Managed Risk Program: Harden and Wargame

a. Red Team Wargame

eSentire will, through a variety of means (for example, social engineering or penetration testing) selected by eSentire, attempt to infiltrate Client's network on an annual basis. A Red Team Exercise may include the following:

- Attempt to establish an undetected persistent foothold in Client's network that could be used to pivot to other internal systems;
- Attempt to compromise and gain privileges on workstations, servers, and Client-specified systems; attempt to escalate privileges and gain administrative privileges on workstations, servers, and Client-specified systems (including attempting to gain top domain admin access);
- Attempt to obtain access to key systems and information defined by Client (known as a Capture the Flag exercise);
- Attempt to compromise high profile users (for example, accounts and credentials);
- Attempt to bypass security controls on workstations and servers to execute eSentire controlled code;
- Attempt to use custom, non-destructive malware and other technology (custom websites, executable web applets);
- Open-source intelligence gathering whereby through the use of custom tools and a variety of services data is collected related to Client's employees and their external network (OSINT). This data is used to generate lists of potential usernames and passwords, discover publicly available email addresses, and generate a snapshot of open ports and services for use in penetration testing and Red Team Exercises;
- External penetration testing whereby eSentire identifies the services running on each host, and identifies the service versions running on each host, as well as:
    - Penetration attempts on hosts and/or services identified by Client, and which have known vulnerabilities;
    - Attempt external infrastructure attacks (excluding denial of service attacks);
    - Attempt external data access attacks (including brute force attacks);
    - Attempt basic technical security violations of external facing applications (including cross site scripting attacks, cross site referencing, and SQL injection attacks); and
    - Attempt a deep dive exploitation of identified weaknesses in external systems into internal systems.
- Social engineering whereby:
    - eSentire identifies Client employees using publicly available information and, at eSentire's discretion, targets such employees for social engineering campaigns based on such employee's role at Client,
    - eSentire potentially conducts phishing campaigns to attempt to access and/or gather confidential information of Client or to exploit other vulnerabilities to compromise Client's data and/or infrastructure security;
    - eSentire potentially conducts vishing campaigns to attempt to access and/or gather confidential information of Client or to exploit other vulnerabilities to compromise Client's data and/or infrastructure security; and
    - eSentire attempts to install custom, non-destructive malware on a Client system, including use of USB dongles, flash drives, etc. or use other technology (custom websites, executable web applets, etc.) in connection with telephone calls to Client employees or phishing emails to access and/or gather confidential information of Client.

b. Managed Phishing and Security Awareness Training (Co-Managed)

Monthly phishing campaigns are run for Client based on Clients defined workflow, throughout the annual term. Security awareness training is provided prior to the phishing campaigns and supplemental training is provided to users who fail phishing campaign simulations. As well, Client has co-managed access to perform ad-hoc phishing campaigns and administer ad-hoc security awareness training to their users.

Support

eSentire will provide onboarding, user level, administer level guides supporting Clients' usage of the SaaS platform. Support is available during normal business hours (EST).

Reporting/Dashboards:

- Awareness and Education
- Exposures
- Course Completion Summaries
- NIST CSF Alignment
- Onboarding Summary
- Phishclick Analysis
- Phishforward Report
- Phishforward Summary
- Outdated Browser Summary
- Security Dissonance Summary
- Survey Results Summary
- Technology Summary
- Top Division Risk Summary
- Top User Risk Summary
- Security News Bulletin
- Phishing simulation Report
- Data Captured Phish Report

Responsibilities

- eSentire will provide 12 phishing campaigns per year (one campaign per month):
    - Each phishing campaign will be selected from the phishing campaign templates library
    - Each phishing campaign will be sent out every 30 days from the initial campaign or on custom workflow agreed upon by Client and the MRS team.
- eSentire will also provide general security awareness training through the online Learning Management System (LMS).
- eSentire's online Learning Management System (LMS) will provide targeted security training for users who fail phishing campaigns
- Client may request on a quarterly basis, a one-hour review of the findings of the campaigns with an eSentire Information Security Consultant
- Client must use Two-Factor Authentication (2FA)

Exclusions

- Client may not adjust frequency of delivery
- eSentire reserves the right to limit support effort as required

Client using Legacy Phishing and Security Awareness Training platform, eSentire will conduct one phishing campaign per quarter against those internal employees identified by Client and eSentire will provide quarterly security awareness training sessions. Each training session may be broken down into a maximum of three sub-sessions and each sub-session shall be no longer than one-hour in length.

