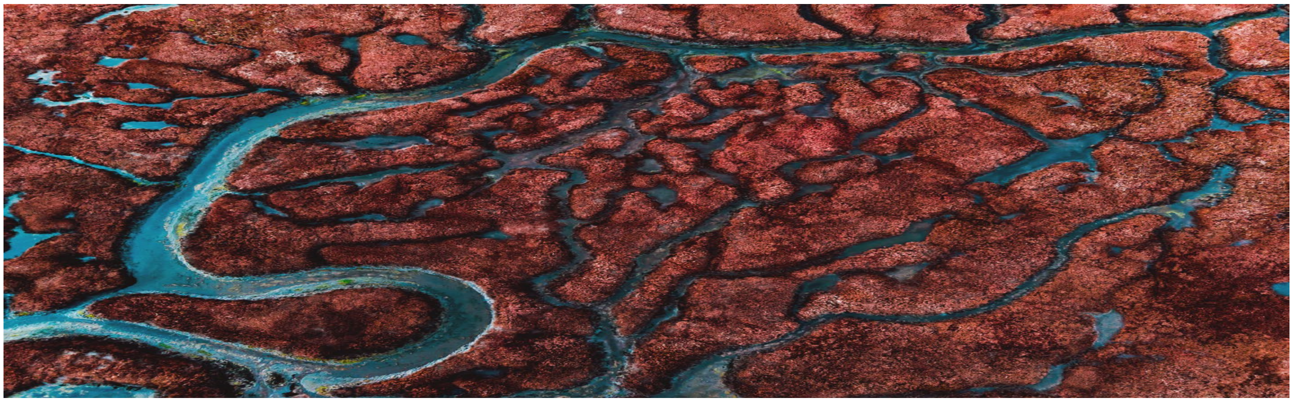
