

UNCLASSIFIED



BROMIUM SECURE PLATFORM 4.x SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

10 May 2018

Developed by Bromium and DISA for the DoD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Executive Summary	1
1.2 Authority	1
1.3 Vulnerability Severity Category Code Definitions	2
1.4 STIG Distribution.....	2
1.5 SRG Compliance Reporting.....	2
1.6 Document Revisions	2
1.7 Other Considerations	2
1.8 Product Approval Disclaimer.....	3
2. ASSESSMENT	4
2.1 Security Assessment Information	4
3. TECHNICAL OVERVIEW.....	5
3.1 Bromium Micro-Virtualization Technology	5
3.2 Components and Ports.....	6
3.3 Compatibility with HBSS and Other Endpoint Security Software	7
3.4 Audit Logging	7

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2

LIST OF FIGURES

	Page
Figure 3-1: Bromium Port and Protocols.....	6

1. INTRODUCTION

1.1 Executive Summary

The Bromium Secure Platform 4.x Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the Bromium Secure Platform 4.0. This document provides requirements to secure the functionality of both the Bromium Enterprise Controller (BEC) installed on a Windows server and the Bromium vSentry client installed on an endpoint. The Bromium Threat Cloud Service is out of scope for this STIG.

The Bromium Secure Platform provides virtualization-based application isolation and containment for endpoint protection. Each application is run in a micro-virtual machine (micro-VM) that provides containment for malicious code, malware, and threats. The product does not prevent installation of an unauthorized application but rather allows it to be installed in a micro-VM and run in isolation. This isolation allows the product to collect threat information that can be aggregated by a central events analysis tool and leveraged to protect other devices. When the micro-VM is closed, the threat is eliminated without contaminating other processes and applications on the endpoint. Note that micro-VMs do not have direct network or printer access. The administrator may also opt to use Bromium to restrict access to unauthorized executables, but this function must also be configured with the guidance provided in the Bromium Secure Platform 4.x STIG.

Other endpoint security products such as HBSS do not have visibility into the micro-VMs when installed on the Bromium vSentry client. However, the HBSS client may be installed on the same endpoint.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that “all IT that receives, processes, stores, displays, or transmits DoD information will be [...] configured [...] consistent with applicable DoD cybersecurity policies, standards, and architectures” and tasks that Defense Information Systems Agency (DISA) “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is <http://iase.disa.mil/>.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<http://www.niap-ccevs.org/>) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<http://csrc.nist.gov/groups/STM/cmvp/>) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (<http://www.disa.mil/network-services/ucco>) IAW DoDI 8100.04

2. ASSESSMENT

2.1 Security Assessment Information

A security assessment of the Bromium Secure Platform must consist of a review of the application itself as well as the functions provided by the application. Both the BEC host server and Bromium vSentry endpoint hosts must also be inspected using the appropriate operating system STIG. Since some of the log files are stored in a database, the SQL database used must also be reviewed.

3. TECHNICAL OVERVIEW

The Bromium Secure Platform provides protection at the endpoint against advanced malware. Bromium automatically creates hardware-isolated micro-VMs that secure user tasks (e.g., visiting a web page, downloading a document, or opening an email attachment). Each task runs in its own micro-VM, and all micro-VMs are separated from each other and from the trusted enterprise network. If malware targets the end user, the threat is contained in the hardware-isolated micro-VM. Thus, the attack does not impact the endpoint or the network and is destroyed when the micro-VM is closed. Bromium is intended to be transparent to the end user and is designed to have no discernible impact on user experience or system performance.

The Bromium Secure Platform 4.x STIG contains requirements for securing the two major components of the Bromium Secure Platform: the Bromium vSentry client and the BEC. The Bromium vSentry client includes the Bromium Monitoring Module, which performs detection for malicious activity at the application layer, registry layer, files, and network layer. Bromium is meant to isolate and prevent the most common threat vectors, including web browsing, Internet downloads, email attachments, and USB thumb drives. Through hardware isolation of each untrusted activity, Bromium prevents against spear phishing attacks, ransomware, kernel exploits, zero-day attacks, and advanced persistent threats (APTs).