c. Internal Penetration Testing

eSentire will on a semi-annual basis attempt to compromise and gain privileges on workstations, servers and domain controllers specified by Client, and escalate privileges and gain administrative privileges on Client specified systems or domain controllers.

d. External Vulnerability Scan and Penetration Test and OSINT

This engagement includes eSentire quarterly scanning, the quantity of IP Addresses (including cloud-hosted and on-premise assets) as set out on the applicable Order Form and which have been provided to eSentire by Client, identifying services running on each host, and identifying service versions running on each host, as well as:

- Penetration attempts on hosts and/or services identified by Client, and which have known vulnerabilities;
- Attempt external infrastructure attacks (excluding denial of service attacks);
- Attempt external data access attacks (including brute force attacks);
- Attempt basic technical security violations of external facing applications (including cross site scripting attacks, cross site referencing, and SQL injection attacks); and
- Attempt deep dive exploitation of identified weaknesses in external systems into internal systems.
    - **External Vulnerability Rescan**. eSentire will perform an External Vulnerability Rescan if Client received a one-time or annual recurring External Vulnerability Scan. After remediation activities undertaken by Client have been completed following an External Vulnerability Scan, eSentire will, no later than three months following eSentire delivering to Client its draft report, rescan only those servers identified by eSentire to have high or critical security issuers to validate such remediation.
    - **Open-Source Intelligence Gathering**. eSentire will use custom tools and a variety of other services to collect data related to Client employees and their external network (OSINT) to generate lists of potential usernames and passwords, discover publicly available email addresses, and generate a snapshot of open ports and services for use in penetration testing.

e. Managed Vulnerability Service – Cloud, Co-managed

Managed Vulnerability Service is an eSentire and Client co-managed service which provides access to a vulnerability scan-management and reporting platform and delivers vulnerability reports and vulnerability trending on a predetermined periodic basis, including the following capabilities (the "**MVS**"):

- **Vulnerability Scanning**. Vulnerability scanning delivers vulnerability reports and vulnerability trending on a predetermined periodic basis, weekly for external scans and monthly for internal scans to determine Client's vulnerability posture and allow Client to guide network/system configuration and controls. Client also has limited access to co-managed platform to define and direct their own scanning in cooperation with eSentire.
- **Vulnerability Reporting**. Various reports for external and internal findings are sent by eSentire to Client following each scan conducted. eSentire may also direct Client to reporting platform portal to receive vulnerability reports in addition to or instead of providing scan report findings.
- **Monthly Review**. Client may request once per month a one-hour review of the findings of the scans conducted above with an eSentire Information Security Consultant.

- Ad-Hoc Vulnerability Scanning. Client may also direct their own ad-hoc vulnerability scanning via the eSentire-provided vulnerability scan-management and reporting portal with limitations and provided such scanning does not unduly interfere with eSentire delivery of the MVS or other eSentire supplied services.
- This engagement includes weekly external scanning and monthly internal scanning, the quantity of IP Addresses (including cloud-hosted and on-premise assets) set out in the applicable Order Form and which have been provided to eSentire by Client.
- Co-managed service. Client will be provided tenant access to an eSentire-managed scan-management and reporting platform portal. Client may direct their own scans and access reporting independent of eSentire and during this process shall not interfere or otherwise modify agreed scanning policies and scan frequencies as defined by eSentire. Client shall not otherwise interact with the provided tenant access in a manner that adversely affects the delivery of the MVS or any other eSentire-provided Client services with without prior written consent by eSentire.
- Quarterly PCI Attestations. Client may request that eSentire submits external PCI scan results to the approved scanning vendor for PCI-ASV attestation. Such scanning shall be performed a minimum of once per calendar quarter, provided it is Client's sole responsibility to request that scan results are submitted for ASV certification as needed and all required information is provided. It is Client's responsibility to complete a Self-Assessment Questionnaire (SAQ) and assess what level of PCI compliance is required, as well as to provide a complete and accurate scope of assets. The MVS PCI add-on relates to PCI DSS 11.2.2. For the avoidance of doubt, external PCI scans and Attestations of Scan Compliance are not included in the standard MVS offering and additional fees will apply. Quarterly PCI Attestations shall only be provided in connection to the Managed Vulnerability Service.
- Web Application Scanning ("WAS") delivers the ability to scan external facing web applications for known vulnerabilities to determine Client's web application posture and allow Client to guide web configuration and controls. Client also has limited access to co-managed platform to define and direct their own scanning in cooperation with eSentire. For the avoidance of doubt, the Web Application Scanning is not included in the MVS, and additional fees will apply, and the Web Application Scanning shall only be provided in connection to the Managed Vulnerability Service.
- Container Security ("CS") delivers the ability to scan containers for known vulnerabilities to determine Client's container security posture and allow Client to guide container security configuration and controls. Container Security provides detection for container infrastructure and associated applications. Client also has limited access to co-managed platform to define and direct their own scanning in cooperation with eSentire. For the avoidance of doubt, Container Security is not included in the standard Managed Vulnerability Service offering and additional fees will apply. Container Security shall only be provided in connection to the Managed Vulnerability Service.

