, and the acronym *CSIRT* (Computer Security Incident Response Team) seems to be not only the most commonly adopted in the industry, but also the one which better defines them. In order for an organization to be considered a *CSIRT*, and thus provide a proper *SOC* service to its constituents, it should provide a way for them to suitably report any alleged cybersecurity incidents, give incident handling support whenever necessary and disseminate any incident-related information to constituents and external parties.

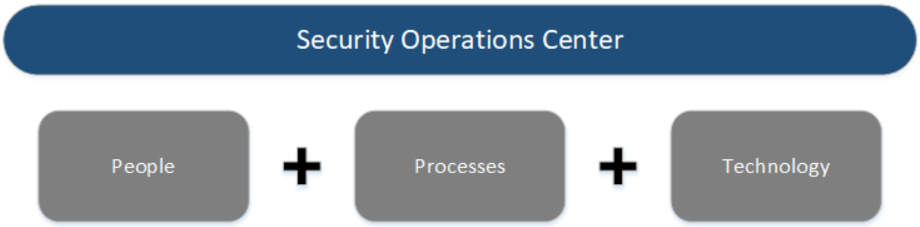


Figure 2.1 SOC requirements

A properly assembled *SOC* provides a complete and accurate visibility of the infrastructure that's being monitored which results in a stronger security posture. The congregation of information security specialists with significant data into a central location allows for faster and more efficient threat detection.

In order to reduce security risks across an organization, a *SOC* leverages people, processes and technology (see figure 2.1) [7]. Greatly trained and certified professionals that are accustomed to work with the most diverse security-based scenarios and can prioritize and manage time efficiently are unquestionably a must have. This is important because new threats and vulnerabilities keep being discovered on almost a daily basis, and people who can learn by themselves/ adjust to new situations and think outside the box can and will certainly make a difference.

Quality *SOCs* require great action standardization to ensure nothing gets omitted or fabricated. The design of different workflows and processes (by adapting the industries standards and best practices to the organization's specific needs) will not only allow the team to know how to respond, set severity and escalate different incidents and threats, but also to work together in a consistent manner, which will significantly reduce errors during emergency situations and thus operation costs and, on the other hand, raise productivity and efficiency [8] and [9].

When it comes to technology, selecting the right tools is essential. In order to do a proper monitoring of its own resources, an organization not only needs at its disposal a different set of tools, but it also requires interoperability between them. A data collection, aggregation, detection, analytic and management solution is the essential technology base for any successful *SOC*. Without these, it wouldn't be possible for it to work properly. An efficient security monitoring system will continuously incorporate data that is being collected from the monitoring of the different sources (for example, systems and networks). With this collection happening before and during security incidents, the team is able to immediately start using the monitoring system as a detection tool instead of an investigative one, go over suspicious incident related activities, and manage response plans and necessary actions to implement.

2.2.1 Team constitution

Depending on the constituency's size (small, medium or large) and business scope, the number of required security experts as well as applicable procedures might vary. For example, a typical midsize *SOC (*10-20 engineers) should prevent cybersecurity incidents trough proactive analysis (for example, by collecting and correlating network logs, performing vulnerability scans or examining security policies). It should also monitor, identify and examine possible attacks in real time or based on past events from important data sources, respond to incidents through resource management and appropriate countermeasure suggestion and provide awareness and report on relevant cybersecurity threats.

Typically, the specialized personal in a *SOC* is divided into two different tiers (see figure 2.2) [5]:

- **Tier 1 - Triage Specialist**, is usually responsible for real-time alert reviewing in order to determine its relevance and urgency (for example, whether it is or not a false positive). If a specific alert gives any indication that a security incident might have occurred, the tier 1 analyst should open a ticket on whatever ticket platform is in use at the SOC and request the tier 2 analysts for further analysis. It can also run vulnerability scans and review vulnerability assessment reports and manage and configure different security monitoring tools (for example, firewalls, switches or routers).
- **Tier 2 - Incident Responder**, is a much more technical and skilled engineer, which is not only responsible for further analyzing tickets which were created by tier 1 analysts but should also be able to deploy incident response and mitigation techniques, perform forensic analysis, proactively investigate new possible ways of harming the infrastructure (for example, trough penetration tests) and give recommendations on how to improve the organization's overall security.

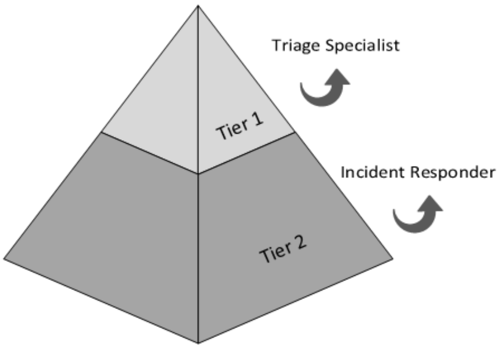


Figure 2.2 SOC 2-tier architecture

In some cases, (for example, large organizations), this responsibility division can be extended into four different tiers (see figure 2.3) [5]:

Tier 1 – Triage Specialist, remains exactly the same as before.

Tier 2 – Incident Responder, is now more focused on reviewing tier 1 tickets and performing incident response and mitigation techniques.

Tier 3 - Threat Hunting, is more directed into vulnerability/ threat finding and providing possible countermeasures for these.

Tier 4 – SOC Manager, this person should have all the previously described technical skills along with strong leadership and communication capabilities. His main duty is to supervise the activity of the *SOC*, to recruit, train and access the staff, to define and manage all used procedures (for example, incident reports or incident response plans), to specify and implement an emergency communication plan and to define different key performance indicators (KPIs) which should reflect the value of security operations to the administration board.

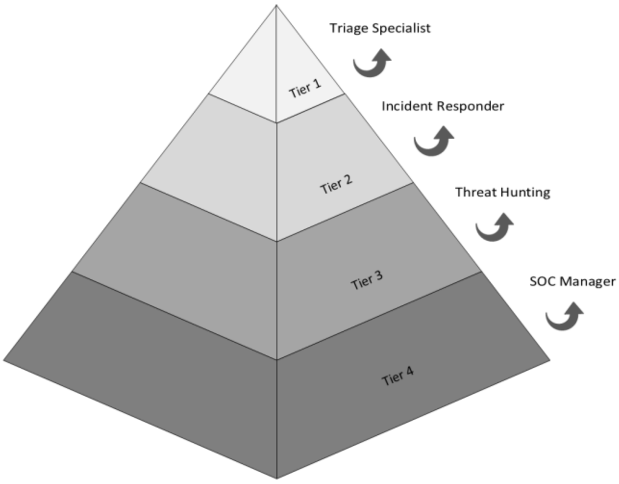


Figure 2.3 SOC 4-tier architecture

2.2.2 Maturity steps

Whether or not an organization is planning on building a small, medium or large *SOC*, in order for it to be able to reach a certain maturity level, where the specialized team can competently do incident prevention, detection and response, it first needs to go through a series of growing and maturing stages. [5] These are Technology, Organization, Policy, Operation and Intelligence, and will be described below (figure 2.4):

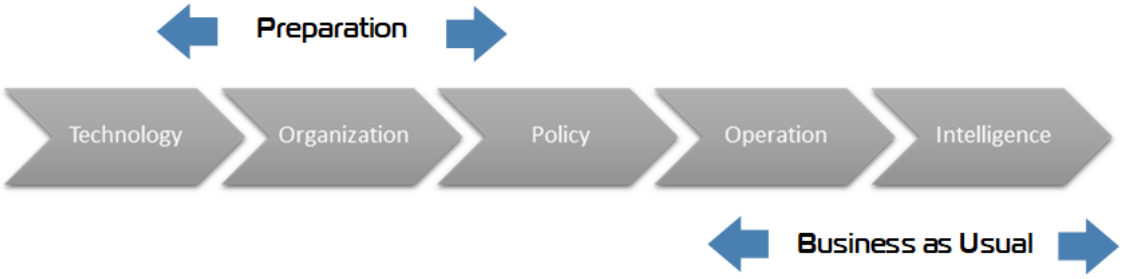


Figure 2.4 SOC Phases

Technology phase

In this first phase, it's all about getting to know the environment. After establishing its area of responsibility, the team should first list all existing equipment, draw a network's high-level design if none is yet available, and come up with a plan for monitoring the different assets. Also, this is where new equipment will start to be installed in order to convene the organization's requirements. However, this is not going to be the only stage where new installations of security technology will happen, but it is where they will begin.

