ScienceLogic Security Posture

How ScienceLogic Ensures a Secure Hybrid IT Monitoring Platform

ScienceLogic understands that a strong security posture, one that is regularly updated and tested against, is a requirement for today's enterprises, government agencies, and managed service providers. ScienceLogic is committed to ensuring our platform delivers on this posture by routinely conducting internally-administered penetration tests using industry-standard tools and practices as well as annually contracting with an independent certification organization to perform penetration testing. Findings from these tests are considered in priority and severity order for inclusion in upcoming software releases.

Internal Penetration Testing

The ScienceLogic Quality Assurance team uses a variety of scanning tools such as Nessus and Burp to detect vulnerabilities in the user interface and platform. The team specifically looks for the OWASP Top Ten Vulnerabilities. The programing level items (Various XSS, SQL injection, broken authentication, session management, etc.) listed in the Top Ten are evaluated using Portwigger's Burp. ScienceLogic validates the Top Ten Security Configurations using the most current version of Nessus. Items such as validating functional level access controls and updating modules with known vulnerabilities are currently checked in both manual and automated fashion.

The purpose of internal penetration testing is twofold:

- Ensure no vulnerabilities have accidently been introduced into the ScienceLogic platform
- Prepare for external penetration testing

External Penetration Testing

ScienceLogic regularly contracts with independent, accredited organizations that are recognized as authorities in security testing, such as 7Safe and Illumant. These companies conduct annual tests on current and upcoming ScienceLogic platform releases with the intent of constantly increasing our security posture in response to the expanding set of known vulnerabilities identified by industry experts.

ScienceLogic has contracted with companies in both the U.S. and U.K. in order to achieve a global perspective on the evolving security landscape. These companies conduct thorough scans of the ScienceLogic platform with a suite of commercially-available tools (Burp, Nessus, Nikto, Nexpose, Netsparker), as well as proprietary test methods. If an exploit is found, they exercise it to the maximum extent possible. The results are then shared with ScienceLogic so that changes can be made.

To offer complete transparency, ScienceLogic can provide customers with results of these external penetration tests under non-disclosure agreement, upon request.

In addition, ScienceLogic customers with specific security obligations sometimes perform additional penetration tests tailored to their unique requirements. These companies report their findings back to ScienceLogic's security team for consideration.

DoDIN APL

ScienceLogic is named on the U.S. Department of Defense Information Network (DoDIN) Approved Products List (APL). ScienceLogic was the first and only end-to-end IT infrastructure monitoring company ever to conform to the DoD's rigorous security and interoperability standards. As part of the APL agreement, ScienceLogic complies with the request for timely patching of issues to maintain the operational availability, confidentiality, and integrity of our customers' systems. To accomplish this, we work with customers to address any critical security issues within 24 hours, and important issues within one business week.

FIPS 140-2 Compliant Cryptography

Products that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information must be certified for use in U.S. government departments and regulated industries (such as financial and health-care institutions).

Federal Information Processing Standards (FIPS) are the criteria and guidelines for information processing developed by NIST and approved by the Secretary of Commerce as requirements for the federal government for information assurance and interoperability.

The ScienceLogic platform uses FIPS 140-2 compliant cryptography methods for data encryption and communication between appliances and storing of passwords.

In summary, ScienceLogic dedicates itself to providing customers with the most secure monitoring platform possible. The underlying operating system is completely locked down and all communication is fully encrypted. ScienceLogic is deployed in some of the most secure networks throughout government and commercial sectors. Regular internal and external testing ensures the platform complies with the highest of current security standards.

About ScienceLogic

The ScienceLogic SL1 platform enables companies to digitally transform themselves by removing the difficulty of managing complex, distributed IT services. We use patented discovery techniques to find everything in your network, so you get visibility across all technologies and vendors running anywhere in your data centers or clouds.

The power of our solution is that we collect and analyze millions of data points across your IT universe to help you make sense of it all. We automatically provide a complete inventory, track dynamic relationships between technologies, notify you about issues needing immediate attention, and enable you to initiate corrective actions – all in real-time. We also collaborate with you to integrate the platform with the rest of your IT management ecosystem so you can share data and automate your IT processes.