Assurance | Advisory
Risk | Compliance

Independent Service Auditor's Report SOC 3®
at Hoxhunt Relevant to
Security, Availability, and Confidentiality

January 1, 2020 through December 31, 2020

Table of Contents

SECTION 1 – INDEPENDENT SERVICE AUDITOR'S REPORT

AARC-360
8000 Avalon Boulevard, Suite 100, Alpharetta, GA 30009
Tel: +1 866 576 4414
www.AARC-360.com

Independent Service Auditor's Report

To: The Management of Hoxhunt

Scope

We have examined Hoxhunt's ('the Company', or 'the Service Organization') accompanying assertion titled "Assertion of Hoxhunt Management" (assertion) that the controls within Hoxhunt's Automated Phishing Prevention Platform and SaaS System (system) were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Hoxhunt's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Hoxhunt uses Amazon Web Services ('AWS') and Google Cloud Platform (GCP) (collectively, 'the Subservice Organizations') to provide Cloud Hosting and certain Managed Services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Hoxhunt, to achieve Hoxhunt's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Hoxhunt's controls. The description does not disclose the actual controls at the Subservice Organizations. Our examination did not include the services provided by the Subservice Organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Hoxhunt, to achieve Hoxhunt's service commitments and system requirements based on the applicable trust services criteria. The description presents the complementary user entity controls assumed in the design of Hoxhunt's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Hoxhunt is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Hoxhunt's service commitments and system requirements were achieved. Hoxhunt has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Hoxhunt is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the Service Organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Hoxhunt's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Hoxhunt's service commitments and system requirements based the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Hoxhunt's Automated Phishing and Prevention Platform and SaaS System were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Hoxhunt's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

AARC-360

Alpharetta, Georgia
January 15, 2021

SECTION 2 – ASSERTION OF HOXHUNT MANAGEMENT

Assertion of Hoxhunt Management

January 15, 2021

We are responsible for designing, implementing, operating, and maintaining effective controls within Hoxhunt's ('the Company', or 'the Service Organization') Automated Phishing Prevention Platform and SaaS system (system) throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Hoxhunt's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

Hoxhunt uses Amazon Web Services ('AWS') and Google Cloud Platform ('GCP') (collectively, 'the Subservice Organizations') to provide Cloud Hosting and certain Managed Services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Hoxhunt, to achieve Hoxhunt's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Hoxhunt's controls. The description does not disclose the actual controls at the Subservice Organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Hoxhunt, to achieve Hoxhunt's service commitments and system requirements based on the applicable trust services criteria. The description presents the complementary user entity controls assumed in the design of Hoxhunt's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that HoxHunt's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Hoxhunt's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 4.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Hoxhunt's service commitments and system requirements were achieved based on the applicable trust services criteria.

Pyry Avist

Pyry Avist
Chief Technology Officer
Hoxhunt

SECTION 3 – HOXHUNT'S DESCRIPTION OF THE BOUNDARIES OF ITS AUTOMATED PHISHING PREVENTION PLATFORM AND SAAS SYSTEM

Hoxhunt's Description of its Automated Phishing Prevention Platform and SaaS System Throughout the period January 1, 2020 through December 31, 2020

Company Background

Hoxhunt is a cybersecurity company founded in Finland in 2016. Hoxhunt cybersecurity services are provided with the support of multiple business teams: Service Experience, Technology, Sales Marketing and Customer Success, and Business Support. The Company has approximately 80 employees at time of writing, opening a UK office in early 2019. Growth continues to be fueled in spite of the ongoing COVID19 pandemic by the loyalty of Hoxhunt's international clientele who rely on Hoxhunt's services daily to keep their businesses safe from cybersecurity threats. Hoxhunt's customers operate in a diverse range of industries, including public sector, financial, healthcare, telecoms, manufacturing, security and utility services. Users of the Hoxhunt system are situated in all five continents and number over one million.

Overview of Services Provided

Gamified Phishing Training Platform — Hoxhunt's core application, the Gamified Phishing Training Platform, conditions employees to detect and report email-based social engineering phishing attacks. The service sends social engineering attacks in the form of phishing emails to the users of the service. Users learn to identify and report these malicious messages. Hoxhunt installs a plugin to the customer's email application. The plugin provides a button the users can click to report both real and simulated malicious attacks.

Incident Response Module — Hoxhunt's integrated Incident Response Module prioritizes user-reported emails to the administrator's attention based on preset triggers. The module decreases the number of incidents that the selected administrator(s) needs to handle by filtering out email threats which do not match the preset criteria. The incident response feature increases the efficiency of analyzing user-reported emails by reducing the possibility of human error and reacting automatically within seconds to potential anomalies.

Infrastructure

Hoxhunt is provided as a SaaS. It is hosted on Google Cloud Platform servers in Belgium and on servers provided by Amazon Web Services in Ireland.

Software

The Hoxhunt platform results in high employee engagement toward reporting threats, both real and simulated. This stems from continuous training. Due to the Hoxhunt plugin being installed in employee's email clients, whether mobile, desktop or web, the organisation can report threats as a part of their everyday workflow of processing their email inboxes—all from one single button, used for both reporting simulations and real threats. The message to individual employees is clear and easy to understand: whenever an email looks fishy, press the Hoxhunt button.