Additionally, detection of malicious code in the micro-VM on one endpoint can be leveraged to monitor endpoints across the enterprise to detect a wide-scale attack. Upon detection of malicious code on one endpoint, the Bromium Monitoring Module can be configured to inventory all executables involved in the attack and send that inventory to the BEC in the form of hashes. The BEC uses these hashes to detect and notify security personnel if the executables are found on other endpoints in the enterprise. Note that it is also possible to configure policies that restrict access to known, unauthorized executables.

3.1 Bromium Micro-Virtualization Technology

Bromium micro-VM technology uses the Bromium Microvisor, a purpose-built, Xen-based, security-focused hypervisor, in conjunction with the VT features built into IntelR, AMDR, and other CPUs to create hardware-isolated micro-VMs for each task a user performs on information originating from unknown sources. These hardware-isolated micro-VMs provide a secure environment where user tasks are isolated from one another, the protected system, and the network to which it is attached.

A task is composed of all computations, both within an application and within the kernel, that are required to complete a particular user-initiated activity (e.g., opening a single web browser tab or a PDF document is considered an individual task). Bromium applies the principle of least privilege to each task, granting access to only the specific resources that are needed to complete the particular task: files, network services, the clipboard, interaction with the user, devices, or network shares.

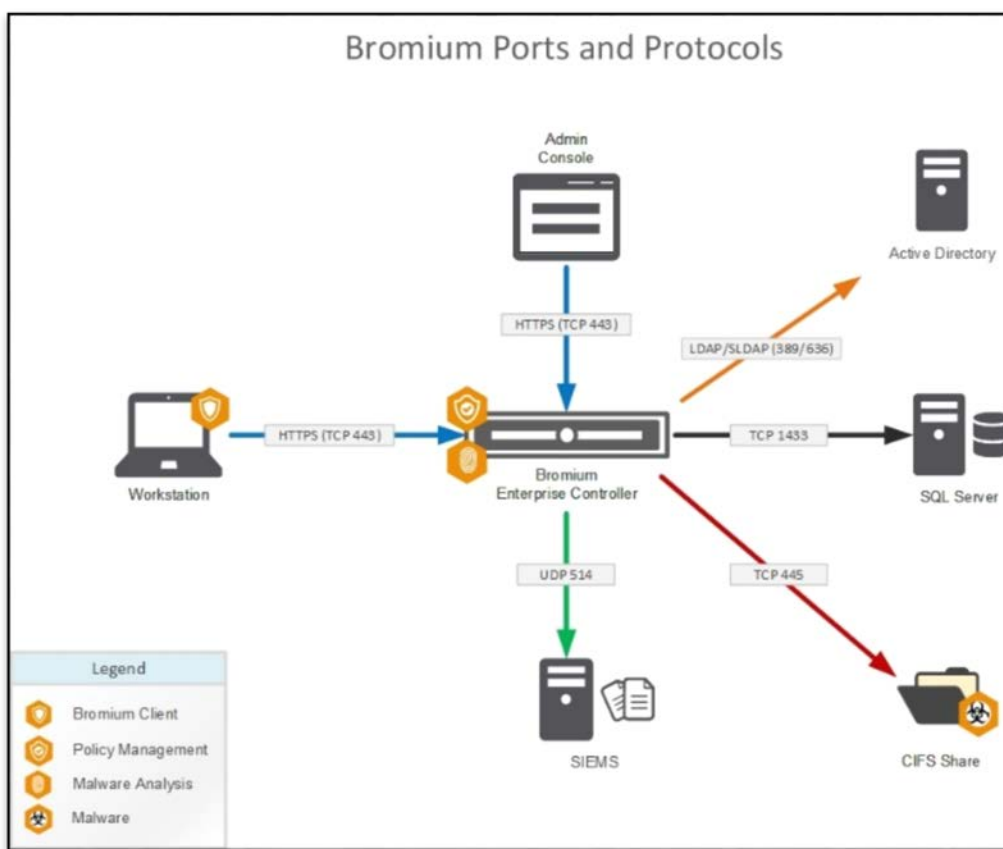
The Bromium Monitoring Module provides a view of tasks running within a micro-VM. This provides a view of the attack as it happens and can detect attacks targeted below the operating system, such as rootkits and bootkits. Each endpoint updates the BEC with threat detection