Organization phase

When a SOC reaches this phase, most if not all of the security equipment will by now be under the security team's administration. Then, a health check of all equipment should be carried out, in order to see if they are operating as it would be expected. Also, some staff training might happen here, if any elements of the security team are not familiarized or sufficiently experienced with some of the systems being used.

After that, processes to manage and maintain all systems up to date will begin to be developed. Also, and in case these involve any sort of modifications to the existing systems, they must be properly documented for future reference. It is normal for the security team to experience some issues during this phase, especially when it comes to gaining control over equipment that is typically maintained by a traditional IT department, because these changes can make people become emotional and feel like they are losing responsibility. In order to mitigate this, it is important for both teams to encourage dialogue and to try to work together as much as possible.

Policy phase

This phase is divided into two parts:

First, there's the revision of the current organization's IT security policy. Most organizations have some security policies already defined, in order to control the usage of the IT systems inside their infrastructure. However, if no policies exist, this is the time to create and spread them. If this is the case, then the *ISO 27000* family is a good starting point to achieve basic guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization, since it provides general guidance on the commonly accepted goals of information security management as well as the industries current best practices. After this policy definition, the security team should then go over all previously implemented tools in order to ensure those policies are being properly applied.

Second, there's the definition of the *SOC's* internal policies and procedures (for example, how to control the systems it is now managing). Communication in this stage is absolutely crucial and should be addressed as such. A good *SOC* needs to make sure any incoming incidents are properly reported to a previously established point of contact within the organization, any relevant security events are promptly communicated to the respective system administrators, and any required actions are appropriately taken.

Operation phase

In this phase, it's time to finally start the *SOC*. First a full infrastructure check should be carried out in order to make sure everything is working as expected, and, if necessary, make some adjustments. After this, the different systems will be integrated into the *SOC*, and it's monitoring will begin. This should be done in a controlled manner, to make sure all systems are properly configured and integrated. A *SOC* can be considered to be in the operational phase when the security team can follow the previously defined processes and get the expected results.

Intelligence phase

In this last phase, it's time to give some intelligence to the SOC, so it can independently deal with security incidents. Basically, the SOC will collect data from different sources, correlate them, and send alerts if something out of the ordinary happens in the organization's infrastructure. The use and application of intelligence is what can and most certainly will differentiate one SOC from another, and it is what will allow it to become proactive in detecting different types of information security issues. Additionally, some data mining tools and techniques can also be applied to the SOC to give it even more independence.

2.2.3 Logging

Logs are a crucial aspect in understanding what's happening in an organization's network infrastructure. They can help analysts check the network's health and at the same time give valuable insight into several different types of security issues. Without them, organizations would have a limited vision on what's going on in their networks, and security experts would have a lot more difficulties in identifying malicious behaviors or actors that are motivated to harm the infrastructure. [5]

So, what is a log? According to [5], a log is "the most basic form of information a system can generate". It can be generated by an operating system, application, service, or almost anything that records basic information about something that just happened. They are usually produced as a form of audit, so they can give indication that something went wrong and provide hints on how to proceed. Nowadays, what modern Security Incident and Event Management systems (*SIEMs*) do is take different logs from different sources, combine them (log correlation) and them do something with that information (for example, alerting the *SOC* security team that a specific user is performing any unusual activity).

Logs can help diagnose problems (for example, services not starting properly or failed user login attempts), can provide valuable information, such as which accounts accessed which services and all the actions that were performed, and even let the user know when everything is just running as it is supposed to.

Another important aspect is log storage. If the organization keeps its system's logs under storage for a certain period of time, the security experts can them dive into them and check for how long the infrastructure has been vulnerable to this kind of breach and try to figure out when it might have started.

Proactive logging

Being proactive about something means to have an anticipatory, change-oriented and self-initiated behavior. A proactive logging security approach leverages from the appliance of intelligence to itself and is able to provide real time visibility into ongoing activities across the infrastructure, by correlating and analyzing different types of logs, so when any suspicious activity happens, the right people can be immediately alerted, and a security incident can be avoided.

Reactive logging

On the other hand, if an organization chooses to have a reactive logging tool instead of a proactive one, it would only be able to react after some security problem has already been identified. This can be bad for the organization, since it doesn't have the ability to search for unusual behavior, and instead has to wait for a security breach to happen in order to be able to protect itself from it.

2.2.4 Events

By checking a dictionary [10], an event can be defined as" something that happens or is regarded as happening; an occurrence, especially one of some importance.". Now, if we apply that to computing, we can say that an event can be any identifiable occurrence that has significance for system hardware or software. Finally, if we bring this definition to an information security context, we can say that security events are events that may have some significance for the security of systems or data (for example, a change in a network's usual operating mode or an indication that a certain policy might have been violated). All events are an input to the *SOC*, which then require further filtering and analysis from the security team, in order to determine if it requires further investigation and, if that is the case, if it's necessary to deploy any actions (for example, a spam complain from a user might not require much response, however a Distributed Denial of Service (*DDOS)* attempt by multiple attackers might do). [5]

2.2.5 Alerts

Once again, if we check the dictionary, an alert is defined as" a warning to people to be prepared to deal with something dangerous". Well, by transporting this definition into information security, we can say that an alert is a particular event of some interest that requires further analysis by a security expert who has the appropriate tools and authority to do so [5]. They are typically triggered from the occurrence of certain events. For example, let's say a user fails its login credentials many times at an unusual hour (very early in the morning). Here, the event would be the login errors themselves, and the alert would be a message sent by the SOC to the security team letting them know what just happened.

However, not all events are worthy to be considered alerts. It is the duty of the SOC's security team to find a" sweet spot", where there's a balance between the events that might occur and the alerts that should be generated, because the more alerts the SOC receives, the more work it would need to perform and thus its performance may be affected.

False positives

If after an alert is triggered and the security team has looked into it only to find legitimate events, then this alert can be considered a false positive. This can occur when a rule to detect a specific behavior which is considered to be harmful for the infrastructure is created but then it turns out some applications actually do that exact thing as one of its normal functions. This is why it is very important to thoroughly test the SOC before deploying it to a production environment (although this might not always be possible), in order to avoid this kind of misleading events, which can inadvertently consume much of the security team's valuable time.

False negatives

Although false positives are something any SOC's security team doesn't want, since it just generates noise and wastes their time looking for something that isn't wrong, it is way better to have a SOC generating" fake alerts" than a SOC that fails to generate some. When something out of the ordinary is happening in the organization's infrastructure and the SOC fails to detect it, it is considered to be a false negative. A false negative is something very serious because it not only implies the failure of the currently implemented tools, but also of the defined procedures. Again, this is why it is very important to test the SOC, to make sure it doesn't become" over tuned", which might result in it letting some harmful events pass.

True Positive

A true positive is the event in which the SOC detects that something bad has or is still happening in the organization's infrastructure. These are alerts that are configured correctly and are triggered properly to notify the right people that a security issue exists, and further analysis or remediation is needed.

