IceCube Cybersecurity Improvement Plan

Recommendations to Enhance IceCube's Cybersecurity Program

January 2014
Version 1.0
For Public Distribution

James Marsteller & Randy Heiland

About CTSC

The mission of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC, trustedci.org) is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors. This mission is accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community.

Acknowledgments

CTSC's engagements are inherently collaborative; the authors wish to thank the IceCube team, especially Steve Barnet, Gonzalo Merino, Paul Wisniewski, and Matt Newcomb, for the collaborative effort that made this document possible.

This document is a product of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). CTSC is supported by the National Science Foundation under Grant Number OCI-1234408. For more information about the Center for Trustworthy Scientific Cyberinfrastructure please visit: http://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Using & Citing this Work

Site this work using the following information:
J.A. Marsteller and R.W. Heiland, "IceCube Cybersecurity Improvement Plan," Center for Trustworthy Scientific Cyberinfrastructure, trustedci.org, January 2014. Available: http://hdl.handle.net/2022/17364

This work and updates (if any) are available on the web at the following URL:
http://trustedci.org/icecube/

Table of Contents

Status

The IceCube Cybersecurity plan is in active status. Future revisions will be documented in this section.

Abstract

CTSC and IceCube undertook a collaborative effort to conduct a cybersecurity risk assessment that analyzed the existing IceCube cybersecurity plan and cyberinfrastructure. The risk assessment was used to gather, document, and prioritize IceCube risks. From that assessment CTSC and IceCube developed this cybersecurity plan with a set of recommendations for IceCube to improve their existing cybersecurity program. This cybersecurity plan was developed based on the identified risks, threats and vulnerabilities from the assessment exercise. The result is an informed approach to the cybersecurity for the IceCube cyberinfrastructure.

For the purpose of this document we are defining a Cybersecurity Plan as a long-term structured approach to develop, implement and maintain an environment that ensures the reliability and trustworthiness of organizational assets.

1 IceCube Cybersecurity Plan Overview

CTSC team members and IceCube staff undertook a collaborative effort to conduct a cybersecurity risk assessment and to develop a cybersecurity plan for the IceCube. This effort began in May 2013 with the formation of the CTSC team and initial communications with Steve Barnet and Gonzalo Merino of IceCube. Over the following months, the CTSC and IceCube conducted a risk assessment exercise considering both IceCube's cyberinfrastructure and existing cybersecurity plan that identified key areas in need of development that would strengthen the security posture of the IceCube environment.

In addition to this cybersecurity plan, a separate report documenting the risk assessment process and its findings are included in the final deliverables for this engagement. Cybersecurity planning begins with identifying the assets that are of value to the organization and implementing a set of controls to minimize the risk to those assets from a wide variety of threats. The result of such an assessment can be used to prioritize tasks and allocate the resources providing the most effective risk management strategy.
When approaching the task of developing a cybersecurity plan for IceCube, the CTSC team members applied the cybersecurity planning lifecycle methodology featured in Figure 1. Steps 1 through 3 have been completed during this engagement:

1. Defining the project goals and documenting the operational environment. Including review of IceCube's existing Cybersecurity policies, procedures and plan.
2. Identifying risks, threats and impact to IceCube assets.
3. Identifying controls that can be implemented to minimize the risk to IceCube assets.

The next step is to apply the recommendations (controls) to the IceCube environment found in Section 2, "IceCube Cybersecurity Planning Goals." The recommendations have been categorized into a plan based upon a number of considerations including the findings of the risk assessment process, observations made during the engagement and comparison to commonly used best practices for the CI community.

As a result of the work performed in the engagement, it should be acknowledged that the CTSC team found IceCube to have a relatively mature cybersecurity program in comparison to other CI projects of similar size. For reference, the following existing IceCube policies, procedures and related documents that support the IceCube cybersecurity program were reviewed:

- UW-IceCube Security Policy and Procedures
- Acceptable Use Policy and IceCube VO[1]
- IceCube Incident Response and Escalation Procedures

[1] http://icecube.wisc.edu/collaboration/aup

- IceCube Network Security Zones (Infrastructure Diagram - “i3zones.pdf”)
- IceCube Science DMZ (Infrastructure Diagram - “Science DMZ.pdf”)
- IceCube Live System Security[2]

It seems clear that having to interact with the facility at the South Pole, which operates under FISMA, caused IceCube to have to initially consider and document their cyberinfrastructure and cybersecurity. However, as with any cybersecurity plan, IceCube’s must be regularly reviewed and adjusted as the environment and personnel are always in a state of change. New threats emerge and the cybersecurity plan must anticipate these new hazards and offer protection and guidance when they arise. And finally, one must be alert to degradations in the program due to the distractions from the day-to-day operation of scientific cyberinfrastructure and the loss of knowledge that can come about from personnel changes.