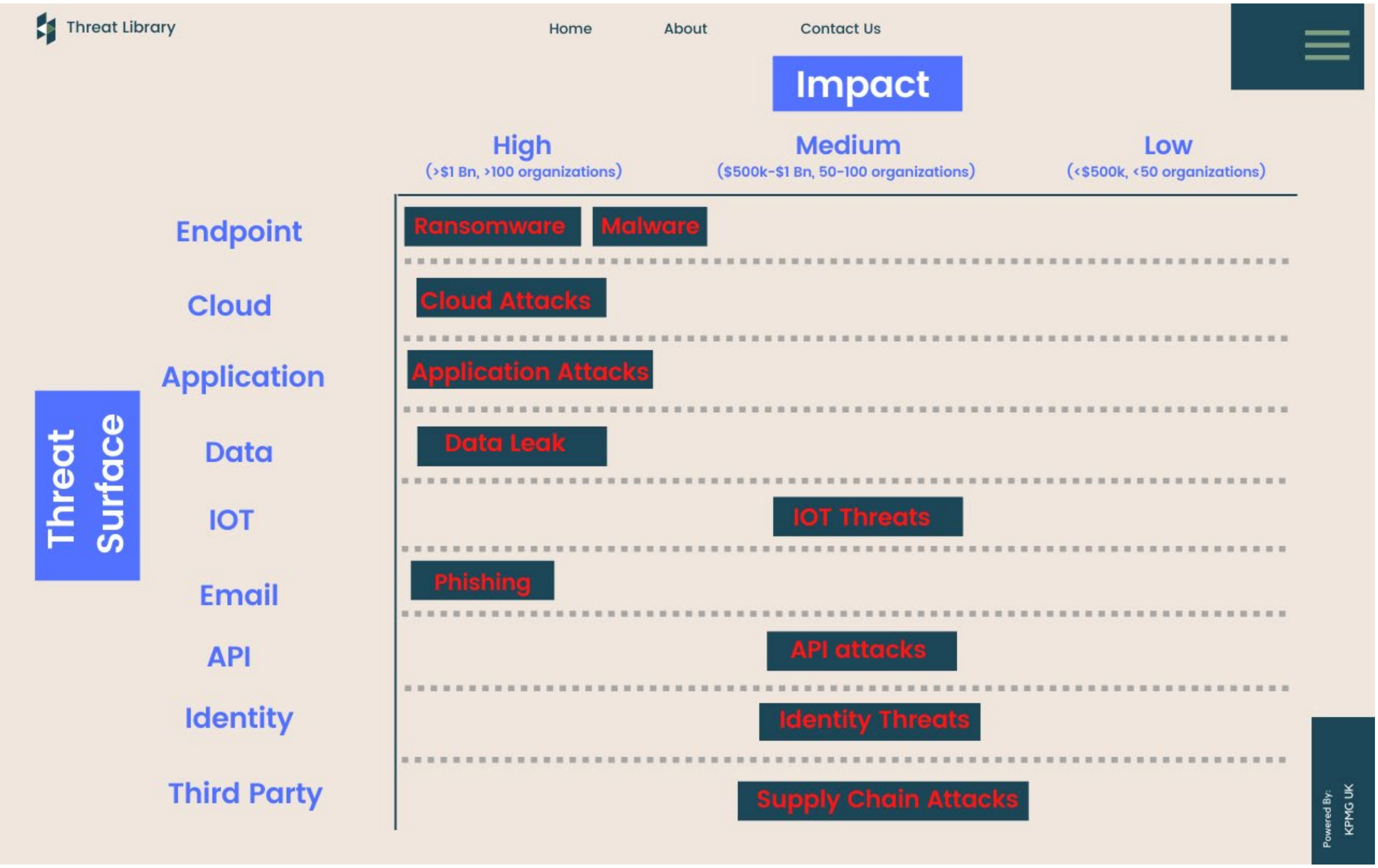
Threat Library Wireframe