True Negative

A true negative event occurs when no alarms are raised. This means that the SOC's rules and tools are working properly, and nothing out of the ordinary is happening. It is important though to be careful when tuning the SOC, since true negatives can be turned into false positives. Once again, this is why the testing part of the SOC is so important, and several different scenarios should be tested in order to make sure it is properly tuned.

2.2.6 SIEMs

A *SIEM* is a hybrid solution that combines both *Security Information Management (SIM) and Security Event Management (SEM)* tools into an all-in-one Security Management System in order to provide the end-user a bird's eye view of an IT infrastructure. It fulfills two main objectives: detect security incidents in (near) real-time and efficiently managing logs. With this in mind, it can be said that the principle behind every SIEM is its capabilities for collecting, storing and prioritizing all sorts of events from multiple different sources, identify unusual behaviors, and then take the appropriate and necessary actions. For this purpose, it has built-in functions that can aggregate and correlate events and generate totally new security-relevant ones, which can then be investigated by the *SOC's* security team.

Nowadays, most *SIEM* systems work by setting up several collection agents in order to collect security-related events not only from the end-users, servers and network equipment, but also from specialized security equipment like firewalls, antivirus or intrusion prevention and detection systems. These collectors will then forward events to a centralized management console, which is where they will be analyzed by the security team, in order to establish the appropriate relations and priorities between them, according to previously defined use cases (see figure 2.5).

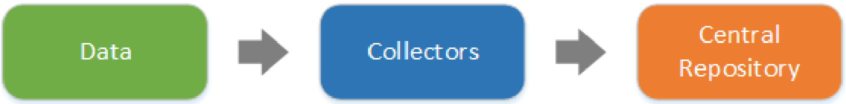


Figure 2.5 SIEM Architecture

Every SIEM should provide a variety of different services and capabilities:

- Event and Log Collection, by collecting logs and data from multiple sources across the organization's infrastructure.
- Real-Time Dashboards, which should give a back-to-back view of the infrastructure being monitored.
- Normalization and Categorization, by translating original logs and data to a universal format, and then categorizing them into previously defined categories.
- Correlation, by giving context to the data and forming real-time or historical rule, architecture and alert-based relationships between them.
- Adaptability, since a *SIEM* should be able to work with all kinds of vendors.
- Alerting, by triggering alerts to the security team. Email and SMS are usually the most commonly used alert mechanisms.
- Prioritization, by highlighting important security event over less critical ones. This is usually accomplished by event correlation with vulnerability data.
- Reporting, which covers all historical views of the collected data. It should also be possible to generate analytic reports to aid forensic investigations, and to detect and predict possible upcoming security breaches.
- Compliance, which helps to maintain a solid security posture and, at the same time, adapt to the existing regulations.
- Log Management, through log and event storage.

- Security role workflow, by providing incident management capabilities like opening cases and carrying out investigative tasks, as well as automatically or semi-automatically executing conventional tasks for security operations.

Besides this, there's one really important aspect to take into consideration when talking about *SIEMs*, which is performance. The volume of logs and data a *SIEM* might be required to process can escalate very quickly across time, so it is crucial to only send to it exactly what is needed in order not to affect its performance (for example, by splicing unnecessary fields from logs).

Generally speaking, a *SOC* that operates without a *SIEM* as its integrated part is seriously handicapped, since *SIEMs* are one of the best available tools that take advantage of security intelligence in order to proactively monitor an entire infrastructure for any suspicious activities.

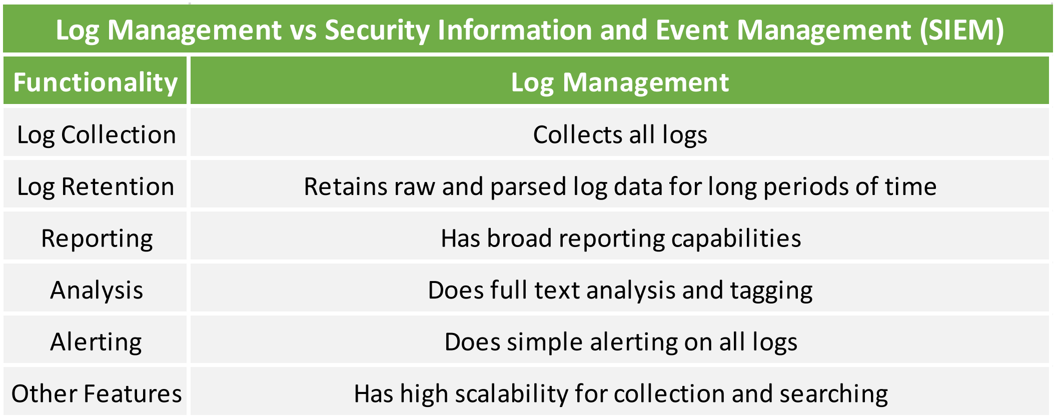
2.2.7 Log management

Log Management can be defined as the processes and policies employed to manage and simplify the production, spread, examination, storage, archiving and removal of log data created within a certain information system. It should be considered a system capable of long-term storage of complete raw event data, with some advanced search and reporting capabilities which allow auditors to ensure compliance and for the security team to perform forensic analysis as well as historical research.

Every log management solution should include some key features:

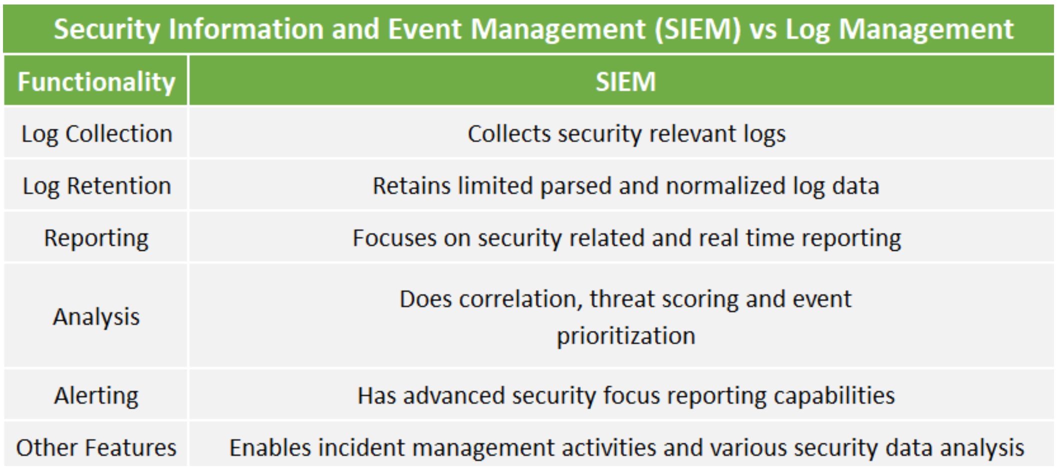
- Log data collection, by collecting all sorts of logs.
- Efficient retention, since collecting very large amounts of data and still be able to provide fast search and quick access to it can be challenging. Also, several regulations order explicit terms for log data retention, usually for a few years, which makes this functionality critical for log management solutions.
- Searching, which is the principal way of accessing information, and therefore essential for investigative use of logs, log forensics and finding faults while using logs for application troubleshooting.
- Log indexing or parsing, by taking advantage of indexing technology which creates a data structure called an index that allows very fast keyword and Boolean searches across the log storage solution.
- Reporting and scheduled reporting, which cover all the data collected by the log management solution and is similar to *SIEM* reporting (covers all historical views of the collected data and can generate analytic reports to aid forensic investigations among other purposes).