Figure 1. Cybersecurity Program Lifecycle

[2] https://docushare.icecube.wisc.edu/dsweb/Services/Document-55765

2 IceCube Cybersecurity Planning Goals

This section lists overall recommendations for risk mitigation that have been categorized into a plan based upon a number of considerations including the findings of the risk assessment process, observations made during the engagement and comparison to commonly used best practices for the CI community. IceCube's past work in developing a cybersecurity program was considered during the assessment process and as a result, it was found to be well positioned in addressing the most critical threats that were identified. Because of this past work, there were no high risk threats that were identified.

2.1 High Risk Mitigation Recommendations

There were no 'High' risk threats identified through the risk assessment process.

2.2 Medium Risk Mitigation Recommendations

This section sets out recommendations for controls that (a) would have a significant impact on improving the IceCube cybersecurity posture and/or (b) are deemed important enough that work should begin on them as soon as is possible. These recommendations have been suggested to address the 'Medium' threats identified out of the risk assessment process.

1. Identify information security responsibilities for IceCube, i.e., the person (or team) that leads IceCube security. At a minimum this should include operational security, security policies, incident response, and the overall vision for the IceCube security program. Security teams are effective when they have representation from key areas within a project such as networking, system administration and management.

2. Increase frequency and automate vulnerability scans for all IceCube network connected devices. The risk assessment identified medium level risk in vulnerable IceCube servers. Identifying and addressing vulnerabilities in IceCube's infrastructure is critical in protecting against attackers who are continually scanning the Internet for resources they can compromise. IceCube conducts vulnerability scans on a semi-monthly basis. We recommended this activity be increased to weekly scans. The scanning tool IceCube uses (Nessus) can be scheduled to run automatically without human involvement. Failed scans can be sent to an email list 'security-alert@icecube.wisc.edu' (that includes members of the security team) for remediation. We also recommend web application scanning (e.g., IBM Security Appscan[3]) of the i3Live web server on a weekly basis as well. And we recommend the security team sign up to automatically receive

[3] http://www-03.ibm.com/software/products/en/appscan/

vulnerability notices[4] for the Django web application framework[5] and apply upgrades accordingly.

3. Review, update and communicate IceCube operational procedures. IceCube has a number of existing policies, including the UW-IceCube Security Policy and Procedures document, Acceptable Use Policy and Incident Response procedures. Having documented policies and procedures helps ensure that all users, PIs, and staff members understand their respective roles and responsibilities. The existing policies were developed some time ago by a former IceCube staff member. We recommend reviewing these policies, updating them and communicating them on an annual basis. There were some specific areas that were identified in the risk assessment that could benefit from continued development. For example, some additions to the acceptable use policy covering credential management (using strong passwords, managing and protecting) would help promote awareness of IceCube's policies. The University of Wisconsin-Madison Office of Campus Information Security publishes a "Creating a Strong" password guide[6] that could be referenced.

2.3 Long Terms Goals / Recommendations

The set of controls in this category are deemed important, but are recognized as being involved and needing additional time to develop. Like the controls found in previous areas in this report, several will need a more formal process put in place to address the issues on a continual basis. These long term recommendations should be considered and planned as soon as possible.

The long term recommendations have been broken into the following two, broad categories: Operational Recommendations and Auditing and Review Process Recommendations.

Operational Recommendations

1. Develop a cybersecurity awareness program. A security awareness program is an organized approach to inform staff about IceCube's security related policies and procedures as well as general security related tips (identifying social engineering attacks, keeping desktops/laptops secure, etc.). The awareness program can use a variety of ways to communicate to users: email notifications, annual training sessions,

[4] http://www.cvedetails.com/vulnerability-feeds-form.php
[5] http://www.cvedetails.com/vulnerability-list/vendor_id-10199/product_id-18211/Djangoproject-Django.html
[6] http://www.cio.wisc.edu/security-secure-passwords.aspx

on-line resources, etc.. Ideally some form of cybersecurity awareness should be incorporated into new employee training program.

2. Implement an intrusion detection system. An intrusion detection system (IDS) monitors network and system activities for malicious activities or policy violation. These systems can take the form of software or devices. There are a number of different options available but one crucial component is the development of the skills needed to understand the results of the IDS. IDS systems can be broken into two categories: network and host based systems.