Sensors.

eSentire may provide at least one physical or virtual security appliance (a "Sensor") as specified on the applicable Order Form and to the extent required to provide to Client the MVS.

eSentire will configure and remotely manage the Sensor and its embedded software for all devices as part of the MVS. Client may only access the configuration of such Sensor with eSentire's prior written authorization. eSentire shall only access the configuration of other network devices connected to the Sensor with Client's authorization and shall do so through an encrypted and secure means.

Client Responsibilities.

Client is responsible for:

- Any and all data and systems which Client grants access to for receipt of the MVS;
- Obtaining all necessary licenses, permissions, and consents to enable eSentire to access Client's network and servers in order to provide the MVS, including any 3rd party permissions as required;
- Designating a Project Coordinator to work directly with and serve as the primary Client contact with eSentire for the duration of Client receiving the MVS;
- Providing eSentire a complete copy of its security (including privacy) policies, as available. Client is solely responsible for the creation, maintenance, and enforcement of its security policies to protect the security of Client Data and Systems;
- Its choice of equipment, systems, software, and online content;
- Providing the necessary resources, information, documentation and access to personnel, equipment, systems and scanning schedules, as reasonably required by eSentire, to allow eSentire to perform the MVS;
- Notifying eSentire of any change or contemplated change to its network in advance of Client effecting such change;
- Complying with all applicable local, state, provincial, federal, and foreign laws in using the MVS and any provided tools used in conjunction with MVS including but not limited to the vulnerability scan-management and reporting platform portal;
- Advising eSentire of network and IP/endpoint range changes to scope. for the avoidance of any doubt, any material changes to the IP/endpoint count including overages that are greater than a five percent (5%) increase to the contracted scope in any sustained manner greater than 30 days may incur additional costs at the then-current contract rate and shall be calculated by eSentire and billed to Client minus any newly applicable volume discount.

Client responsibilities for Web Application Scanning.

Client is responsible for:

- Specifying one valid Web application address/port for each web application being scanned. Each additional web application being scanned will be billed to Client minus any newly applicable volume discount;
- Accessing WAS service reporting via the eSentire-provided vulnerability scan-management and reporting platform portal;
- Conducting and remediating the found risks and vulnerabilities for each respective Web application;
- Any 3rd party hosting permissions as required.

Client responsibilities for Quarterly PCI Attestations.

Client is responsible for:

- Being proactive towards the remediation of discovered vulnerabilities, contacting eSentire ahead of submission deadlines and in responding to communications regarding PCI compliance;
- Providing all documentation required for their PCI compliance submission a minimum of three weeks before submission, providing updates as required, until documentation is formally submitted; and
- Requesting one scan per calendar quarter so that eSentire submits external scan results to the approved scanning vendor for PCI ASV validation and certification. It is Client's responsibility to request that scan results are submitted for ASV certification as needed.

In the event Client fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption outlined herein with respect to the MVS Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages. In the event that Client fails to notify eSentire of network changes as contemplated above, then eSentire shall be released from any and all obligations to scan Client's network until Client has notified eSentire of such change.

Exclusions.