2.2.8 SIEM vs log management



Log Management vs Security Information and Event Management (SIEM)	
Functionality	Log Management
Log Collection	Collects all logs
Log Retention	Retains raw and parsed log data for long periods of time
Reporting	Has broad reporting capabilities
Analysis	Does full text analysis and tagging
Alerting	Does simple alerting on all logs
Other Features	Has high scalability for collection and searching

Table 2.1 Log Management Solutions



Security Information and Event Management (SIEM) vs Log Management	
Functionality	SIEM
Log Collection	Collects security relevant logs
Log Retention	Retains limited parsed and normalized log data
Reporting	Focuses on security related and real time reporting
Analysis	Does correlation, threat scoring and event prioritization
Alerting	Has advanced security focus reporting capabilities
Other Features	Enables incident management activities and various security data analysis

Table 2.2 SIEM Solutions

The main divergence between *Security Information and Event Management systems (SIEMSs) and Log Management* solutions (see tables 2.1 and 2.2) stems from the fact that *SIEMs* focus on security (security information and event management, along with the use of different IT related data for security purposes), while log management has its main focus on logs (usually raw and unmodified) and extensive uses for log data, both within and outside the security domain [11], [12] and [13].

If an organization's wants to start monitoring its own IT infrastructure, it first needs to decide which technology to deploy first: *SIEM* or *Log Management*? This can be easily answered. If it has logs, it needs a log management solution. This is applicable whether it has just one or more than ten thousand servers. The technology they use in order to properly manage logs will naturally be different, but the principle behind them remains exactly the same. Baring this in mind, and with a log management solution implemented, an organization can now begin to search its own logs. These searching capabilities will not only increase the security team's investigative skills but will also help them meet any compliance mandates that might exist.

Afterwards, and with the deployment of a log management solution for security, compliance and operational purposes now finished, the expected and reasonable next step for the organization is to progressive escalate to a near real-time event management tool in the form of a *SIEM*. But first, it needs to review some criteria in order to be able to take full advantage of this technology.

Generally, an organization should:

- Have the ability to respond to alerts as soon as they are produced.
- Have security monitoring capabilities in the form of a Security Operations Center or, at least, a dedicated IT team responsible for monitoring the infrastructure.
- Have the ability to tune and customize the *SIEM* tool, because out-of-the-box deployments hardly succeed in reaching their full potential.

After both log management and *SIEM* are deployed and fully operational, an organization is then able to switch from complete log ignorance to a near-real-time security monitoring. This process is composed by various transition phases, as it can be seen in the figure below (figure 2.6):

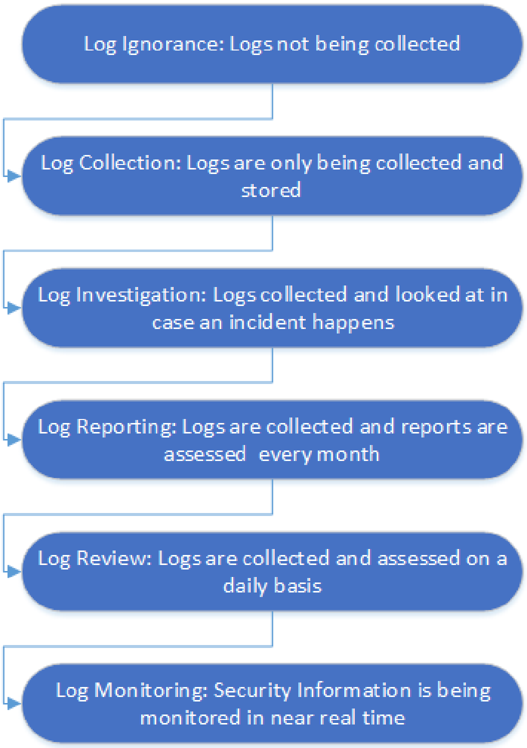

Log Ignorance: Logs not being collected
Log Collection: Logs are only being collected and stored
Log Investigation: Logs collected and looked at in case an incident happens
Log Reporting: Logs are collected and reports are assessed every month
Log Review: Logs are collected and assessed on a daily basis
Log Monitoring: Security Information is being monitored in near real time

Figure 2.6 Log transition phases

Following these processes, organizations should continuously try to improve their *SIEM* solutions by integrating it with more and more different sources, which will allow them to make better use of its analytic capabilities, and thus do a more efficient monitoring of the overall infrastructure.

2.2.9 Incidents

As a central topic of this work, it is critical to accurately define what a security incident actually is. According to *NIST* [14] *"is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices"*. These can consist of attempts to gain unauthorized access to a system or its data, can be denial of service attacks, unauthorized changes to system hardware, firmware, or software without its owner's knowledge, instruction, or consent, among others [4,5].

When the *SOC* starts to be built, and in order to enable the security team to check if it is performing as it would be expected, security incidents are a good way to achieve this, and without them, it wouldn't be possible to test the *SOC*. After they happen, the security team can then perform further analysis on the data and find out whether they're facing a false positive, or on the other side, a very serious security breach.

An incident is something that needs to be dealt with in a quick and effective way and can be very detailed or contain very little information. One important point though is to know that talking about incidents is not the same as talking about incident response. Although every incident naturally requires an incident response, the *SOC* will handle incident response 24/7 and some of those might never reach a single member of the security team (simpler incidents that can be resolved right away), where others will require the involvement of a multitude of specialized personal. For example, an unauthorized access to a certain system and a massive distributed denial of service attack, will typically require very different incident response plans.

2.2.9.1 Incident lifecycle

Unfortunately, when responding to incidents, it is just not possible to have a set of instructions for every type of attack or incident that might happen. Instead, every specialized security team should follow a generalized agreed upon script that enables them to properly manage any incoming threats. This is crucial because there are so many different types of attack vectors, that without a repeatable, effective and logical process to rely on, incident management and incident response tasks would become confusing and thus difficult to perform.

The above-mentioned script describes the sequence of steps an incident should pass through, from the moment it is first detected to the moment it is resolved – Incident Lifecycle (see figure 2.7)[15]. It should start as something modest (simple set of tasks) and then be subsequently expanded into more complex ones, always depending on the real work and needs the security team has experienced across time.

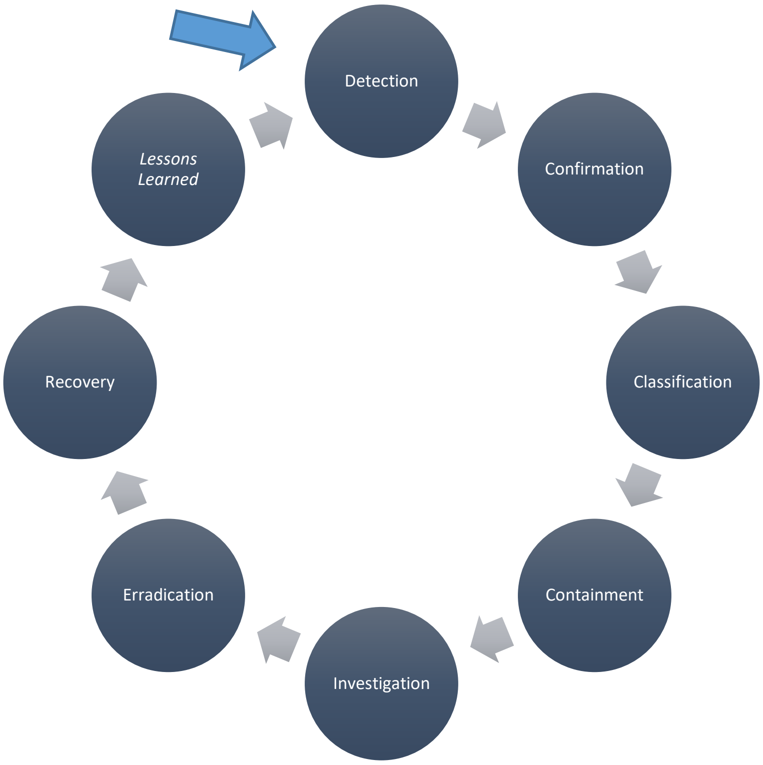


Figure 2.7 Incident Lifecycle

Detection

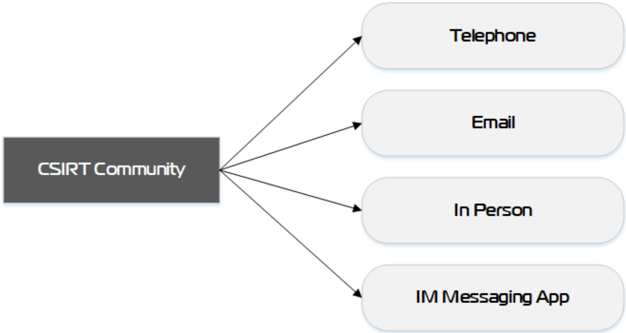


Figure 2.8 Generic SOC Reporting Channels.

