Cyber Insurance & PUMA's entitlements

How to use this guide:

1. Organizations differ in size, complexity, and their stage in the cyber security journey. Most have cyber insurance policies, with coverage varying by industry, size, and risk. **Tokio Marine** is commonly used by brokers to underwrite these policies.

2. The application is intended to be used for preliminary evaluation of a submission. It's used for new coverage (new customers) as well as renewals on an annual basis. When submitted, the application is used to determine whether to authorize the binding of the insurance. In short, underwriters are now using the application to determine the overall risk of the policy holder to approve or reject coverage. The application now determines the effective rate, coverage amounts, eligibility, and outcome if a security incident hits.

3. The mapping below takes the controls (copy/pasted from app) and maps them directly to Service Desk Entitlements. Green = Core, Purple= Core+, and Blue= Add-on license which is ancillary to the business's needs.

Link to latest Tokio Marine Cyber Application

https://www.tmhcc.com/en-us/-/media/project/tokio-marine/tmhcc-us/documents/cplg_taceoa_empia.pdf

Email Controls / Ransomware Controls

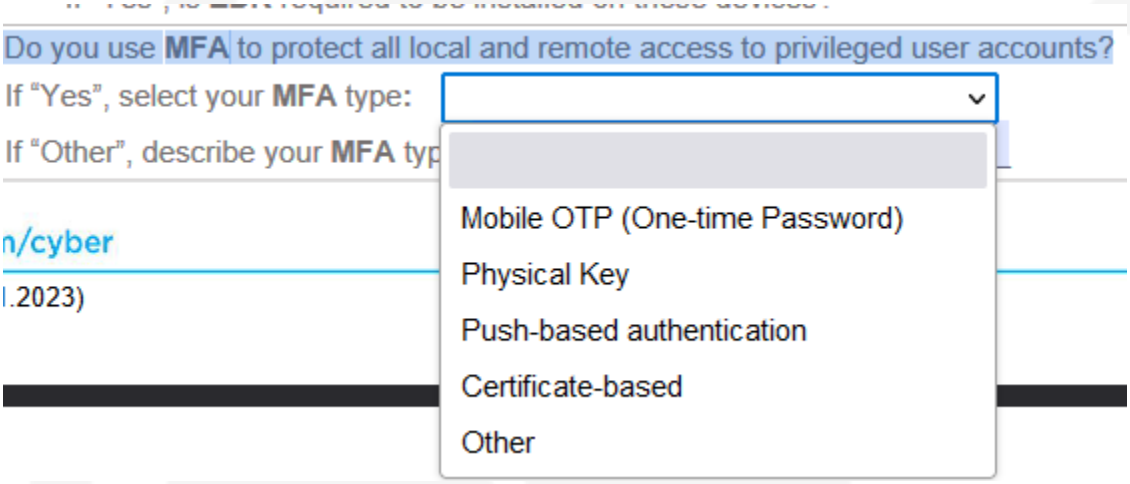
Automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user. **Microsoft License entitlement – Per License**

- Do you pre-screen emails for potentially malicious attachments and links? **Core- Microsoft 365 support & mgmt.**
- Do you tag external emails to alert employees that the message originated from outside the organization? **Core-Microsoft 365 support & mgmt.**
- Sender Policy Framework (SPF) **Core - Hardened Security Baseline for all endpoints**
- DomainKeys Identified Mail (DKIM) **Core - Hardened Security Baseline for all endpoints**
- Domain-based Message Authentication, Reporting & Conformance (DMARC) **Core - Hardened Security Baseline for all endpoints**
- Can your users access email through a web application or a non-corporate device? **Core - Hardened Security Baseline for all endpoints**
    - If "Yes", do you enforce Multi-Factor Authentication (MFA)? **Core - MFA**
- Do you use Office 365 in your organization? **Microsoft License entitlement – Per License**
- If "Yes", do you use the Office 365 Advanced Threat Protection add-on. **Microsoft License entitlement – Per License**

