National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Exabeam Security Management Platform

Report Number: CCEVS-VR-VID10923-2019
Version 1.0
September 4, 2019

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers, Senior Validator
Aerospace Corporation

Meredith Hennan, Lead Validator
Aerospace Corporation

Common Criteria Testing Laboratory

Chris Gugel
Herbert Markle
Alex Massi
Christopher Rakaczky
Courtney Simon

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Security Management Platform provided by Exabeam, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in August 2019. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314* (NDcPP).

The Target of Evaluation (TOE) is the Exabeam Security Management Platform, running the software version Core (PLT-i10). The Security Management Platform 's primary functionality is to collect network traffic and events, correlate the data collected to detect threats, and provide recommendations for responses to safeguard the network against cyberattacks. The SMP model with the Data Lake software provides the capability to collect the network traffic and events and will send that data to the other TOE component over TLS for threat detection and response recommendation. The SMP model receiving the collected events has the Advanced Analytics software which will detect threats and the Incident Responder software that will create response actions that the network administrator can perform to mitigate the threat. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDcPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the NDcPP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Exabeam Security Management Platform Security Target v1.0*, dated July 26, 2019 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Exabeam Security Management Platform, running software version Core (PLT-i10) Refer to Table 2 for Model Specifications
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	Exabeam Security Management Platform Security Target v1.0, dated July 26, 2019
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Exabeam Security Management Platform" Evaluation Technical Report v1.0 dated August 5, 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Exabeam, Inc.
Developer	Exabeam, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Jerome Myers, Senior Validator - Aerospace Corporation Meredith Hennan, Lead Validator - Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.
- It is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack against a TOE component and that auditing is functioning on all TOE components.
- TOE Administrators are trusted to ensure that there is no unauthorized access possible for sensitive residual information on the TOE when it is removed from its operational environment.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.UNAUTHORIZED_ADMINISTRATOR_ACCESS** – Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
- **T.WEAK_CRYPTOGRAPHY –** Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
- **T.UNTRUSTED_COMMUNICATION_CHANNELS** – Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
- **T.WEAK_AUTHENTICATION_ENDPOINTS –** Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the

Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

- **T.UPDATE_COMPROMISE –** Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
- **T.UNDETECTED_ACTIVITY** – Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
- **T.SECURITY_FUNCTIONALITY_COMPROMISE –** Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
- **T.PASSWORD_CRACKING –** Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
- **T.SECURITY_FUNCTIONALITY_FAILURE –** An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314*, 14 March 2018, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the Security Management Platform's capabilities to collect

network traffic and events, correlate the data collected to detect threats, and provide recommendations for responses to safeguard the network against cyberattacks described in Section 1.3 of the Security Target were not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

The evaluated configuration of the TOE is the EX3000 and EX4000 described in Table 2 running the software version Core (PLT-i10). In the evaluated configuration, the TOE uses TLS/HTTPS to secure remote web-based administration, SSH to secure remote command-line administration. and TLS to secure transmissions of security-relevant data from the TOE to an external syslog server. The TOE includes administrative guidance in order to instruct Security Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The TOE is a network device as defined in the NDcPP which states: "This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device… A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network." The TOE consists of the EX3000 and EX4000 models as TOE components, running the software version Core (PLT-i10). Thus, the TOE is a network device composed of hardware and software.

4.2 Physical Boundary

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

Model Number	EX3000	EX4000
Size	1 RU	1 RU
Power	AC	AC
Processor	Intel Xeon E5-2620	Intel Xeon E5-2690
Memory (RAM)	192GB DDR4 2666MHz (6 x 32GB)	256GB DDR4 2400MHz (8 x 32GB)
Storage	• 9x Seagate EC3.5v5 4TB SATA 512E 6Gbps SATA3 7200rpm 128MB 3.5i • 2x Samsung PM863a 1.92TB SSD • 1x Intel S4500 240GB SSD • Maximum Storage Capacity: 35.6TiB • Maximum Usable Capacity: 27.5TiB	• 1x Intel S3500 150GB SSD • 3x Samsung PM863A 960GB SSD • 6x Seagate EC2.5 2TB HDD

Table 2 – Hardware

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Component	Definition
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. For the TOE to be managed remotely the management workstation is required to have: • Browser to access the TOE's GUI • SSHv2 client to access the TOE's secure shell command-line interface The TOE's secure shell command line interface can also be accessed locally with a physical connection to the TOE using a keyboard and monitor.
Syslog Server	The TOE connects to a syslog server to send syslog messages for remote storage via TLS connection where the TOE is the TLS client. This is used

	to send copies of audit data to be stored in a remote location for data redundancy purposes.
OCSP Responder	A server deployed within the Operational Environment which confirms the validity and revocation status of certificates.