information; therefore, information about the vector, target, and methods used by an attacker and full details of the attack are preserved, including network traffic, file signatures, and all changes that malware attempted to make to the operating system or file system. Thus, the BEC threat database contains information about memory exploits, execution of new tasks, attempts to download and save files, and attempts by malware to connect to external command-and-control systems to support security analysis and incident reports.

3.2 Components and Ports

The information in this section is provided to help ensure all components and dependencies are considered during the security review. Figure 3.1 below shows the high-level Bromium Secure Platform components and architecture. Ports used for communications between components are also included in Figure 3.1 for use in restricting unneeded ports. Components include the BEC, the Bromium vSentry Client, and the integration points with existing infrastructure such as SQL servers, security information and event management (SIEM), and common Internet file system (CIFS) shares.

Figure 3-1: Bromium Port and Protocols



The BEC consists of Bromium Dashboard components loaded onto IIS and hosted on a Windows Server. The BEC requires two Microsoft components: IIS and SQL Server. The BEC can be installed on Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2,

and Windows Server 2016. The BEC requires Microsoft IIS 7.5 or later with the Common Gateway Interface (CGI) module installed and .NET 4 Extended. The BEC requires a back-end SQL server to store configuration and alert data. Bromium supports the following versions of SQL: SQL Server 2008 R2 64-bit, SQL Server 2012, SQL Server 2014, and SQL Server 2016.

If multiple Bromium Controllers are used, a Common Internet File System (CIFS) share should be leveraged to store the detailed Bromium threat data so the data can be read/updated by each of the management servers.

3.3 Compatibility with HBSS and Other Endpoint Security Software

DoD mandates the use of endpoint security protections such as Host Intrusion Prevention System (HIPS) and anti-virus software. These products may interfere with or prevent the normal operation of Bromium isolation. Necessary actions may consist of excluding or whitelisting all isolation processes and binaries from the endpoint security product. To create exclusions, refer to the third-party product documentation. The absence of exclusions may result in failed isolation initialization or slow or blocked applications.

DoD requires the use of Host Based Security System (HBSS) for endpoint security on all endpoints. The Bromium Protection agent is part of the Bromium Secure Platform and is also a HIPS product. However, it is not installed by default. The Bromium Protection agent does not meet DoD requirements for HIPS, and thus cannot be used instead of HBSS. Furthermore, the Bromium Protection agent does not provide signature-based anti-virus or IDPS functions. Since the agent is compatible with HBSS and can be run at the same time, use of the agent in addition to HBSS is allowed but not necessary.

HBSS injects into the running process on the endpoint and can significantly degrade the performance of Bromium's isolation process. To mitigate this performance risk, HBSS must be configured to use a whitelist that includes exclusions for each of the Bromium processes listed in the "McAfee Virus Scan/HIPS" section of the Bromium Security Platform Deployment Guide.

Organizations must obtain approval for file exceptions to HIPS and other endpoint security software from the ISSO, ISSM, AO, or other approving authority.

3.4 Audit Logging

The system log is kept on the BEC management server in a file named "history.log". This log contains log records for administrative events such as user privilege changes or changes to the BEC configuration. The Bromium Secure Platform 4.x STIG provides guidance for explicitly configuring a backup agent to enable the capability to send "history.log" events to the central log server. Because the "history.log" file is on a Windows server, the syslog protocol will not natively be able to listen to changes made to the "history.log" file.

The endpoint activity log contains events of threats and monitored activity on the Bromium vSentry endpoint and is stored in a SQL database rather than on the BEC server. A third-party backup agent must be provided to ensure this log is sent to the central log server.