Internal Controls / Ransomware Controls

- Are you HIPAA compliant? – **Core+ - HIPAA mgmt. platform - SRA**
- Do you use MFA to secure all cloud provider services that you utilize - **Core - MFA**
- Do you encrypt all sensitive and confidential information stored on your organization's systems and networks – **Core – Encryption**
- Segregation of servers that store sensitive and confidential information. **Core – Identity**
- Access control with role-based assignments? **Core – Identity**
    - Yes", do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections? **Core - MFA**
- Does your MFA configuration ensure that the compromise of a single device will only compromise a single authenticator? **Core - MFA**
- Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? **Core - NGAV**

- Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise? **Core - EDR**
- Do you enforce application whitelisting/blacklisting? **Core+ - Application Whitelisting**
- Is EDR deployed on 100% of endpoints? **Core - EDR**
- Can users access the network with their own device ("Bring Your Own Device")? **Core+ - Application Whitelisting**
- Do you use MFA to protect all local and remote access to privileged user accounts? **Core+ = Elevation Control (PAM)**



- Do you manage privileged accounts using privileged account management software (PAM) **Core+ = Elevation Control (PAM)**
    - Is access protected by MFA **Core - MFA**

Do you actively monitor all administrator access for unusual behavior patterns? **Core+ = Elevation Control (PAM)** **Add-hoc - Security – SIEM** **Microsoft License entitlement – Per License**

- Do you roll out a hardened baseline configuration across servers, laptops, desktops and managed mobile devices? **Core - Hardened Security Baseline for all endpoints**
- Do you record and track all software and hardware assets deployed across your organization? **Core - Asset lifecycle mgmt. & inventory**
- Do non-IT users have local administration rights on their laptop / desktop? **Core - Hardened Security Baseline for all endpoints**
- How frequently do you install critical and high severity patches across your enterprise? **Core - Patching, security & feature OS & LoB**

- Do you have any end of life or end of support software? **Core - Asset lifecycle mgmt. & inventory**
-
    - If “Yes”, is it segregated from the rest of your network? **Core - Hardened Security Baseline for all endpoints**
- Do you use a protective DNS service (PDNS) (e.g. ZScaler, Quad9, OpenDNS or the public sector PDNS to block access to known malicious websites? **Core+ - DNS Advanced filtration**
- Do you use endpoint application isolation and containment technology on all endpoints **Core+ Application Whitelisting**
- Can users run Microsoft Office Macro enabled documents on their system by default? **Core – Hardened Security Baseline** **Core+ - Ringfencing**
- Do you implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft? **Core – Hardened Security Baseline** **Core+ - Ringfencing**
- Do you utilize a Security Information and Event Management system (SIEM)?

Add-hoc - Security - SIEM

- Do you utilize a Security Operations Center (SOC)?

Core+ - MDR + 24/7/365 SOC

    - Is your SOC monitored 24 hours a day, 7 days a week?

YES

- Do you use a vulnerability management tool?

Core+ - Vulnerability scanning (ext. pen testing)

- What is your patching cadence? 1-3 days 4-7 days 8-30 days 1 month or longer

Core - Patching, security & feature OS & LoB

Backup and recovery policies- **Add-hoc - Data protection with PUMA**

- Do you use a data backup solution? **Core - Data backup mgmt.**
    - If “Yes”: Which best describes your data backup solution?
        - Backups are kept locally but separate from your network (offline/air-gapped backup solution).
        - Backups are kept in a dedicated cloud backup service.

- You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).