Table 5 – IT Environment Components

5 Security Policy

5.1.1 Security Audit

Audit records are generated on each model for various types of management activities and events that occur on that model. These records include the date and time stamp of the event, the event type, and the subject identity. Audit records are stored in rsysreceived.log on each TOE model and can be configured to also be sent to a syslog server via a TLS connection. When the storage space allocated to rsysreceived.log is exhausted, the model will delete the oldest log file, archive the previous active file, and generate a new active file to which audit records are written.

5.1.2 Cryptographic Support

Each TOE model provides cryptography in support of communications between itself and the Operational Environment. The protocols used for this are TLS, HTTPS, and SSH. The TOE uses TLS to secure the automatic transfer of syslog audit records. TLS/HTTPS is used to secure the connection for remote management of the TOE via the GUI and SSH is used to secure the remote CLI interface for remote management of the TOE. TLS mutual authentication is used for communication between TOE components.

Exabeam's implementation of these has been validated to ensure that the algorithms are appropriately strong for use in trusted communications. The TOE collects entropy from sources contained within the device to ensure sufficient randomness for secure key generation.

Cryptographic keys are generated using the CTR_DRBG provided through this module and the references to the keys are destroyed when no longer needed.

The following table lists the CAVP algorithm certificates for the OpenSSL 6.0 cryptographic module:

SFR	Algorithm/Protocol	OpenSSL CAVP Cert #
FCS_CKM.1	RSA FIPS 186-4 Key Generation	2786
FCS_CKM.1	DSA FIPS 186-4 Key Generation for Diffie-Hellman FFC	1346
FCS_CKM.2	FFC Key Establishment 2048 bits (CVL)	1687
FCS_COP.1/ DataEncryption	AES-128-CBC, AES-256-CBC, AES-256-GCM, AES-256-CTR	5203
FCS_COP.1/ SigGen	RSA FIPS 186-4 Signature Generation and Signature Verification	2786
FCS_COP.1/Hash	SHA-1, SHA-256, SHA-384, SHA-512	4193
FCS_COP.1/KeyedHash	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	3445
FCS_RBG_EXT.1	CTR_DRBG (AES)	1975

Table 6 – Cryptographic Algorithm Table

5.1.3 Identification and Authentication

Each TOE model provides a local password authentication mechanism for the GUI, local CLI, and remote CLI that obscures password upon entry. Users accessing the remote CLI on each model can also authenticate using their SSH public key. The TOE models also enforce password

length requirements and will lock users out due to too many failed authentication attempts. The only function available to an unauthenticated user is the ability to acknowledge a warning banner.

The TOE uses X.509 certificates to authenticate servers that it connects to over TLS. This includes each model connecting to the syslog server as well as EX3000 and EX4000 verifying the other TOE component's X.509 certificates when they communicate. The TSF determines the validity of the certificates by confirming the validity of the certificate chain and verifying that the certificate chain ends in a trusted Certificate Authority (CA). The TSF connects with an OCSP Responder through HTTP to confirm certificate validity and revocation. The TSF can generate a Certificate Request that contains the "Common Name" and public key.

5.1.4 Security Management

Each model of the TOE can be administered locally and remotely and uses role based access control (RBAC) to restrict privileges to authorized roles. The Security Administrator roles on the CLI are the "Exabeam user" role and the root account (can authenticate via the local CLI only). For the GUI, users with the "Administrator" role are considered the Security Administrators.

5.1.5 Protection of the TSF

The TOE stores passwords in a variety of locations on each model depending on their use and encryption. They cannot be viewed by any user regardless of the user's role. Additionally, pre-shared keys, symmetric keys, and private keys cannot be accessed in plaintext form by any user. There is an underlying hardware clock on each model that is used for accurate timekeeping and is set by the Security Administrator. Power-on self-tests are executed automatically on each TOE model during the boot process which includes verifying the TOE software's and cryptographic module's integrity. The TOE's DRBG also performs its own health tests.