Before an incident can be identified as such, the whole process starts with something or someone detecting and reporting an event which requires a closer look. The way this gets done can naturally vary (see figure 2.8). It can be the *SIEM* that after receiving a certain log from a system and analyzing it against some previously defined conditions, decides that a *ticket* must be created in the *SOC's* ticketing system requiring further analysis, or it can be a user, a system administrator or an external entity that called or emailed to reporting something out of the ordinary.

Confirmation

In this stage, and after the creation of a ticket for the reported event, this will be further examined by the security team in order to determine whether it is a false positive or an actual security incident. Sometimes inexperienced constituents might report some events that do not constitute security threats, and therefore these will be rejected in this stage.

Classification

After analyzing all the information available on the ticket and confirming that it is in fact a security incident, it is now time to give it a classification. This should be done accordingly to the security team's previously defined incident classification schema. This is not an easy task to perform, since not all the information required to do it is usually available at this stage. However, incidents should always be classified.

Containment

In this stage, it's all about minimizing the possible consequences of the pre-identified incident. The security team usually recommends the deployment of certain actions to try to contain the threat. The main goal of this actions is to ensure that the incident won't have any further impact on the infrastructure and can be as broad as simply blacklisting an email address, isolating a system from the network, or even greatly intensifying the monitoring of certain resources.

Investigation

This is the stage where a truly detailed and meticulous investigation takes place, in order to determine the full scope of exactly what happened. All available sources of information should be searched, and the retrieved information properly analyzed. If necessary, additional information might be requested from external sources as a complement to the investigation. After this, the security team should now be able to tell not only exactly how successful the attack was (what was compromised, which data was accessed and/or modified), but also what has caused such intrusion. Additionally, a proper way to eradicate the attack should also be given.

Eradication

Once the investigation is finished, and the security team has in its possession all relevant information regarding the incident, it is now time to completely eliminate its root cause. This is the stage to do so.

Recovery

Here, and in case the eradication stage has been successfully completed, the necessary arrangements are made in order to make sure the organization's infrastructure will keep functioning correctly and as expected. This can range from a simple reinstallation of a specific server or system, to a complete redesign of the organization's network. Also, besides recovering the infrastructure to a functional and correct state, measures to prevent this type of incident from happening again should also be deployed.

Lessons Learned

This is the last stage of the incident lifecycle and it is where a complete review of all the incident's stages will be carried out, all collected evidences will be compiled along with the suggested countermeasures and other appropriate measures that were applied. From this, a complete report on the incident will be created. This report should be able to clearly answer all questions anyone might have regarding the incident (typically who? what? where? when? how? and with how much impact?). As a *SOC* needs to gain maturity, these kinds of reports will help it to achieve just that.

2.2.10 Ticketing

Incident tracking is a must have feature of any SOC, and it's the security team's responsibility to deploy the right tools to make sure this is done properly - a ticketing system. Every time an incident occurs, a ticket must be created, assigned and tracked until the incident is considered to be resolved. Ticketing categories can also be created, in order to facilitate and organize incidents (sort them by relevance, for example). These ticketing systems should be heavily integrated with the SIEM, vulnerability management, incident response, case management processes, and other tools, in order to allow the gathering of as many information as possible regarding a certain incident.

Using a ticketing system will also allow for a central repository of all notes and data used to perform all sorts of event analysis. This will not specifically instruct the team on how to do a particular job but will help contribute to a better understanding of workflows and best practices and will allow others to follow behind them, read their notes, and validate their findings - a knowledge base.

2.3 RFC2350

One central point of this work is the revision of the RFC2350 [16]. This document specifies the Internet best current practices for the Internet community, being its main purpose the expression of the general Internet community's expectations of *Computer Security Incident Response Teams* (*CSIRTs*). Since it is not feasible to delineate a set of requirements that would apply to all security teams, a description of some general topics and issues are given in order to provide some guidance. *CSIRT* constituents need and have the right to know and fully understand all policies and procedures of ’their’ *Computer Security Incident Response Team*. In order to achieve this, the *CSIRT* should supply a formal and detailed form template which contains all this information for the users to consult.

2.3.1 CSIRT’s

One main contribution of this document is the proper definition of what a *CSIRT* team actually is, and what services it offers to the community. According to the document [16], a *CSIRT* is” a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency. Any group calling itself a *CSIRT* for a specific constituency, must therefore react to reported security incidents, and to threats to ‘their’ constituency in ways which the specific community agrees to in its general interest”. It is essential for any community member to be able to understand what can be expected from their *CSIRT* team. Therefore, it is the team’s responsibility to define and make clear what services it offers to the community. Then, after they’re properly defined, they should be published and made visible for everyone in the organization.

Another important aspect the *CSIRT* team must bear in mind is the procedure one should follow in order to report a certain incident. In order to that, a template that *CSIRT* teams can follow to give such information is provided. User input is vital to the *CSIRT*, and without them the effectiveness of its service can be greatly diminished. Since some incidents can be originated from outside local community boundaries and affect inside sites, or the other way around, it is possible that some cooperation between different *CSIRT* teams might be required. Constituent communities need to know exactly how their *CSIRT* will be working with other *CSIRTs* and organizations outside their constituency, and what information is going to be shared. There are different kinds of response teams. Some can have very broad constituencies, while others have some more bounded or even very restricted ones. However, they all should be knowledgeable about the team’s policies and procedures. Again, and according to the document,” A *CSIRT* should communicate all necessary information about its policies and services in a form suitable to the needs of its constituency”.

However, “It is important to understand that not all policies and procedures need to be publicly available. For example, it is not necessary to understand the internal operation of a team in order to interact with it, as when reporting an incident or receiving guidance on how to analyze or secure one’s systems”. Instead of supplying this kind of information in multiple ways, like it was done in the past (Operational Framework, FAQs or even papers, for example), it is recommended that each *CSIRT* publishes its guidelines and procedures on their own information server, since this will allow its constituents to easily access it.

It is expected that in the near future, information regarding *CSIRT's* will become searchable, which will greatly facilitate this whole process. Before using the information presented in these forms, it is highly recommended though that the user first checks its authenticity (these kinds of documents should be protected by digital signatures). This way, the user will be able to verify that the template was indeed published by the *CSIRT* and that it has not been changed.

Relationships between different *CSIRTs*

When working with other *CSIRT's* is something strictly necessary, the different teams should be clarified about the nature and extent of such collaboration, as sensitive information may be disclosed in the process. This collaboration can involve interchanging of advices, knowledge dissemination of problems, and strict collaboration in order to resolve a certain security incident. They can be established in the form of a peering agreement, in which the *CSIRTs* involved agree to work together and share information, or as a simple co-operation, where a *CSIRT* simply contacts another and asks for help or advice.

