Estate Valuations & Pricing Systems, Inc.
Intrusion Detection and Audit Process

Overview

This document defines Estate Valuations & Pricing Systems, Inc.'s process and policy for the detection and response to unauthorized intrusion into its computer systems. An audit of access logs is performed once a month by EVP's technical staff, with automated systems scanning for breaches on an on-going basis. In the event of an intrusion, quarantine measures are put into place and all affected clients are informed per the company's "Security Incident Response Policy."

Data Center Systems

EVP Systems maintains its data center as part of the Amazon Web Services infrastructure. (See "Disaster Recovery and Business Continuity" for more details.)

The servers use the Canonical Ubuntu operating system. Password-based logins on each production machine are disabled, and access is granted only via a closely-held private key.

Several standard system logs track access to and usage of these machines, including: `auth.log`, `boot.log`, `kern.log`, `syslog` and `lastlog`. For machines that run the Apache webserver, additional logs include: `error.log` and `access.log`. For machines that run the Tomcat webserver, additional logs include: `catalina.out`. Each of these logs are collected off-site via the Papertrail (`www.papertrailapp.com`) service, and are aggregated into a single, searchable database.

Dozens of automated searches are run on each new log-line that is sent to Papertrail, and e-mail, SMS and Slack alerts are sent to the technical staff if irregularities are found, including but not limited to:

- Off-hours access
- Access from unknown IPs
- Badly formatted packets
- Creation of new users or groups
- High volume connections from unknown IPs
- Badly formatted HTTP requests

The root-kit detector `rkhunter` (with the `unhide` extension) is run on each machine nightly, and the results are sent to Papertrail, with exceptions included in the automated searches.

The log-analyzer `fail2ban` is run on each machine, to temporarily ban IP addresses that attempt to log in repeatedly, reducing log noise and discouraging script-based attackers. (The servers themselves do not use password-based authentication.)

On the first Saturday of the month, the Papertrail logs are also reviewed by a member of EVP Systems' technical staff, for new or unexpected activity. Modifications to the automated searches are made as appropriate.

Desktop Systems

EVP Systems uses the Windows 10 and 11 operating systems, for both office administration, and development and testing. Older and newer versions of Windows are used in isolation for testing.

Each machine on the EVP Systems LAN in both the Santa Barbara and Woodland Hills offices run Windows Definenter antivirus to prevent the installation of backdoors and remote exploits, with the virus signature file updated nightly.

On the first Saturday of the month, the standard Windows Event Log is reviewed by a member of EVP Systems' technical staff, for unexpected activity.

Third-Party Services

EVP Systems uses several third-party services in the course of its business: Google Workspace for e-mail and shared documents, Dropbox for file storage, GitHub for source code configuration management and revision history, Papertrail for log aggregation, Uptime Robot for uptime monitoring, Slack for intra-office communication, among others.

Each of these services provides different levels of account-access review. Where appropriate, two-factor authentication (2FA) has been enabled, as well as first-time access alerts. Individual accounts are isolated from each other via individual security measures, including unique passwords and 2FA phone numbers.

Unauthorized Access Response

In the event that unauthorized access is discovered, EVP Systems will take steps to quarantine the affected systems, repair or replace them as appropriate, and notify clients per the company's "Security Incident Response Policy."

If the breach is to a data center system, it will be taken off-line immediately and all server processes shut down, isolating the system from the public Internet. A new instance will be built from scratch to replace the affected system, and then a forensic analysis of the breach will be performed by EVP Systems' technical staff. Additions will be made to the automated searches if possible, and the attack vector will be addressed to prevent a recurrence. (Please see "Internet Vulnerability Responses" for a history of preventive measures taken to repair data center systems before breaches.)

If the breach is to a desktop system, it will be taken off-line immediately and the computer itself will be replaced, with software being re-installed from original sources. A forensic analysis will then be performed by a member of EVP Systems' technical staff, and countermeasures updated accordingly.

If the breach is to a third-party system, the affected account will have its password changed and other security measures reset. Data in the account will be reviewed for changes and any available audit logs provided by the vendor will be used to determine the source of the access.

In all cases, EVP Systems will seek criminal prosecution of anyone breaching its systems.

It is important to note that EVP Systems does not have access to client's personally identifiable information (PII), so it cannot be compromised by a breach of EVP Systems' computers.

Staff Education

Once a year, all members of the EVP Systems staff will receive training on proper security practices.

Audit History

Manual audits were performed on the follow dates:

May 1, 2016	Complete; no intrusions detected (Audit: GK)
June 4, 2016	Complete; no intrusions detected (Audit: GK)
July 2, 2016	Complete; no intrusions detected (Audit: GK)
August 6, 2016	Complete; no intrusions detected (Audit: GK)
September 3, 2016	Complete; no intrusions detected (Audit: GK)
October 1, 2016	Complete; no intrusions detected (Audit: GK)
November 5, 2016	Complete; no intrusions detected (Audit: GK)
December 3, 2016	Complete; no intrusions detected (Audit: GK)
January 7, 2017	Complete; no intrusions detected (Audit: GK)
February 4, 2017	Complete; no intrusions detected (Audit: GK)
March 4, 2017	Complete; no intrusions detected (Audit: GK)