The version of the software installed on each model is verified via the GUI. The Exabeam user will SCP push (over SSH) the software package from their management workstation to each TOE component and then will run the commands to update the TOE component's software. The software update process includes two different verifications of a SHA-256 public hash.

5.1.6 TOE Access

The TOE models display a configurable warning banner on each user interface prior to the user authenticating to that interface. The TOE components can terminate local CLI, remote CLI, and GUI sessions after a specified time period of inactivity. Administrator users have the capability to terminate their own sessions. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

5.1.7 Trusted Path/Channels

The TOE components connect and send data to IT entities via trusted channels. In the evaluated configuration, each model connects to a syslog server via TLS to send audit data for remote storage. TLS is used for the transfer of collected network event data from EX3000 to EX4000. TLS/HTTPS and SSH are used for remote administration of the TOE via the GUI and remote CLI respectively.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Exabeam Security Management Platform Supplemental Administrative Guidance for Common Criteria v1.0
- Exabeam Appliance Setup Guide Gen 2 EX2000 & EX4000
- Exabeam Appliance Setup Guide EX3000

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the EX3000 communicating with the EX4000 as a combined TOE, running the software version Core (PLT-i10). Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, each TOE component is configured to communicate with the following environment components:

- Management Workstation for local and remote administration
- Syslog Server for recording of audit data
- OCSP Responder for confirming the validity and revocation status of certificates

To use the product in the evaluated configuration, the product must be configured as specified in the *Exabeam Security Management Platform Supplemental Administrative Guidance for Common Criteria Version 1.0* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Assurance Activity Report for a Target of Evaluation "Exabeam Security Management Platform" Assurance Activities Report v1.0* dated August 5, 2019.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *Exabeam Security Management Platform Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network. Testing was performed against all three management interfaces defined in the ST (local CLI, remote CLI, and GUI).

The TOE was configured to communicate with the following environment components:

- The platform used for the Syslog server was Linux 4.9.0-3-amd64 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) x86_64.
    - Syslog Server for recording of syslog data (rsyslogd 8.24.0)
- The platform used for the OCSP Responder was Linux 3.16.0-4-amd64 #1 SMP Debian 3.16.51-3 (2017-12-13) x86_64 GNU/Linux.
    - OCSP Responder for responding to validity requests (OpenSSL 1.0.1t)
- Management Workstation for local and remote administration:
    - Debian VM (Linux 3.16.0-4-amd64 #1 SMP Debian 3.16.51-3 (2017-12-13) x86_64 GNU/Linux)
        - Tcpdump: version 4.9.2
        - Libpcap version 1.8.1
        - OpenSSL version 1.0.2r
    - HP EliteBook Laptop with Windows 10
        - WireShark: version 2.6.4
        - Firefox Quantum: version 68.0.1
        - Internet Explorer: version 11.726.16299.0
        - Google Chrome: version 75.0.3770.142
        - PuTTY SSH Client: version .70
    - Kali VM (Linux 4.15.0-kali2-amd64 #1 SMP Debian 4.15.11-1kali1 (2018-03-21) x86_64 GNU/Linux)
        - Tcpdump: version 4.9.2
        - Libpcap version 1.8.1
        - OpenSSL version 1.0.2k
    - Dell Precision M4800 Laptop dual boot setup with Windows 10 and Debian Linux 3.16.51-3
        - WireShark: version 2.6.2
        - Bitvise SSH Client: version 7.31
        - PuTTY .70
        - nmap: version 7.70
        - Nessus Professional: version 7.1.3 (#120) LINUX
        - Burp Suite Professional: version 1.7.36
        - Firefox Quantum: version 61.0.2
        - Metasploit stable release 4.14