Establishing secure communications

After two parties have agreed to share information, they need to make sure all communications are done using secure channels. This can be achieved by ensuring the following properties:

- Confidentiality - ensure no one else beside the two parties is able to access the content of the communication.
- Integrity - ensure the content of the communication is not manipulated.
- Authenticity - ensure the communication is done between the right persons.

Communication is something vital to all aspects of incident response, and the teams should use whatever algorithms and mechanisms they feel are needed in order to ensure they can communicate in a secure way

Information, policies and procedures

In this section, all types of information that the community needs to receive from its incident response team will be listed. The most important thing is that a *CSIRT* has a policy and that those who interact with the *CSIRT* are able to obtain and properly understand it. Since *CSIRT* details tend to change with time, the completed template must indicate when it was last changed, as well as how to find out about future updates. The relevant fields will be listed above:

- Date of last update - The most important thing is that a *CSIRT* has a policy and that those who interact with the *CSIRT* are able to obtain and understand it.
- Distribution list - Mailing lists are a convenient and important mechanism to deliver up-to-date information to a large number of users.
- Location of the document – It should state where a current version of the document can be accessed through a team's online information services.

The *CSIRTs* contact form, should contain the following fields:

1. Name of the *CSIRT*
2. Mailing address
3. Time zone
4. Telephone number
5. Facsimile number
6. Other telecommunication services
7. Electronic mail address
8. Public keys and encryption
9. Team members
10. Operating hours
11. Additional contact info

Besides these fields, a *CSIRT* might decide to provide more detailed information, which might include different contacts for different services, or a list of online information services, for example. Specific procedures for accessing some specific services can also be explained here.

2.3.2 Charter

For every *CSIRT*, there must be a charter, which should clearly specify what the team does, and the authority under which it will do it. The charter should include at least the following items:

- Mission Statement – it should be mainly focused on the team's main activities, which were already stated in the definition of the *CSIRT*. To be considered a *CSIRT*, the team must support incident reporting and assistance to its constituency by dealing with different kinds of security incidents.
- Constituency – The definition of a *CSIRT's* constituency should create a perimeter around the group to whom the team will provide its services. In some cases, there might be some constituency overlapping, when, for example, an *Internet Service Provider (ISP*) provides a *CSIRT* that delivers services to customers that also have *CSIRTs*. In these cases, the Authority section of the *CSIRT's* should make these relationships clear.
- Sponsorship / Affiliation – The entity which will authorize the different actions of the *CSIRT*, should be specified here.
- Authority - This section will depend in whether a *CSIRT* is organizational or community based. In the first case, its authority will be given by the management of the organization, while in the second case, it will be supported and chosen by the community, usually in advisory role. Here, it should be clearly specified the scope of the CSIRT's control as distinct from the perimeter of its constituency. If other *CSIRTs* operate hierarchically within its perimeter, this should be mentioned, and all related *CSIRTs* should also be identified.

2.3.3. Policies

Types of Incidents and Level of Support

All types of incident which the team is able to address, along with the level of support for each one of them, should be summarized in this Policies section. This last one may vary depending on factors such as the team's workload and the completeness of the information available. As a list of known types of incidents will be incomplete with regard to possible or future incidents, a *CSIRT* should also give some background on the" default" support for these kinds of incidents. Also, the team should state whether it will act on received information regarding vulnerabilities which can constitute opportunities for future incidents.

Co-operation, Interaction and Disclosure of Information

Here, it should be stated the different groups the CSIRT usually interacts with, being its main purpose to give the constituency a basic understanding of what kind of interactions are established and what their purpose is.

1. Incident Response teams - such interactions can include, for example, the report of incidents within the constituency to other teams, the handling of incidents which occurred within the constituency, but were reported from outside of it, observations reported from within the constituency indicating suspected or confirmed incidents outside of it, acting on reports of incidents from outside the constituency, the passage of information about possible vulnerabilities to vendors, giving feedback to parties reporting incidents or vulnerabilities, provisioning contacts from members of the constituency, among others.

2. Vendors - a *CSIRT* might need to work directly with a vendor to suggest improvements or modifications, to analyze a technical problem or to test some solutions.

3. Law-enforcement agencies – These can include the local police among other investigation agencies. *CSIRTs* should bear in mind the local laws and regulations, which can vary considerably in different countries.

4. Press - The press might approach a CSIRT asking for some information. A properly defined policy concerning any kind of information disclosure can be very useful, particularly for clarifying the expectations of a *CSIRT's* constituency.

2.3.4 Communication and Authentication

A policy which describes methods for secure and verifiable communication is a must have for every *CSIRT*. It should include public keys or pointers to them, key fingerprints, along with guidelines on how to use this information to check authenticity, as well as how to deal with corrupted information. At the time of this document's writing, every *CSIRT* should at least have an available *PGP key*. However, some countries do not allow strong encryption technology, and CSIRTs should naturally bear this kind of situations in mind. Besides this, all exchanged correspondence should include digital signatures, and telephone communications can have secret authentication data.

2.3.5 Services

CSIRT services can be divided into real-time activities, which are directly related to incident response, and non-real time proactive activities, which are supportive of the incident response tasks.

Incident Response

Incident response normally consists in assessing incoming reports about different incidents and then follow up on these with other CSIRTs, ISPs and sites. It can be divided into three parts:

1. Incident Triage, which includes report assessment (the interpretation of the different incident reports that arrive, their prioritization and correlation with ongoing incidents and trends) and verification (checking if an incident has, or has not, occurred).

2. Incident Coordination, which includes information categorization (categorizing the incident related information - log files, contact information, etc.) and coordination (notifying other involved parties on a need-to-know basis).

3. Incident Resolution, which includes technical assistance, eradication (elimination of the security incident's root cause) and recovery (restoring the system(s) to their status before the security incident has occurred).

Proactive Activities

Some proactive activities the CSIRT should carry out are described below:

1. Information provision - this often include an archive of known vulnerabilities, patches or resolutions of past problems, or advisory mailing lists.
2. Security Tools - This may include tools for auditing a Site's security.
3. Education and training
4. Product Evaluation
5. Site security auditing and consulting

2.4 Existing Work

2.4.1 SANS

Figure 2.9 SANS Logo

The SANS institute white paper called "Building a World-Class Security Operations Center: A Roadmap" [17] is a great reference for organizations that seek guidance on how to build, incorporate and maintain a Security Operations Center.

First, it addresses the importance of creating a plan for each incremental phase of implementation, since it will not only allow the execution of controlled and regular incremental improvements, but also to establish different milestones that lead the organization towards an optimized security posture and proper incident response capabilities. Then, it defines a SOC as an intrinsic collaboration and communication among multiple functions (people), disparate security products (technology), and varying processes and procedures (processes).

For people, it alerts for the importance of having highly specialized security professionals who can effectively perform incident response and other SOC related tasks. It structures the team into three different tiers, being the first one the Alert Analyst which continuously monitors the alert queue, triages security alerts, checks the health of security sensors and endpoints and gathers data and context necessary to initiate Tier 2's work. The tier 2, on the other hand, is composed by incident responders and they are responsible for carrying out deep incident analysis by correlating data from different sources, determine if a certain system has been compromised, advise on possible mitigation techniques and provide support for new threat detection methods. The tier 3 is then composed by the so-called Hunters, which are responsible for developing, tuning and implementing threat detection analytics. After these three different tiers, there's the SOC Manager. Its main responsibilities are to manage all SOC resources (for example, personnel, budget, shifts, different strategies and communication with management) and at the same time serve as an organizational point of contact for any business-critical incidents that might happen.