April 1, 2017	Complete; no intrusions detected (Audit: GK)
May 6, 2017	Complete; no intrusions detected (Audit: GK)
June 3, 2017	Complete; no intrusions detected (Audit: GK)
July 1, 2017	Complete; no intrusions detected (Audit: GK)
August 5, 2017	Complete; no intrusions detected (Audit: GK)
September 2, 2017	Complete; no intrusions detected (Audit: GK)
October 7, 2017	Complete; no intrusions detected (Audit: GK)
November 4, 2017	Complete; no intrusions detected (Audit: GK)
December 2, 2017	Complete; no intrusions detected (Audit: GK)
January 6, 2018	Complete; no intrusions detected (Audit: GK)
February 3, 2018	Complete; no intrusions detected (Audit: GK)
March 3, 2018	Complete; no intrusions detected (Audit: GK)
April 7, 2018	Complete; no intrusions detected (Audit: GK)
May 5, 2018	Complete; no intrusions detected (Audit: GK)
June 2, 2018	Complete; no intrusions detected (Audit: GK)
July 7, 2018	Complete; no intrusions detected (Audit: GK)
August 4, 2018	Complete; no intrusions detected (Audit: GK)
September 1, 2018	Complete; no intrusions detected (Audit: GK)
October 6, 2018	Complete; no intrusions detected (Audit: GK)
November 5, 2018	Complete; no intrusions detected (Audit: GK)
December 3, 2018	Complete; no intrusions detected (Audit: GK)
January 5, 2019	Complete; no intrusions detected (Audit: GK)
February 2, 2019	Complete; no intrusions detected (Audit: GK)
March 2, 2019	Complete; no intrusions detected (Audit: GK)
April 6, 2019	Complete; no intrusions detected (Audit: GK)
May 4, 2019	Complete; no intrusions detected (Audit: GK)
June 1, 2019	Complete; no intrusions detected (Audit: GK)
July 6, 2019	Complete; no intrusions detected (Audit: GK)
August 4, 2019	Complete; no intrusions detected (Audit: GK)
September 7, 2019	Complete; no intrusions detected (Audit: GK)
October 5, 2019	Complete; no intrusions detected (Audit: GK)
November 2, 2019	Complete; no intrusions detected (Audit: GK)
December 7, 2019	Complete; no intrusions detected (Audit: GK)
January 4, 2020	Complete; no intrusions detected (Audit: GK)
February 1, 2020	Complete; no intrusions detected (Audit: GK)
March 7, 2020	Complete; no intrusions detected (Audit: GK)
April 4, 2020	Complete; no intrusions detected (Audit: GK)
May 2, 2020	Complete; no intrusions detected (Audit: GK)
June 6, 2020	Complete; no intrusions detected (Audit: GK)
July 4, 2020	Complete; no intrusions detected (Audit: GK)
August 1, 2020	Complete; no intrusions detected (Audit: GK)
September 5, 2020	Complete; no intrusions detected (Audit: GK)
October 3, 2020	Complete; no intrusions detected (Audit: GK)

November 7, 2020	Complete; no intrusions detected (Audit: GK)
December 5, 2020	Complete; no intrusions detected (Audit: GK)
January 2, 2021	Complete; no intrusions detected (Audit: GK)
February 6, 2021	Complete; no intrusions detected (Audit: GK)
March 6, 2021	Complete; no intrusions detected (Audit: GK)
April 3, 2021	Complete; no intrusions detected (Audit: GK)
May 1, 2021	Complete; no intrusions detected (Audit: GK)
June 5, 2021	Complete; no intrusions detected (Audit: GK)
July 3, 2021	Complete; no intrusions detected (Audit: GK)
August 7, 2021	Complete; no intrusions detected (Audit: GK)
September 4, 2021	Complete; no intrusions detected (Audit: GK)
October 2, 2021	Complete; no intrusions detected (Audit: GK)
November 6 2021	Complete; no intrusions detected (Audit: GK)
December 4, 2021	Complete; no intrusions detected (Audit: GK)
January 1, 2022	Complete; no intrusions detected (Audit: GK)
February 5, 2022	Complete; no intrusions detected (Audit: GK)
March 5, 2022	Complete; no intrusions detected (Audit: GK)
April 2, 2022	Complete; no intrusions detected (Audit: GK)
May 7, 2022	Complete; no intrusions detected (Audit: GK)
June 4, 2022	Complete; no intrusions detected (Audit: GK)
July 2, 2022	Complete; no intrusions detected (Audit: GK)
August 6, 2022	Complete; no intrusions detected (Audit: GK)
September 3, 2022	Complete; no intrusions detected (Audit: GK)
October 1, 2022	Complete; no intrusions detected (Audit: GK)
November 5, 2022	Complete; no intrusions detected (Audit: GK)
December 3, 2022	Complete; no intrusions detected (Audit: GK)
January 7, 2023	Complete; no intrusions detected (Audit: GK)
February 4, 2023	Complete; no intrusions detected (Audit: GK)
March 4, 2023	Complete; no intrusions detected (Audit: GK)
April 1, 2023	Complete; no intrusions detected (Audit: GK)
May 6, 2023	Complete; no intrusions detected (Audit: GK)
June 3, 2023	Complete; no intrusions detected (Audit: GK)
July 1, 2023	Complete; no intrusions detected (Audit: GK)
August 5, 2023	Complete; no intrusions detected (Audit: MW)
September 2, 2023	Complete; no intrusions detected (Audit: MW)
October 7, 2023	Complete; no intrusions detected (Audit: MW)
November 4, 2023	Complete; no intrusions detected (Audit: MW)
December 2, 2023	Complete; no intrusions detected (Audit: MW)
January 6, 2024	Complete; no intrusions detected (Audit: MW)
February 3, 2024	Complete; no intrusions detected (Audit: MW)
March 2, 2024	Complete; no intrusions detected (Audit: MW)

Last update: March 2, 2024