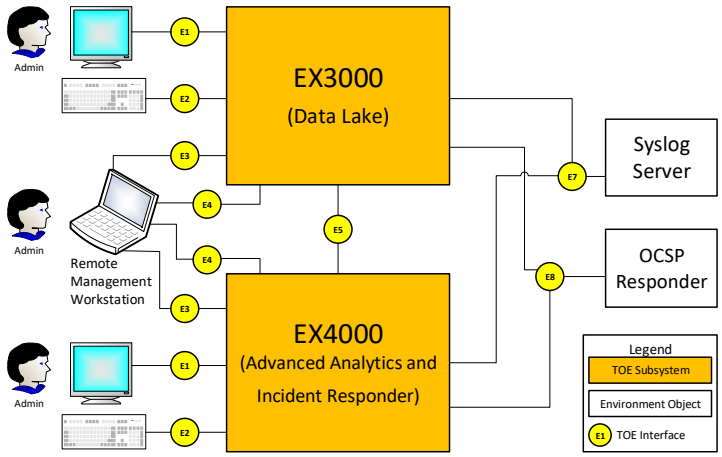

Figure 1 - Test Configuration

8.2 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the NDcPP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
Exabeam	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
Security Management Platform	This is a generic term for searching for Security Management Platform.
SMP	This is a generic term for searching for Security Management Platform.

Keyword	Description
EX3000	This is a generic term for searching for known vulnerabilities for specific model of the specific product line.
EX4000	This is a generic term for searching for known vulnerabilities for specific model of the specific product line.
CentOS (7.6)	This is a generic term for searching for known vulnerabilities for the underlying TOE operating system. Version used for filtering results.
OpenSSL (1.0.2r)	This is a generic term for searching for known vulnerabilities for the underlying TOE cryptographic module. Version used for filtering results.
OpenSSH (7.4p1-16)	This is a generic term for searching for known vulnerabilities for the TOE SSH server. Version used for filtering results.
stunnel (5.49)	This is a generic term for searching for known vulnerabilities for the stunnel software. Version used for filtering results.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources on August 4, 2019. The following public vulnerability sources were searched:

- NIST National Vulnerabilities: https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- SecurITeam Exploit Search: www.securiteam.com
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.

- Web Interface Vulnerability Identification (Burp Suite)
  The Web Interface vulnerability scan: This scan was the primary emphasis on the penetration testing for both automated scanning and manual attempts and was meant to look for OWASP Top 10 vulnerabilities. Attempted to scan all open ports found by the port scan.

- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by exploiting a vulnerability in OpenSSH as described in CVE-2018-15473.

- Force SSHv1
  This attack determines if the client will accept both SSHv1 and SSHv2 connections when the TOE claims to only support SSHv2.

- Remote Network Scan (Nessus)
  This attack attempts to detect known vulnerabilities against the platform (and discovered software) connected to the network. The vulnerability scan will produce a prioritized list of vulnerabilities and possible remediation procedures.

- Additional tests were run around potential exploits

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Security Management Platform product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work units. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Exabeam Security Management Platform Supplemental Administrative Guidance for Common Criteria Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Exabeam Security Management Platform Security Target v1.0*, dated July 26, 2019.

13 List of Acronyms

Acronym	Definition
CA	Certificate Authority
CC	Common Criteria
CLI	Command-line Interface
CN	Common Name
CRNGT	Continuous Random Number Generator Test
CPU	Central Processing Unit
CVL	Component Validation List
DSS	Digital Signature Standard
DN	Distinguished Name
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
NDcPP	collaborative Protection Profile for Network Devices, version 2.0 + Errata 20180314
NIAP	National Information Assurance Partnership
OCSP	Online Certificate Status Protocol
OS	Operating System
POST	Power-On Self Test
PP	Protection Profile
PKCS	Public-Key Cryptography Standards
RBAC	Role Based Access Control
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMP	Security Management Platform
SSL	Secure Sockets Layer
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

14 Terminology

Term	Definition
Security Administrator	The claimed Protection Profile defines a Security Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be the Exabeam user for the local or remote CLI, the root user for the local CLI, and any user with the permissions provided to the 'Administrator' role for the GUI.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018
6. Exabeam Security Management Platform Security Target v1.0, dated July 26, 2019
7. Exabeam Security Management Platform Supplemental Administrative Guidance for Common Criteria Version 1.0
8. Exabeam Appliance Setup Guide Gen 2 EX2000 & EX4000
9. Exabeam Appliance Setup Guide EX3000
10. Assurance Activity Report for a Target of Evaluation "Exabeam Security Management Platform" Assurance Activities Report v1.0 dated August 5, 2019
11. Evaluation Technical Report for a Target of Evaluation "Exabeam Security Management Platform" Evaluation Technical Report v1.0 dated August 5, 2019