For processes, it states that defining repeatable incident triage and investigation strategies, will standardize the security analyst's actions and thus ensure that no important tasks are left behind. Also, the different tiers that compose the SOC's security team will have specifically defined roles, which will allow for greater work efficiency.

For technology, it refers the importance of adopting technologies that can perform continuous data collection, aggregation, detection, analysis and management tasks, as they constitute the core technology behind any successful SOC.

After these three definitions, the importance of threat intelligence in a SOC related environment is discussed, and some obstacles to efficient SOC incident handling are briefly referred.

However, this paper has a major drawback: it lacks a practical approach to its theoretical content. Anyone who reads this paper, will become acquainted with the main concepts behind developing and maintaining a Security Operations Center, but since there's always a difference between theory and practice, organizations that want to rely on this paper in order to build their SOC, will most likely run into some implementation problems along the way.

2.4.2 MITRE

Figure 2.10 MITRE Logo

The book entitled “Ten strategies of a world-class Cybersecurity Operations Center” from MITRE [1] is also a very good reference for anyone in the information security field since it constitutes a solid and complete knowledge base for SOC related material. It contains what the authors considered to be tenth most important strategies to discuss and follow regarding computer network defense and it is aimed at everyone immersed in SOC related environments (from the least experienced security analyst all the way to the SOC manager).

For SOC Managers, for example, this book will not only help them understand how the SOC can be positioned inside the organization or the constituencies it protects, but also how it should be structured, what services it should offer, how to deploy some useful data collection strategies and how to train the specialized staff.

For technical personnel, the book addresses important topics such as training, development and role related functions in a SOC environment, different data analysis techniques, procedures, technologies and tools, and the purpose of SOCs in the modern enterprise world.

Besides this, the book also has a whole chapter dedicated to Cyber Threat Intelligence, which has become a central discussion topic these days. Advanced Persistent Threats (network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time) are becoming more and more refined, making it crucial to develop defensive mechanisms in order to effectively protect the organization’s information and intelligence from these.

There’s one aspect though that this book doesn’t address: a practical approach to Security Operations Centers. Although all theory is greatly covered, and this being a reference book from a prestige institution on how to properly build a SOC, it would be expected that, in addition to the theoretical part, a practical example was provided. This way, readers could see that the discussed topics and proposed actions would actually work as expected in a production environment.

Chapter 3

[Confidential]

Chapter 4

[Confidential]

Chapter 5

[Confidential]

Glossary

SOC Security Operation Center

CSIRT Computer Security Incident Response Team

NOC Network Operation Center

SysAdmin System Administrators

DDOS Distributed Denial-of-Service

XSS Cross-Site-Scripting

SQLi SQL Injection

SIEM Security Information and Event Management

RTIR Request Tracker for Incident Response

Chapter 7

Bibliography

[1] C. Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*, Bedford, MA: MITRE Corporate Communications and Public Affairs, 2014.

[2] S. Schinagl , K. Schoon and . R. Paans, "A framework for Designing a Security Operations Centre (SOC)," 48th Hawaii International Conference on System Sciences, Hawaii, 2015.

[3] V. FRILIGKOS , "Setting up and Fine Tuning a Security Operations Centre," Chalmers University of Technology Department of Computer Science and Engineering , Göteborg, Sweden, 2013.

[4] J. Muniz , . G. McIntyre and . N. AlFardan , Security Operations Center - Building, Operating and Mantaining your SOC, Indianapolis, Indiana , USA: Cisco Press , 2016.

[5] D. Nathans, *Designing and Building a Security Operations Center,* Waltham, MA: Elsevier Inc., 2015.

[6] A. Michail, Security Operations Centers: A Business Perspective, Utrecht : Utrecht University .

[7] . A. Torres , "Building a World-Class Security Operations Center: A Roadmap," SANS Institute , 2015.

[8] D. Kelley and . R. Moritz, "Best Practices for Building a Security Operations Center," InfoSec Today, 2006.

[9] H. Slatman, "Unboxing Security Analytics: Towards Effective Data Driven Security Operations," University of Twente, Twente, 2016.

[10] Dictionary.com, "Dictionary.com," [Online]. Available: http://www.dictionary.com/browse/events. [Accessed 8 6 2018].

[11] D. Swift, "Successful SIEM and Log Management Strategies for Audit and Compliance," SANS Institute, 2010.

[12] Layer8, "SIEM & Log Management Framework," Layer8, Lisbon, 2018.

[13] K. M. Kavanagh and T. Bussa, "Magic Quadrant for Security Information and Event Management," Gartner, 2017.

[14] P. Cichonski, T. Millar, T. Grance and K. Scarfone, Computer Security Incident Handling Guide, U.S. Department of Commerce, 2012.

[15] Layer8, "SOC8 Incident Lifecycle," Layer8, Lisbon, 2018.

[16] N. Brownlee, E. Guttman, The University of Auckland and Sun Microsystems, RFC2350 - Expectations for Computer Security Incident Response, Internet Engineering Task Force, 1998.

[17] A. Torres, Building a World-Class Security Operations Center: A Roadmap, SANS Institute, 2015.

[18] TechRepublic, "TechRepublic.com," [Online]. Available: https://www.techrepublic.com/blog/it-security/how-to-choose-a-siem-solution-an-overview/. [Accessed 8 6 2018].

[19] ManageEngine, "ManageEngine Blog," [Online]. Available: https://blogs.manageengine.com/active-directory/log360/2017/10/10/six-things-to-consider-before-choosing-a-log-management-solution.html. [Accessed 8 6 2018].

[20] I. Institute, "InfoSec Institute," [Online]. Available: https://resources.infosecinstitute.com/structure-csirt-soc-team/#gref . [Accessed 8 6 2018].

[21] H. P. Enterprise, "Helwett Packard," [Online]. Available: https://www.hpe.com/us/en/what-is/security-monitoring.html. [Accessed 12 6 2018].

[22] C. Portugal, "Centro Nacional de Cibersegurança," [Online]. Available: https://www.cncs.gov.pt/certpt/coordenacao-da-resposta-a-incidentes/. [Accessed 12 6 2018].

[23] R. Tracker, "Request Tracker for Incident Response," [Online]. Available: https://bestpractical.com/rtir/. [Accessed 12 6 2018].

[24] Layer8, "SOC8 Ticketing System," Layer8, Lisbon, 2018.

Chapter 8

Annexes

8.1 Annex A – Registering a CSIRT Team

When first assembling a Computer Security Incident Response Team (CSIRT) [22], and since it is "a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency", it is then important to have multiple engineers specialized in different information security related areas, in order to make the team more capable of addressing different security related tasks.

