Recommendations For Improving the Security of a Science Gateway

by Trusted CI

Science gateway teams often have smaller staffs and limited cybersecurity time and funding resources. In this document we have provided actionable takeaways to empower science gateway teams as they confront cybersecurity challenges.

As part of its mission to enable trustworthy scientific research, **Trusted CI** has partnered with **Science Gateways Community Institute** to provide cybersecurity expertise for high-powered computing research enabled by science gateways. Through this partnership we have worked with many science gateways and have seen recurring cybersecurity challenges. The following recommendations address common problems for the science gateway community and are ordered by an estimation of the ease of implementation by a typical small science gateway team. The numbered pillar icons 1 denote the **Trusted CI Framework Must(s)** most relevant to the recommendation. For more info and implementation guidance related to the Musts, science gateways should reference the **Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators**.
For an updated version of this document, please visit **https://trustedci.org/sciencegateways**

A. Harden Secure Shell (SSH) configuration 15

SSH provides console and command line access to servers, exposing SSH to attackers. To ensure properly hardened and patched servers, follow SSH best practices: enable two-factor authentication (Duo, YubiKey); prohibit root user logins; utilize an automated blocking mechanism for excessive failed logins; force public key only authentication and disable password logins; disable known weak cipher/MAC/key-exchange algorithms; filter (when possible) known good source addresses
Resources: SSH hardening guide, Duo, YubiKey, Lynis, fail2ban, CIS Controls #16

B. Monitor system health 15 16

Lack of system health monitoring and alerting can affect service availability through the threat of resource exhaustion. Install software on the endpoints to monitor the system and send issue alerts. Deploy logwatch scripts to analyze logs and send daily summary emails.
Resources: Wazuh, Icinga, Grafana, Zabbix, Nagios. CIS Controls #8

C. Implement a maintainable system architecture 1 11 12 13 14

All projects have a finite amount of resources. It's tempting to overdesign or implement the latest and greatest technologies, but if staff do not have time to maintain them, it becomes a security liability. An example is deploying a Content Management System, but not having sufficient technical staff to keep it patched and secured. These issues are often rooted in the overall architectural design of a gateway. List the software needed for an architecture and assign roles and the time needed to maintain each component. Then determine if there is enough time and expertise for maintenance. If not, then re-evaluate the architecture.

D. Determine acceptable cybersecurity risks 2 5 6 7

When running an information security program there are always more security technologies to implement and associated staff to hire, but with limited resources, all of them cannot be adopted. Deploy a security assessment tool to identify risks and tweak systems and processes as needed, but realize there may still be some security gaps.
Resources: Information Asset Inventory Template, CIS Controls, CIS Benchmarks

E. Create and maintain architectural diagrams 3

Gateways can be a complex collection of different services and software stacks, interconnected in new and novel ways. To aid in understanding how components interact, produce architectural and/or flow documents to diagram the components, how they interoperate, and the trust relationships between components. This provides the ability to flag potential weaknesses in design. Assign sub-component ownership to the flow documents. Gateway owners and developers should meet to discuss, document, create, and maintain the diagrams.
Resources: Visio, diagrams.net

F. Create and maintain a data flow diagram 3

Important for easy visualization, a flow diagram represents the flow of data through a process or system and provides information on outputs and inputs of each entity and the overall process itself. This helps the project understand the potential points of exposure for data. This and the architectural diagrams recommended above are also a good first step towards completing an asset inventory, mentioned later in this document.
Resources: Diagram Software and Flowchart Maker, Flowchart Maker & Online Diagram Software

G. Adopt an Incident Response Plan 7 9 13 15

Each gateway group should designate an information security officer and create a team to handle security issues and implement an Incident Response Plan. Security personnel contact information should be made available to stakeholders (and the general public, e.g., security@project.org, depending on the type of project and funding). Having a clear communications plan and contact information in place lowers the stress during an incident and provides a step-by-step path forward during an emergency.
Resources: Trusted CI Incident Response Plan Template, CIS Controls #17

