Validation Evidence

In order to provide an additional level of assurance, your customer may request that you perform evidence validation after completing a CyberGRX cyber security questionnaire. Below is guidance around what sort of documents are helpful to use when completing the CyberGRX assessment. They can also be used as evidence if you are required to go through evidence validation.

Useful Documents

The following list of documents is meant to be illustrative of the types of documentation that can be helpful in filling out the CyberGRX questionnaire. The items on list below should not be considered required or exhaustive of all documents that may help or be accepted as proof in validation.

Threat Analysis Documents

Supporting documents that indicate the type threat analysis (i.e. attack kill chains, modeling of attacks, etc.)

Example brief of threat intelligence that is ingested into organization tools and processes

Screenshot of organizational tools that indicates ingestion of threat information (i.e. Known Bad IP Addresses, indicators of compromise)

Technologies that can help provide the above

STIX/TAXII/CYBOX | AlienVault | OpenIOC | OASIS Cyber Threat Intel. | Cyber Threat Alliance | ISAC Feeds

Vulnerability Scan Administrative Evidence

Policies and procedures, may be helpful for describing the context of the control implementation.

Screenshot of vulnerability scan tool or other tools that shows the assets being scanned

Screenshot of vulnerability scan tool or other tool that shows the frequency of scans conducted

Technologies that can help provide the above

Nessus Security Center | SCAP | Rapid 7 | Qualys | Cronos | Vericode

Alert Contents and Responses Procedural Documents

Sample alert from SIEM tool

Sample alert from other monitoring tools (malware, configuration management, etc.)

Screenshot(s) from automated monitoring tools showing alerting configuration

Technologies that can help provide the above

SIEM Tools (Splunk, Qdar, LogRythm) | NetWatcher Netwrok Monitoring | Tenable Security Center

Incident Response Program Requirements Documents

Incident Containment Capability Procedural Documents

Screenshot of incident management/forensics tool illustrating threat removal process

Documents associated with NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response

Documents associated with NIST 800-61 Computer Security Incident Handling Guide

Documents associated with ISO/IEC 27035 Information security incident management

Technologies that can help provide the above

SANS Investigative Tool Kits (SIFT) | Sluethkit | GRC workflows

RCA Archer Incident Mngmt

Backup and Recovery Capability Procedural Documents

Screenshot(s) from data backup tools showing the types of backups that are scheduled and the target data

Proof of restoration

Technologies that can help provide the above

Veeam Backup & Replication | Dell EMC | Code42 | Veritas NetBackup

Background Screenings Procedural Documents

Redacted background screening report

Security Awareness Requirements Documents

Security Awareness Procedural Documents

Security Awareness Training Samples

Screenshot(s) from security awareness training modules

Screenshot(s) from security awareness training tracking tools

Technologies that can help provide the above

CyberVista | ITPro.tv | SANS

Least Privilege Procedural Documents

- Sample user account request form
- Role descriptions with access requirements

Screenshot(s) from account management tools

Screenshot(s) from physical access management consoles

Screenshot(s) from user access request ticketing system

Technologies that can help provide the above

Active Directory Security Groups | NetIQ | BadgePass | HID VertX | Genetec

Secure Code Repositories Controls Procedural Documents

Screenshots from ticketing tools showing security design processes in place

Technologies that can help provide the above

JIRA | ServiceNow

Encryption Procedural Documents

Screenshot(s) showing bootup password for full device encryption

Screenshot(s) from backup server configurations showing encryption settings

Screenshot(s) of NAS configuration settings

Technologies that can help provide the above

Symantec Backup Exec | Synology | Microsoft SQL EncryptByKey | Drobo | HTTPS / TLS | IPSec | Symantec Gateway Email Encryption | Secure Real-Time Transport Protocol (SRTP)

Hardening and Patching Procedural Documents

Screenshot(s) describing logging and auditing are in place

Screenshot(s) from configuration management tools

Screenshot(s) from configuration management tools

Technologies that can help provide the above

Microsoft Windows Services | Linux/Unix | MacOS | Chef | BigFix

Browser Hardening Procedural Documents

Sample browser configuration standard

Screenshot(s) showing browser settings

Technologies that can help provide the above

Google Chrome | Internet Explorer | Mozilla Firefox

Anti-Malware Implementation Administration Samples

Screenshot(s) from anti-malware tools used for desktops and laptops

Technologies that can help provide the above

Symantec SEP | ESET Antivirus | Kaspersky Antivirus | Malware Bytes

Hardening and Patching Procedural Documents

- Screenshot(s) of disabled service(s)
- Screenshot(s) describing logging and auditing are in place
- Screenshot(s) showing login is required
- Screenshot(s) from configuration management tools