So, the first thing an organization needs to do is to register its team as an official CSIRT. In order to do that, some requirements must be met, and since this work is being written in Portugal, the requirements listed below will be the ones currently required in this country:

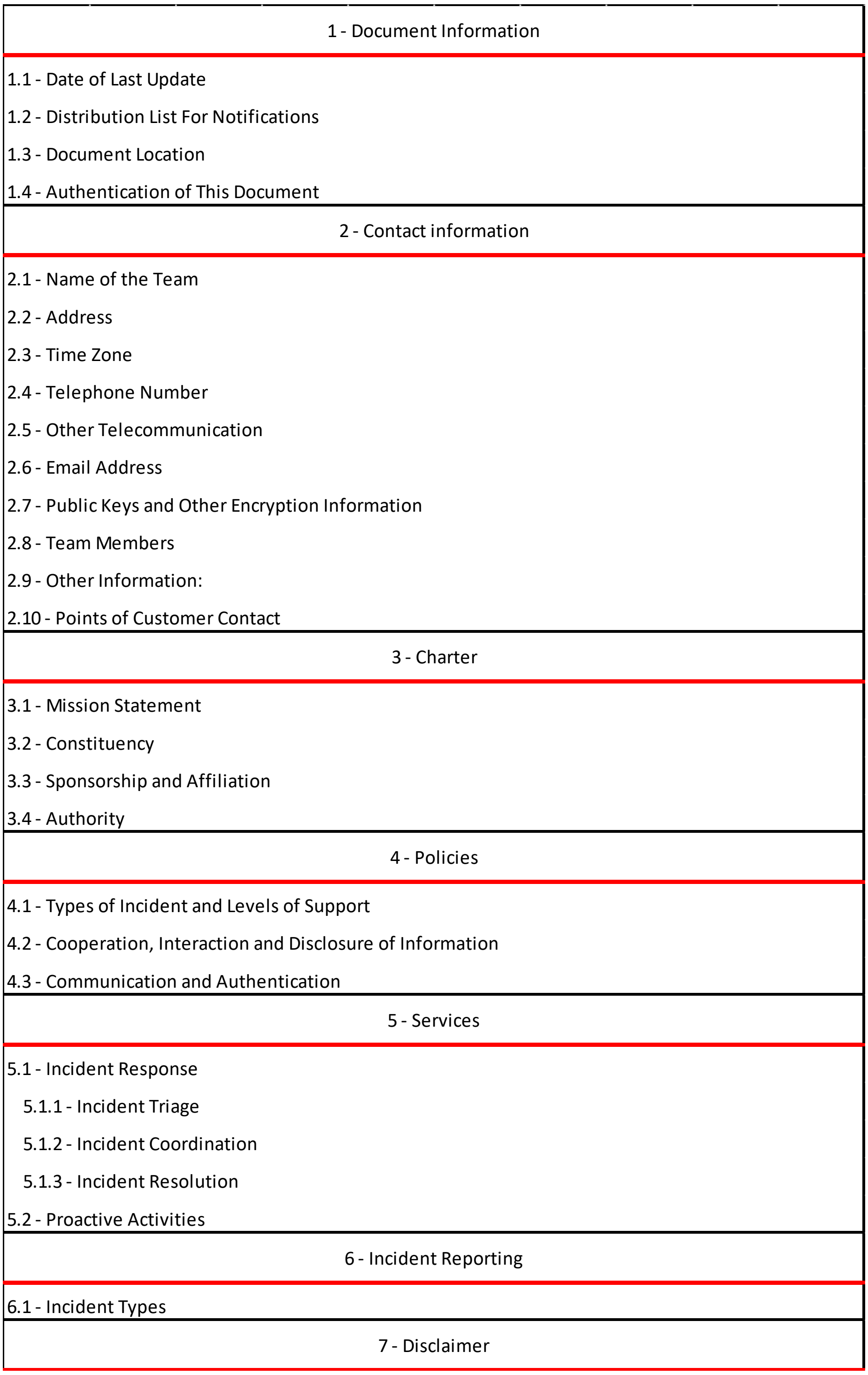
1. The candidate must be a collective person.
2. It must offer a variety of services in the information security area including, at least, the handling of security incidents.
3. It must have an incident response team (CSIRT) properly formalized and announced.
4. It should act by reference to a relevant and well-defined community of users, inside its national territory, which is characterized by at list two of the following points:
    a. Address space (CIDRs or IP ranges).
    b. Autonomous System Number (ASN) enumeration (for example, AS 64996).
    c. Sub-domains. (for example, *.pt).
    d. Clear and concise definition about the type and number of users of the served community (for example, 2500 active users from the company X).

After making sure these requirements are met, the organization can then submit its own application to integrate its country's CSIRT network. In order to do that, the following information should be submitted:

a. CSIRT name.
b. Entity name.
c. Constituent’s community description.
d. Description of all the security services the entity offers.
e. Motivation to integrate the CSIRT network.
f. The candidate should collect at least two recommendations from other network members, stating the above mention requirements.
g. The candidate should possess a written approval and authorization from the organization it is representing, in order to validate the whole application process.

The request is then analyzed by the network’s executive committee. During this process, some additional information by be required. If there are no objections, the candidate will be submitted to a vote in the network’s general meeting, and depending on its approval, will become, or not, a part of the national CSIRT network.

After the organization sees its CSIRT team officially recognized, it should tell its constituents (SOC costumers) how they can properly report any security incidents that might happen within their organization’s infrastructure. To do this, CSIRTs should rely on the RFC2350 [16] and create a form similar to the one presented in the RFC which should specify the full details on how to contact the CSIRT. A detailed example on how this document should look like will be shown below (figure 8.1):



1 - Document Information

1.1 - Date of Last Update

1.2 - Distribution List For Notifications

1.3 - Document Location

1.4 - Authentication of This Document

2 - Contact information

2.1 - Name of the Team

2.2 - Address

2.3 - Time Zone

2.4 - Telephone Number

2.5 - Other Telecommunication

2.6 - Email Address

2.7 - Public Keys and Other Encryption Information

2.8 - Team Members

2.9 - Other Information:

2.10 - Points of Customer Contact

3 - Charter

3.1 - Mission Statement

3.2 - Constituency

3.3 - Sponsorship and Affiliation

3.4 - Authority

4 - Policies

4.1 - Types of Incident and Levels of Support

4.2 - Cooperation, Interaction and Disclosure of Information

4.3 - Communication and Authentication

5 - Services

5.1 - Incident Response

- 5.1.1 - Incident Triage
- 5.1.2 - Incident Coordination
- 5.1.3 - Incident Resolution

5.2 - Proactive Activities

6 - Incident Reporting

6.1 - Incident Types

7 - Disclaimer

Figure 5.1 CSIRT Contact Form

In the first section (Document Information), some information regarding the document itself should be presented: when it was last updated, the distribution list from where the constituents can receive notifications and where the current version of the document can be found.

Then, in the following section (Contact Information), some contact information regarding the CSIRT team itself should be provided. It is important to state though that not all fields are required. For example, it is perfectly normal if an organization wants to keep their CSRIT member's names private.

In the next section (Charter) it should be clearly specified what the CSIRT will do and the authority under which it will do it. The mission statement should specify the team's core activities already stated in the CSIRT's definition. The constituency definition should specify the group to whom the team will provide service. The Sponsorship and Affiliation part will help the users understand the background of the CSIRT and will help to increase trust between constituents and the CSIRT. Lastly, the CSIRT might not have the authority to handle all systems within its perimeter, so in the authority part it should be specified all the areas where the team can intervene.

In the Policy section, the types of incidents and their respective levels of support the team should be able to address should be listed here. The different groups the CSIRT will interact with should also be made explicit, along with the reporting and disclosure policy which should state who will be the recipients of a CSIRT's report in each circumstance. Finally, a policy which describes the secure and verifiable communication methods that will be used by the CSIRT should also be presented.

Then, in the Services section, the CSIRT should describe how it will handle two different categories: Incident Response and Proactive Activities. In the first one, it should be briefly described how the team will access incoming reports about incidents ("Incident Triage"), follow up on these with other teams ("Incident Coordination") and help recover from them ("Incident Resolution"). In the second one, the CSIRT should tell what kind of proactive activities are carried out in order to keep their community up-to-date on security related issues.

Regarding the Incident Reporting section, providing forms can make it substantially easier for users and teams to deal with incidents. By pre-knowing the required questions to report a certain incident, the constituent can make sure it has all the necessary information and answers to the CSIRT's pre-defined questions before submitting the report.

The last section, Disclaimer, should state that despite taking all precautions to properly spread all information through all its communication channels, the CSIRT does not hold itself responsible for any errors or omissions, or any damage caused by the usage of that information.