I. Harden docker/container configurations 16

Gateways often use containerization technologies to easily and reliably interconnect many different applications and services which can be exploited through exposed network ports. Secure and harden docker configurations.
Resources: Docker security, docker-security-bench, Clair, Trivy, CIS Controls #16

J. Train staff in secure coding 9 11 13 14

Gateway projects require awareness or training in secure coding practices. Refer to Open Web Application Security Project (OWASP) Secure Coding Practices for a comprehensive checklist format. Integrate them into the software development lifecycle, as they focus on secure coding requirements rather than looking for vulnerabilities and exploits.
Resources: Introduction to Software Security, OWASP Secure Coding Practices

K. Use HPC and Science Gateway resources 11 14

Make use of HPC and Science Gateway resources for research, operations, teaching, and learning. Refer to the science gateways catalog for resources, such as HUBzero, Jupyter Notebook, Apache Airavata, CILogon, and Open OnDemand.
Resources: Science gateway resources catalog

L. Perform cloud security best practices 15 16

Use cloud security best practices as needed, depending on the service, such as OneDrive, My Drive, Amazon Web Services, Azure, or Box.
Resources:
A Step-By-Step Guide to Cloud Security Best practices, 7 Cloud Security Best Practices to Keep Your Cloud Environment Secure, A Comprehensive Guide to Cloud Security in 2021 (Risks, Best Practices, Certifications.), CIS Controls Mapping to Cloud Security Alliance Cloud Control Matrix

M. Use a Security Assessment Tool 15

Run security assessment tools, such as Lynis, OpenVAS, Mozilla Observatory, Qualys, or others to identify the vulnerabilities in the system and mitigate security risks. These tools aid system hardening and compliance testing. For example, Lynis is a tool that focuses on the target host by looking at it's configuration from within the host. The other solutions listed are designed to test a host from outside by probing active services to detect vulnerabilities.
Resources: Lynis, OpenVAS, Mozilla Observatory, Qualys SSL Labs, CIS CSAT

N. Prepare an asset inventory 3 4

An asset inventory is extremely useful in mapping out and categorizing components of a project, as well as assigning and documenting risk associated with each asset. Once completed, system operators can focus on the assets that are most at risk. Also, consider cloud assets and accounts (such as domain registration, project social media accounts, etc) as part of your inventory.
Resources: Trusted CI Information Asset Inventory Template, Trusted CI Risk Assessment Table, i-doit, Snipe-IT, CIS Controls #1

O. Use institutional resources 5 11 14

Strengthen security by utilizing the cybersecurity of general or centralized IT resources provided by the gateway project's affiliated institution. Most institutions provide these services by default, especially for small projects.
Resources: Consult with the home institution's security staff and involve them as needed.

No doubt cybersecurity will continue to be an ongoing challenge for science gateways and the research community. Trusted CI and SGCI hope these recommendations will provide direction as teams work to mitigate risk. Please contact Trusted CI at ask@trustedci.org for further questions and advice.

About Trusted CI

As the National Science Foundation Cybersecurity Center of Excellence, Trusted CI draws on expertise from multiple internationally recognized institutions, including Indiana University, the University of Illinois, the University of Wisconsin-Madison, the Pittsburgh Supercomputing Center and Berkeley Lab. Drawing on this expertise, Trusted CI collaborates with NSF-funded research organizations to focus on addressing the unique cybersecurity challenges faced by such entities. In addition to our leadership team, a world-class Advisory Committee adds its experience and a critical eye to the center's strategic decision-making. Trusted CI, the NSF Cybersecurity Center of Excellence is supported by the National Science Foundation under Grant #1920430. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

About SGCI

The Science Gateways Community Institute (SGCI), funded by the NSF, provides resources, expertise, community support, and education to the creators of gateways serving science and engineering research and education. Through these channels, SGCI has grown a community around developing and applying science gateways across multiple domain areas. SGCI actively partners with science gateway teams and contributes development expertise, sustainability services, usability analysis, and more. Through SGCI's partnership with Trusted CI, science gateway teams also receive cybersecurity consulting. SGCI is funded by the National Science Foundation under award number ACI-1547611. 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.