[redacted]



Landing Page

The Threats will be classified based on impact (High, Medium, Low) and the Threat Surface they are associated with.



Threat Library

Home About Contact Us

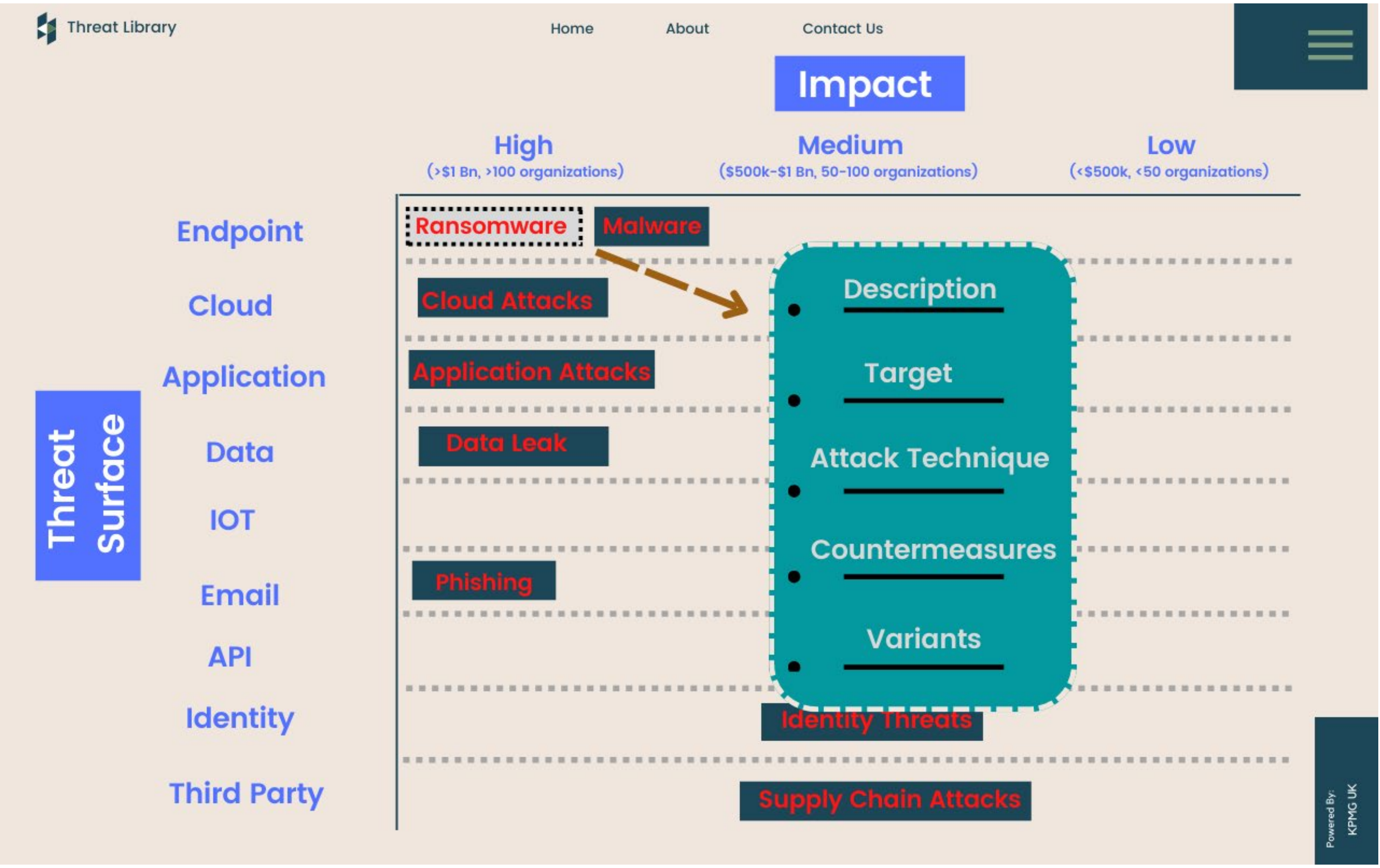
Impact

Threat Surface	High (>$1 Bn, >100 organizations)	Medium ($500k-$1 Bn, 50-100 organizations)	Low (<$500k, <50 organizations)
Endpoint	Ransomware Malware		
Cloud	Cloud Attacks		
Application	Application Attacks		
Data	Data Leak		
IOT		IOT Threats	
Email	Phishing		
API		API attacks	
Identity		Identity Threats	
Third Party		Supply Chain Attacks	

Powered By: KPMG UK

Hovering over a Threat

When a threat will be hovered over, the following elements will be visible for the user providing further details related to the threat such as Target, Attack Technique, Countermeasures etc. For eg. User is hovering over Ransomware.