The MVS excludes the following:

- The design, creation, maintenance, and enforcement of a security policy for Client; and
- eSentire attempting to access Client's servers without Client's express written or verbal consent.

f. Security Program Maturity Assessment

eSentire will review and assess the effectiveness of Client's internal security program against the "Core 15" assessment areas of eSentire's "Cybersecurity Reference Model", other cybersecurity standard(s) or regulatory requirements as may be mutual agreed to by Client and eSentire in writing. The "Core 15" areas of the eSentire Cybersecurity Reference Model include:

- IT Security Strategy & Governance
- Human Resources
- Security Architecture
- IT/Security Risk Management
- Monitoring & Operations
- Incident Response
- Information Management
- Asset Management
- Vulnerability & Patch Management
- Third Party Risk Management
- Compliance & Audit
- Secure Network Design
- Authorization & Access Controls
- Malicious Code Prevention
- Secure Builds

The Security Program Maturity Assessment will also include meetings with appropriate Client designates and subject matter experts, eSentire evaluating risk areas and defining overall risk levels of Client's internal security program, as well as eSentire evaluating and reporting to Client on the quality of Client's processes, routines, and controls. eSentire will provide to Client a baseline assessment of Client's internal security program against eSentire's "Cybersecurity Reference Model", including an executive summary and details findings report in Microsoft Word and Excel formats.

g. Security Incident Response Planning

eSentire will review, assess, and assist in developing a cybersecurity incident response plan appropriate to Client's business needs and in consideration of regulatory and legal requirements applicable to Client. eSentire will conduct one workshop session with Client to collect information, interview appropriate stakeholders and key or relevant personnel, and develop a scenario framework for assisting Client to develop a cybersecurity incident report plan. Cybersecurity Incident Response Planning may also include eSentire:

- Providing documentation of Client's event defense measures currently in place;
- Discussing with Client's subject matter expert(s) to identify "most likely" cybersecurity scenarios (for example, financial loss due to threat or breach, denial of service, viral outbreak of breach, 'threats made);

- Meeting with Client's subject matter expert(s) and other appropriate designates (for example, Client's management team, human resources, or information technology personnel, 'business drivers') to confirm approach in developing a cybersecurity incident response plan for Client;
- Reviewing Client's existing disaster recovery plan(s) and/or business continuity plan(s);
- Reviewing any past vulnerability audit(s) or penetration test(s) conducted by or on behalf of Client;
- Performing 'dry-run' simulations of likely cybersecurity incident scenarios; and
- Providing a logbook of responses to initial 'dry-run simulation identified in (vi) above.

h. Security Policy Review and Guidance

eSentire will review, assess, and assist Client on an annual basis, in the development of Information Security policies to address cybersecurity threat and regulatory compliance requirements. eSentire will:

- Review and assess Client's existing Information Security (and related) policies;
- Evaluate Client's Information Security policy requirements based on applicable legal and regulatory requirements; and
- Provide guidance to Client on the development and adoption of Information Security policies required to meet Client objective and applicable regulatory and/or legal requirements.
- Providing Initial (baseline) assessment and guidance on Information Security policies:
  - Workshop session with Client to collect information and review existing architecture
  - Development of updated Information Security policies based on assessment and findings
  - Guidance and direction on Information Security policy adoption within Client's organization
- Providing Annual re-assessment and review of Information Security policies:
  - Annual review of Information Security policies to identify gaps based on any applicable business, regulatory, or legal changes
  - Provide findings and recommendations report based on annual review

i. Security Architecture Review

eSentire shall review, assess, and provide on an annual basis, recommendations for the Security Architecture of Client's environment. eSentire will:

- Review and assess Client's existing Security Architecture including, but not limited to, network design, network segmentation, access controls, technical controls, and user authentication;
- Provide recommendations for improvement of Client's Security Architecture; and
- Review any past available Vulnerability Audit(s), Penetration Test(s), or Assessment(s).
- Initial (baseline) assessment and review of Security Architecture:
  - Workshop session with Client to collect information and review existing Security Architecture
  - Detailed Recommendations report based on findings with an attached Executive Summary
- Annual re-assessment and review of Security Architecture:
  - Annual review of Security Architecture

Any plans, processes and framework generation are based on a cooperative and collaborative effort between Client and eSentire. If it is Client's responsibility to execute on any action and recommendations as described in the findings and deliverables of this review. eSentire does not assume operational ownership of Security Architecture by engaging in this review.

j. Executive briefings

eSentire will provide an annual executive briefing covering topics such as testing results and subsequent risks, general security trends and the overall threat landscape.

k. Threat advisories

eSentire will send threat intelligence advisories via email on an as needed basis regarding emerging threats and vulnerabilities including mitigation advice.