As the organisation's employees begin enthusiastically reporting suspected threats as a result of the Hoxhunt training, the volume of reported threats shoots up. Going through all of these reports one-by-one, especially as attacks are usually executed as automated mass email campaigns sent to a big recipient list, would be an unreasonable demand for any Security Operations Center; the SOC staff would not be doing much else than analyzing reported threats if every single report would have to be manually processed.

For this reason, Hoxhunt provides a Threat Classification Engine and an associated threat pipeline that compares incoming threat reports based on their similarity and uses a combination of expert analysts and artificial intelligence (AI) based automation to triage, group, filter and categorize threats so that the customer's security organisation can focus on reacting on the most high-risk attacks.

The threat pipeline can be combined with the customer's existing incident response infrastructure—including their ticketing systems, intelligence, analytics platforms (SIEMs) and security automation platforms (SOARs) and more—to automate much of the incident response, so that humans can focus on high value activities that are harder to automate.

All of this comes together to mean that customer organisations can respond faster to emerging threats and use their security staff in the most cost-effective activities, as opposed to low-value data processing which is best left to machines.

Hoxhunt's Incident Response application gathers all reported emails from the customer organisation and provides the Admin and SOC users easy access to view and analyze incidents in detail. Well-designed search and sort functions make it easy to find specific cases and understand how incidents have evolved within the organisation. Security teams can easily customize and prioritize their workflows to review first incidents with larger groupings of similar emails, or other similar heuristics, and take action without delay.

Customers who require a deeper integration between the Hoxhunt services and other information systems can also query the data that is available through Hoxhunt's products directly from Hoxhunt's application programming interface (API). This interface is provided as a modern GraphQL API. For more information and technical documentation, Customers can contact their Customer Success Manager or Account Executive.

The Hoxhunt platform and its simulation-based training is fully autonomous, freeing you to focus on what matters. This means as soon as users are onboarded to the platform, the training automatically starts and adapts to the unique behaviors of each employee.

This enables your InfoSec team to focus on targeted interventions, as opposed to administering classroom or e-learning about the basic nature of phishing attacks.

As the training content is constantly updated according to threat intelligence Hoxhunt receives by analyzing the incoming threat reports from its one-million-plus-strong user base, your organisation benefits by no longer having to invest in creating continuous new training content. Phishing training material has a limited shelf life as attackers get ever-more sophisticated and evolve their attack methods and strategies each day of each week. Hoxhunt takes care of keeping the simulated attacks up-to-date so you do not have to.

As an added benefit, Hoxhunt's automated training is also tailored to your particular company and each individual's skill level and risk profile, which means that the simulations are timely, relevant and realistic—as close as possible to the real threats seen by your organisation each day.

People

Hoxhunt has approximately 80 employees organized across the following functional areas:

- *Service Experience.* Divided into content and support teams. Content team staff are responsible for the content of Hoxhunt simulated threats. Duties include analysis of threat data to maintain Hoxhunt's library of simulated threats, as well as overseeing translation of Hoxhunt into new foreign languages. Support team provides any necessary continuing technical support the Customer may require.

- *Technology.* Technology team is divided into six sub-teams, all working to improve and maintain the Hoxhunt platform, as well as develop new features.

- *Sales, Marketing and Customer Success.* Sales team is divided into two key functions: Sales Development Representatives (SDRs) and Account Executive (AEs). SDRs identify and reach out to prospects who may be interested in benefitting from Hoxhunt services. AEs develop the business relationship with prospective

customers and act as a go-between for the customer and other Hoxhunt teams. Marketing team are responsible for producing company literature on the benefits of using Hoxhunt services, and blog posts on cybersecurity trends within the wider industry. Customer Success team is responsible for successful service launch, and customer account management and education.

- *Business Support.* Business support comprises of People, Finance, and Legal functions. People function is responsible for employee satisfaction and general wellbeing, office management, as well as talent acquisition. Finance team is responsible for company accounting and revenue projections. Legal function deals with contract negotiations and internal compliance

Data

The data processed by the Hoxhunt service can be divided into two categories:

- Threat data — suspicious emails reported by Hoxhunt users via the plug-in; and
- User data — information relating to users of the service.

Threat data is analysed by the Hoxhunt content team to help ensure simulated threats mirror the latest phishing attack methods. The threat pipeline can be combined with the customer's existing incident response infrastructure—including their ticketing systems, intelligence, analytics platforms (SIEMs) and security automation platforms (SOARs) and more—to automate much of the incident response, so that humans can focus on high value activities that are harder to automate.

User data is processed exclusively for the purpose of providing the Hoxhunt service. There are two aspects of the Hoxhunt service which involve processing of user data: user authentication and threat generation. Hoxhunt processes the mandatory categories personal data (listed below at question 1.2) in order to verify their identity and protect the integrity of the Hoxhunt system. Regarding threat generation, the cybercriminals of today are able to tailor phishing emails to the level of individual employees using personal data obtained from illicit sources. Hoxhunt therefore processes personal data provided by the customer in order to make simulated threats an authentic and effective training tool. For example, threats are created to reflect the user's geolocation, and, if the customer chooses to provide it, the user's department and job title. The difficulty of threats generated for the user is also tailored according to the user's historical success rate.