- Your backups are encrypted. **Core - Data backup mgmt.** **Core – Encryption**
- You have immutable backups. **Add-hoc - Data protection (Consumable)**
- Your backups are secured with different access credentials from other administrator credentials. **Core - Data backup mgmt.**
- You utilize MFA for both internal and external access to your backups. **Core - MFA**
- You have tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months. **Core - Data backup mgmt.**
- You are able to test the integrity of backups prior to restoration to ensure that they are free of malware **Core - Data backup mgmt.**
- How frequently are backups run? Daily Weekly Monthly **Core - Data backup mgmt.**
- Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network? 0-24 hours 1-3 days 4-6 days 1 week or longer **Core - Data backup mgmt.**

Phishing controls – **Core+ - Security awareness training** – **Core+ - Phishing Simulation**

- Do any of the following employees at your company complete social engineering training:
  - Employees with financial or accounting responsibilities?
  - Employees without financial or accounting responsibilities?
  - If "Yes" to question 10.a.(1) or 10.a.(2) above, does your social engineering training include phishing simulation?

Core+ - Security awareness training

  - b. Does your organization send and/or receive wire transfers?
- **NOT PUMA POLICIES**
  - If "Yes", does your wire transfer authorization process include the following:

(1) A wire request documentation form?

NOT PUMA POLICIES

(2) A protocol for obtaining proper written authorization for wire transfers?

NOT PUMA POLICIES

(3) A separation of authority protocol?

NOT PUMA POLICIES

(4) A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment or funds transfer instruction/request was received?

NOT PUMA POLICIES

(5) A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the change request was received?

NOT PUMA POLICIES

Reference guidelines for mapping application controls to Puma's service entitlements:

All ad hoc services (add-on services)

PUMA provides additional products and services that vary by type. These services are complementary to our service desk subscriptions and are quoted by usage, consumption, per device, and per license.

Core entitlements that help meet insurance requirements:

Asset Lifecycle & Inventory	https://pumamit.com/sd-assets
Identity Management	https://pumamit.com/sd-identity
Security & Application Patching	https://pumamit.com/sd-patching
Data Encryption	https://pumamit.com/sd-encrypt
Managed Multi-Factor (MFA)	https://pumamit.com/sd-mfa
Vendor Management	https://pumamit.com/sd-vendor
Web Filtration + Content Filter	https://pumamit.com/sd-contentfilter
NGAV Protection	https://pumamit.com/sd-ngav
EDR– 24x7 Managed Detection	https://pumamit.com/sd-edr
Hardened Baseline for all endpoints	https://pumamit.com/sd-baseline
Microsoft 365 Support	https://pumamit.com/sd-microsoft

Core+ entitlements that help meet insurance requirements:

Phishing Simulation	https://pumamit.com/sdp-phishing
Vulnerability & Penetration Scanning	https://pumamit.com/sdp-pentesting
Security Awareness Training	https://pumamit.com/sdp-secawareness
DNS Filtration	https://pumamit.com/sdp-dnsfilter
Dark Web Monitoring	https://pumamit.com/sdp-darkweb
Password & Credential Manager	https://pumamit.com/sdp-passwordmgr
HIPAA Compliance & Management	https://pumamit.com/sdp-hipaa
SRA -Security Risk Assessment	https://pumamit.com/sdp-sra
Application Whitelisting	https://pumamit.com/sdp-appcontrol
MDR & SOC 24/7/365	https://pumamit.com/sdp-mdr-soc
Network Control	https://pumamit.com/sdp-network-control
Ringfencing	https://pumamit.com/sdp-ringfencing
Elevation Control (PAM)	https://pumamit.com/sdp-pam
Storage Control	https://pumamit.com/sdp-storagecontrol

Helpful links:

Tokio Marine HCC

NetGuard Plus Online Application (0-$100M revenues, $500k-$3M limits)

https://www.tmhcc.com/en-us/-/media/project/tokio-marine/tmhcc-us/documents/cplg_taceoa_npoa0-100m.pdf

e-MD® / MEDEFENSE® Plus Insurance Application

https://www.tmhcc.com/en-us/-/media/project/tokio-marine/tmhcc-us/documents/cplg_taceoa_empia.pdf

Puma Managed IT Service Pages

Service Desk Core
https://pumamit.com/servicedesk

Service Desk Core+
https://pumamit.com/servicedesk#sd-plus

Service Desk Complete
https://pumamit.com/servicedesk#sd-complete