Technologies that can help provide the above

Microsoft Windows | Linux/Unix | MacOS | Chef | BigFix

Network Device Procedural Documents

- Screenshot(s) from network device management consoles showing what types of functionality is active
- Screenshot(s) from network device management consoles showing most recent version/FW is in place
- Screenshot(s) from network device management consoles showing high-availability configuration or redundancy

Technologies that can help provide the above

HPE Officeconnect | Aruba | Ubiquity/UniFi | BROCADE | Ruckus Wireless

Archive

Firewall Administrative Evidence

Screenshot(s) from firewall management consoles showing what types of functionality is active

Screenshot(s) from firewall management consoles or GRC tools showing the date of firewall rule reviews

Technologies that can help provide the above

Cisco ASA | SonicWall | Fortinet Fortigate | Palo Alto *Cisco Meraki

Email Configuration Administrative Evidence

Screenshot(s) from email configuration pages

Screenshot(s) from email security tool or webportal

Technologies that can help provide the above

Barracuda | MailWasher | RoaringPenguin | Office365 | G Suite | Proofpoint

Asset Configuration Procedural Documents

Screenshot(s) from configuration management tools that show the types of assets covered

Screenshot(s) from configuration scanning tools that show the frequency and scope of scans

Technologies that can help provide the above

Chef | Puppet | Ansible | BigFix | Tripwire

Vendor Risk Program Procedural Documents

Vendor Risk Program Capability Procedural Documents

Risk Mitigation Procedural Documents

Screenshot(s) from a third party risk management tool

Technologies that can help provide the above

RSA Archer | R-Sam | other GRC tools

Critical Controls

These controls are deemed part of critical killchains and so are always validated.

1.1.2.1

Risk Assessment

Conduct a cyber security and privacy risk assessment that is integrated across the enterprise and coordinates elements of information security and privacy.

2.1.2.1

Threat Analysis

Design and implement a cyber security audit and compliance function

2.2.2.1

Vulnerability Scans

Collect, analyze, and report data on potential threats to the organization and indicators of compromise (IOCs).

2.3.2.1

Assess - Security Alerting and Analytics

Establish a vulnerability prioritization framework that effectively and quickly prioritizes the vulnerabilities across all asset classes in the environment.

2.4.3.1

Incident Containment

Establish a capability to classify security and privacy incidents into distinct categories to enable rapid response capabilities.

2.5.1.1

Restore Normal Operations

Utilize people, process, and technology capabilities to contain a security incident in the environment.

2.6.2.1

Business Continuity Plan

Establish a process and content for notifying key stakeholders of cyber security and privacy incidents.

3.2.1.1

Background Screening

Implement compliance monitoring capabilities to detect non-compliance in the environment.

3.3.1.2

Least Privilege

Establish a capability to notify customers in the event of a data breach.

3.2.1.3

Security Awareness Training

Conduct personnel background screenings and ensure you understand the risk associated with your various personnel roles.

3.3.2.2

Shared Account Restrictions

Grant entitlements to system resources based on the principle of least privilege, ensuring users only have the access necessary for their role.

3.4.2.1

Application and Services Security Design

Use digital certificates to protect enterprise data and communications.

3.5.2.1

Data at Rest Encryption

Create and deploy a data classification standard to ensure sensitive information is classified and protected appropriately.

3.5.4.1

Encryption of Data in Motion

Encrypt data at rest.

3.6.1.1

Desktop and Laptop Hardening

Protect documents stored in the cloud by managing cloud providers, using strong authentication, and monitoring usage.

3.6.1.4

Desktop and Laptop Secure Browsing

Harden desktop and laptop configurations to protect against malicious attacks.

3.6.1.5

Desktop and Laptop Malware Detection

Enable secure browsing controls and capabilities on desktop and laptop web browsers.

3.6.2.1

Server Hardening

Use antivirus and anti-malware tools to protect desktops and laptops from malware threats.

3.6.3.1

Virtualized Endpoint Security

Capture and securely store server logs.

3.6.4.1

Mobile Device Management (MDM)

Harden virtualized endpoints to protect against malicious attacks.

3.7.2.1

Network Device Hardening

Protect against Denial-of-Service attacks.

3.7.2.2

Network Firewalls

Harden network devices to protect against network attacks.