Processes and Procedures

Management has developed and communicated to all employees and contractors procedures to restrict logical access to Hoxhunt systems. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life-cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

SECTION 4 –HOXHUNT'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments and System Requirements

Hoxhunt designs and maintains its processes and procedures related to its service offering to meet its objectives. Those objectives are based on the service commitments that Hoxhunt makes to user entities, the laws and regulations that govern the provision of Hoxhunt services, and the financial, operational, and compliance requirements that Hoxhunt has identified for the services. Hoxhunt operates its services and internal affairs in compliance with the rules and regulations of jurisdictions in which it is established and offers services. These include:

- Personal data privacy laws (notably GDPR, CCPA)
- Anti-bribery laws (notably the FCPA and UK Bribery Act)
- Employment legislation in Finland (including but not limited to the Employment Contracts Act 2001) and the UK (the Employment Act 2002)
- Finnish and UK company and financial reporting laws
- UK and Finnish laws relating to fraud (including but not limited to the UK Fraud Act 2006 and Finnish Penal Code)

Security and service level commitments to user entities are documented and communicated in customer contracts. Security commitments are standardized and include, but are not limited to, the following:

- Technical measures such as browser and plugin traffic encryption; event monitoring and logging; and regular back-ups.
- Organisational measures such as physical and logical access controls; two factor authentication; device management systems; internal training; risk assessment procedures; due diligence of third-party vendors; and secure disposal protocols.

Hoxhunt establishes operational requirements that support the achievement of security commitments, compliance with relevant laws and regulations, and other system requirements. Such requirements are communicated in Hoxhunt's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organisation-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of Hoxhunt's services and its constituent systems.

Complementary Subservice Organisation Controls (CSOCs)

Hoxhunt utilizes Subservicing Organisations to perform certain key operating functions for Hoxhunt services. The accompanying description of controls includes only those policies, procedures and controls at Hoxhunt, and does not extend to policies, procedures and controls at the Subservice Organisations.

Hoxhunt uses the following Subservice Organisations to implement portions of its services and the following table presents the applicable Trust Services Criteria that are intended to be met by controls at each subservice provider, alone or in combination with controls at Hoxhunt, and the types of controls expected to be implemented at the subservice provider to meet those criteria.

Subservice Organisations

The Hoxhunt service is built on top of Google Cloud Platform and Amazon Web Services Infrastructure as a Service (IAAS) and Platform as a Service (PaaS) products. Google Cloud Platform and Amazon Web Services undergo their own rigorous audit processes to include an annual AICPA based SOC2 audit, which are examined annually by Hoxhunt. It is expected that each Subservice Organisation has implemented the following types of controls to support the associated criteria.

Both Subservice Organisations' controls must be evaluated in relation to Hoxhunt's controls, taking into account in particular the related complementary Subservice Organisation Controls (CSOCs) expected to be implemented at the Subservice Organisation as described below.

Subservice Organisation	Services Provided	Applicable Criteria	Control Activity Expected to be Implemented at the Subservice Organisation
Google Cloud Platform Amazon Web Services	Infrastructure as a Service (IaaS)	CC6.1, CC6.4	Subservice Organisation is responsible for maintaining logical and physical security over the servers and other hardware devices upon which the Hoxhunt system is hosted.
		CC7.4	Subservice Organisation is responsible for notifying Hoxhunt of any security incidents related to security over the servers and other hardware devices upon which the Hoxhunt system is hosted.
		A1.2	Subservice Organisation is responsible for monitoring system availability, back up procedures, and recovery infrastructure to meet its objectives.
			The Subservice Organisation is responsible for maintaining environmental monitoring, physical access, fire detection alarms, protection equipment, fire inspection, and other physical safeguard practices to ensure the safety of the data center services provided.

Complementary User Entity Controls

Certain criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of Hoxhunt's controls are suitably designed and operating effectively, along with related controls at Hoxhunt. Complementary User Entity Controls are specific user controls or issues each Hoxhunt client organisation should implement or address respectively in order to achieve the applicable criteria identified in this report. These considerations are not necessarily a comprehensive list of all internal controls that should be employed by user entities, nor do they represent procedures that may be necessary in all circumstances.

1. Customers are responsible for understanding and complying with their contractual obligations to Hoxhunt.
2. Customers are responsible for notifying Hoxhunt of changes made to technical or administrative contact information.
3. Customers are responsible for maintaining their own system(s) of record.
4. Customers are responsible for ensuring the supervision, management, and control of the use of Hoxhunt's services by their personnel.
5. Customers are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Hoxhunt's services.
6. Customers are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
7. Customers are responsible for ensuring that data submitted to Hoxhunt is complete, accurate, and timely.
8. Customers are responsible for having standards and processes in place to follow security and industry guidelines.
9. Customers are responsible for contacting Hoxhunt if there are any issues or concerns with service availability or security.