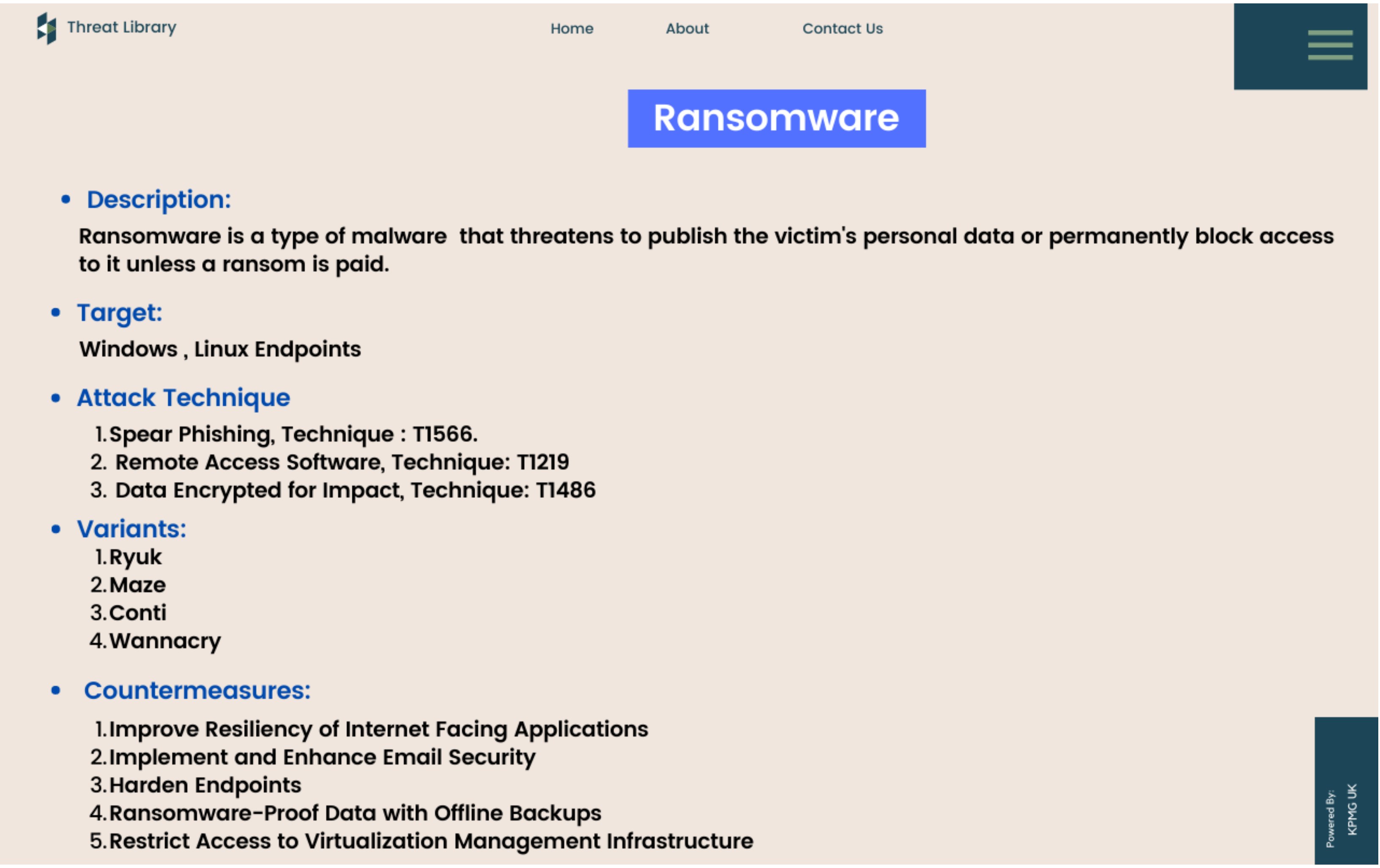
Impact

Threat Surface	High (>$1 Bn, >100 organizations)	Medium ($500k-$1 Bn, 50-100 organizations)	Low (<$500k, <50 organizations)
Endpoint	Ransomware Malware		
Cloud	Cloud Attacks		
Application	Application Attacks		
Data	Data Leak		
IOT			
Email	Phishing		
API			
Identity		Identity Threats	
Third Party		Supply Chain Attacks	

- Description
- Target
- Attack Technique
- Countermeasures
- Variants

Selecting a Threat

When a threat will be selected, details regarding the threat such as Description, Target, Attack Technique, Countermeasures, Variants etc. For e.g., User has selected Ransomware.



Ransomware

- **Description:**

  Ransomware is a type of malware that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid.

- **Target:**

  Windows , Linux Endpoints

- **Attack Technique**

  1. Spear Phishing, Technique : T1566.
  2. Remote Access Software, Technique: T1219
  3. Data Encrypted for Impact, Technique: T1486