3.7.2.8

Segmentation Security

Utilize network intrusion detection technologies to identify potentially malicious activity entering the network.

3.7.3.1

Email Filtering

Isolate or segment your network to minimize the impact of a malicious attack moving across the network.

4.1.3.1

Asset Inventory and Use

Acquire assets through a standardized process.

4.2.2.1

Configuration Management Design and Implementation

Implement procedures for secure disposal of assets and data.

4.6.1.1

Third Party Risk Planning

Maintain the effectiveness of security and privacy performance metrics through adequate coverage, routine metric reviews, and automation.

4.6.3.1

Third Party Risk Mitigation Procedures

Establish a third party risk management framework.

PRI.1.2.1

Privacy Governance Program

Establish a cyber security information sharing program.

PRI.1.4.1

Privacy Transparency

Establish accountability, privacy governance policies, risk management strategies, and governance monitoring for your privacy data.

Additional Controls

Some set of these controls will be required for validation depending on the answers provided.

1.3.3.1

Cyber Security Policy and Standards Approval and Dissemination

Ensure organizations and individuals understand how data is processed and the associated privacy risks.

PRI.1.4.1

Privacy Transparency

Establish accountability, privacy governance policies, risk management strategies, and governance monitoring for your privacy data.

1.4.1.1

Cyber Security Audit and Compliance Design

Obtain approval of cyber security policies and standards from senior leadership, and disseminate them throughout the enterprise.

2.2.2.3

Penetration Tests

Perform vulnerability scans to identify vulnerabilities in the environment.

2.2.3.1

Vulnerability Prioritization

Conduct penetration testing to identify security vulnerabilities (e.g. staff, systems, and facilities).

2.4.2.1

Incident Classification

Leverage data from security monitoring and analytics platforms to alert on known signatures, unknown attacks, and abnormal behavior.

2.5.3.2

Incident Reporting and Notification

Establish an incident recovery plan to restore normal operations following a security incident.

2.6.3.1

Business Continuity Plan (BCP) Testing

Build a business continuity contingency plan that supports the recovery objectives identified in your Business Impact Analysis.

3.1.1.2

Compliance Monitoring

Regularly test your contingency plan to ensure it meets recovery objectives.

3.2.2.3

Customer Notifications

Require end users with access to systems or sensitive information to complete security and privacy awareness training.

3.3.2.5

Password Change Requirements

Restrict or prohibit the use of shared accounts to ensure traceability of system activity and protect against unauthorized access.

3.3.2.7

Account Lockout

Utilize regular password changes and single use passwords to ensure user passwords are initialized and refreshed.

3.3.3.2

Access Reviews

Implement account lockout rules to protect against unauthorized access.

3.3.5.1

Certificate Management

Implement a program to regularly review system access rights and verify the need for continued access.

3.5.1.1

Data Classification

Establish security requirements for internally and externally developed applications.

3.5.4.3

Removable Media Standard

Encrypt data while in transit.

3.5.5.1

Key Management

Control the use of removable media.

3.5.6.2

Cloud Document Protection

Securely manage the encryption keys used to protect sensitive data

3.6.2.6

Server Logging

Harden servers to protect against malicious attacks.

3.6.4.5

Mobile Device Remote Lock and Wipe

Control and manage mobile devices that store or have access to company information.

3.7.1.4

Denial of Service (DoS) Protection

Implement mobile device remote lock and wipe capabilities to protect company information on mobile endpoints.

3.7.2.4

Network Intrusion Detection

Use network firewall capabilities to provide a layer of perimeter defense against malicious network attacks.

3.7.3.2

Web Filtering

Detect and block potentially harmful email content.

4.1.2.1

Asset Acquisition

Detect and block potentially harmful web content.

4.1.4.2

Asset Disposal

Maintain an inventory of company assets including necessary asset attributes and asset use for effective lifecycle management.

4.2.5.1

Change Management

Establish configuration standards to improve the security of default configurations of hardware and software.

4.4.1.1

Security Controls Planning

Establish a change management process.

4.4.3.1

Security Controls Selection

Establish a security controls framework that incorporates all levels of your security controls across people, process, and technology and routinely assesses the control environment to ensure effectiveness.

4.5.3.1

Security Performance Operational Effectiveness

Select security controls based on organizational requirements and level of impact to people, process, and technology.

4.7.3.1

Security Staff Training

Establish a process for prioritizing and mitigating third party risks.

4.8.1.1

Information Sharing Planning

Establish a robust security training framework to acquire and maintain the skills necessary for effective job performance, career growth, and retention of security talent.