   Host based IDS systems monitor the host, or computer, they reside on. These systems look at both the dynamic behavior and the state of the computer. For example, the system would monitor the operating and file systems of the host. A profile would be developed on each file, including such things as size, permissions, modification dates, etc. This information would be watched and tracked. If system files are suspiciously modified or there is other unexpected activity, the IDS could notify administrators for further investigation.

   Network based IDSs detect intrusions by analyzing network traffic and looking for signs of attack. These systems take two forms:

   - Rule based systems look at network traffic and system activities for patterns that match known exploits. These known events are the rules that the system matches against. This is much like how antivirus software works.
   - Analysis based systems monitor network and system activities for events that fall outside the normal usage. This could include such events as abnormal bandwidth, protocols, ports, foreign IP addresses or devices generally not used, etc.

   There are a number of (mostly) open source IDS projects that we recommend:

All Inclusive	Security-onion (http://securityonion.blogspot.com/)
Host Based	OSSEC (http://www.ossec.net/) Samhain (http://la-samhna.de/samhain/) Tripwire (http://www.tripwire.com - Commercial product)
Network Based	Snort (http://snort.org/) Suricata (http://suricata-ids.org/) Bro (http://bro-ids.org/)

3. Expand the IceCube Incident Response Plan. When IceCube experiences a security event, some type of incident response is necessary. A good incident response plan can minimize the effects of a security breach, allowing for a quick recovery and avoiding negative publicity. IceCube has had an established Incident Response and Escalation plan for a number of years. Some consideration should be given to expand the existing policy to give direction on documenting events and learning from them. This will help with measuring the effectiveness of response process and can be used to make adjustments for improvement. It can also act as a learning tool to avoid repeating past mistakes and for new staff that were not involved in the initial response.

   In addition to expanding event documentation, information sharing guidelines should be considered. How are security events communicated to users, project management, funding agencies and other stakeholders? Answers to these questions should be decided upon well in advance of an incident.

   The following resources provide Incident Response plans that can be used for comparison.

   - Tulane University Computer Incident Response Plan[7]
   - RedHat Incident Response Guide[8]
   - NIST Incident Response Guide[9]

4. Track Science DMZ Best Practices. IceCube (at least at UW-Madison) operates a Science DMZ, which is a relatively new concept at this point. We recommend that IceCube continues to track emerging best cybersecurity practices coming from ESnet and the broader community. One recommendation would be to assign at least one member of the IceCube team to subscribe to the ScienceDMZ mailing list[10] in order to learn from and contribute to that community. Additionally, checking network performance and reliability using the recommended tool, perfSONAR[11], on a continual basis would be a good practice. Regarding the (secure) movement of large amounts of data over a DMZ, IceCube may want to investigate the use of Globus Online[12] as a cloud-based service for its user community.

---

[7] http://isowiki.tulane.edu/Tulane_Information_Security_Policies/Tulane_University_Computer_Incident_Response_Plan

[8] https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/ch-response.html

[9] http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf

[10] https://gab.es.net/mailman/listinfo/sciencedmz

[11] http://www.perfsonar.net/

[12] https://www.globus.org/

5. Plan Audit & Review. All of the above proposed recommendations will only be effective if they are closely watched and modified as time progresses. This means there is a need for auditing of the controls themselves so that weaknesses in the approach can be identified and addressed. Along with the auditing, regular reviews are necessary to determine the effectiveness of the control.

   Without regular reviews, a cybersecurity strategy will quickly become out of date and its effectiveness will diminish. At a minimum, an annual review of the cybersecurity plan, beginning with a risk assessment activity, should be conducted to determine what changes have taken place that the plan doesn't address.

   The review may identify the need for new policies, procedures, training/education and security controls that should be added to a revised cybersecurity plan.

3 Author Information

This document is a product of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC - trustedci.org). CTSC is supported by the National Science Foundation under Grant Number OCI-1234408. For more information about the Center for Trustworthy Scientific Cyberinfrastructure please visit: http://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

James Marsteller jam@psc.edu
Carnegie Mellon University
Pittsburgh Supercomputing Center
300 South Craig Street
Pittsburgh, PA 15213
Tel. 412-268-5184

Randy Heiland heiland@iu.edu
Center for Applied Cybersecurity Research
Indiana University
2719 E. 10th Street, Suite 201
Bloomington, IN 47408
Tel. 812-552-6127