- **Variants:**

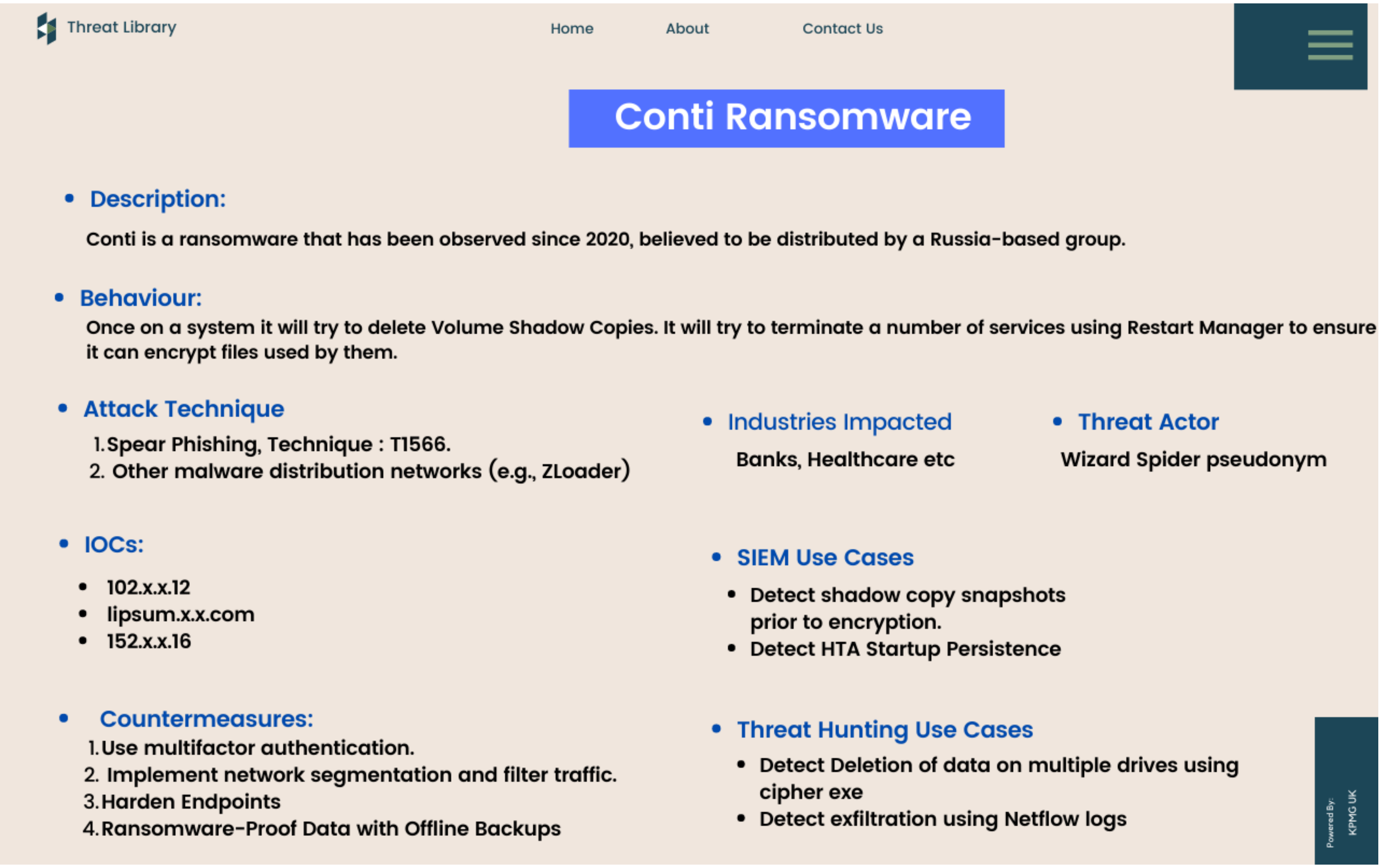
  1. Ryuk
  2. Maze
  3. Conti
  4. Wannacry

- **Countermeasures:**

  1. Improve Resiliency of Internet Facing Applications
  2. Implement and Enhance Email Security
  3. Harden Endpoints
  4. Ransomware-Proof Data with Offline Backups
  5. Restrict Access to Virtualization Management Infrastructure

Selecting a Variant

When a threat variant will be selected, further details regarding the threat such as Description, Threat Actor, SIEM use Cases, Threat Hunting Use Cases etc. For e.g., User has selected Conti Ransomware.



Conti Ransomware

- **Description:**

Conti is a ransomware that has been observed since 2020, believed to be distributed by a Russia-based group.

- **Behaviour:**

Once on a system it will try to delete Volume Shadow Copies. It will try to terminate a number of services using Restart Manager to ensure it can encrypt files used by them.

- **Attack Technique**

1. Spear Phishing, Technique : T1566.
2. Other malware distribution networks (e.g., ZLoader)

- **Industries Impacted**

Banks, Healthcare etc

- **Threat Actor**

Wizard Spider pseudonym

- **IOCs:**
  - 102.x.x.12
  - lipsum.x.x.com
  - 152.x.x.16

- **SIEM Use Cases**
  - Detect shadow copy snapshots prior to encryption.
  - Detect HTA Startup Persistence

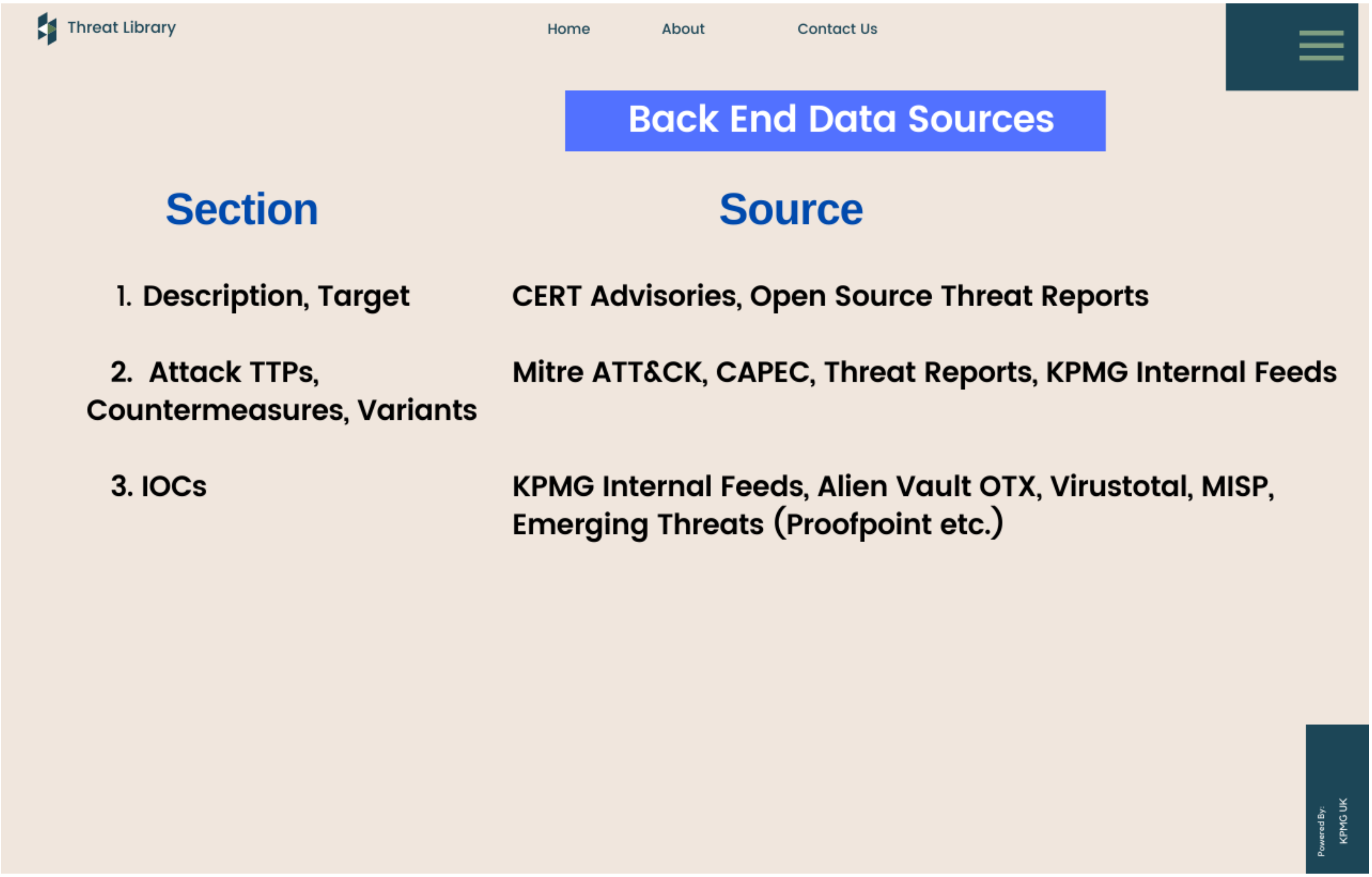
- **Countermeasures:**

1. Use multifactor authentication.
2. Implement network segmentation and filter traffic.
3. Harden Endpoints
4. Ransomware-Proof Data with Offline Backups

- **Threat Hunting Use Cases**
  - Detect Deletion of data on multiple drives using cipher exe
  - Detect exfiltration using Netflow logs

Data Sources at the Back End

Below is the mapping of various Sections in the application and respective data sources.



Back End Data Sources

Section	Source
1. Description, Target	CERT Advisories, Open Source Threat Reports
2. Attack TTPs, Countermeasures, Variants	Mitre ATT&CK, CAPEC, Threat Reports, KPMG Internal Feeds
3. IOCs	KPMG Internal Feeds, Alien Vault OTX, Virustotal, MISP, Emerging Threats (Proofpoint etc.)