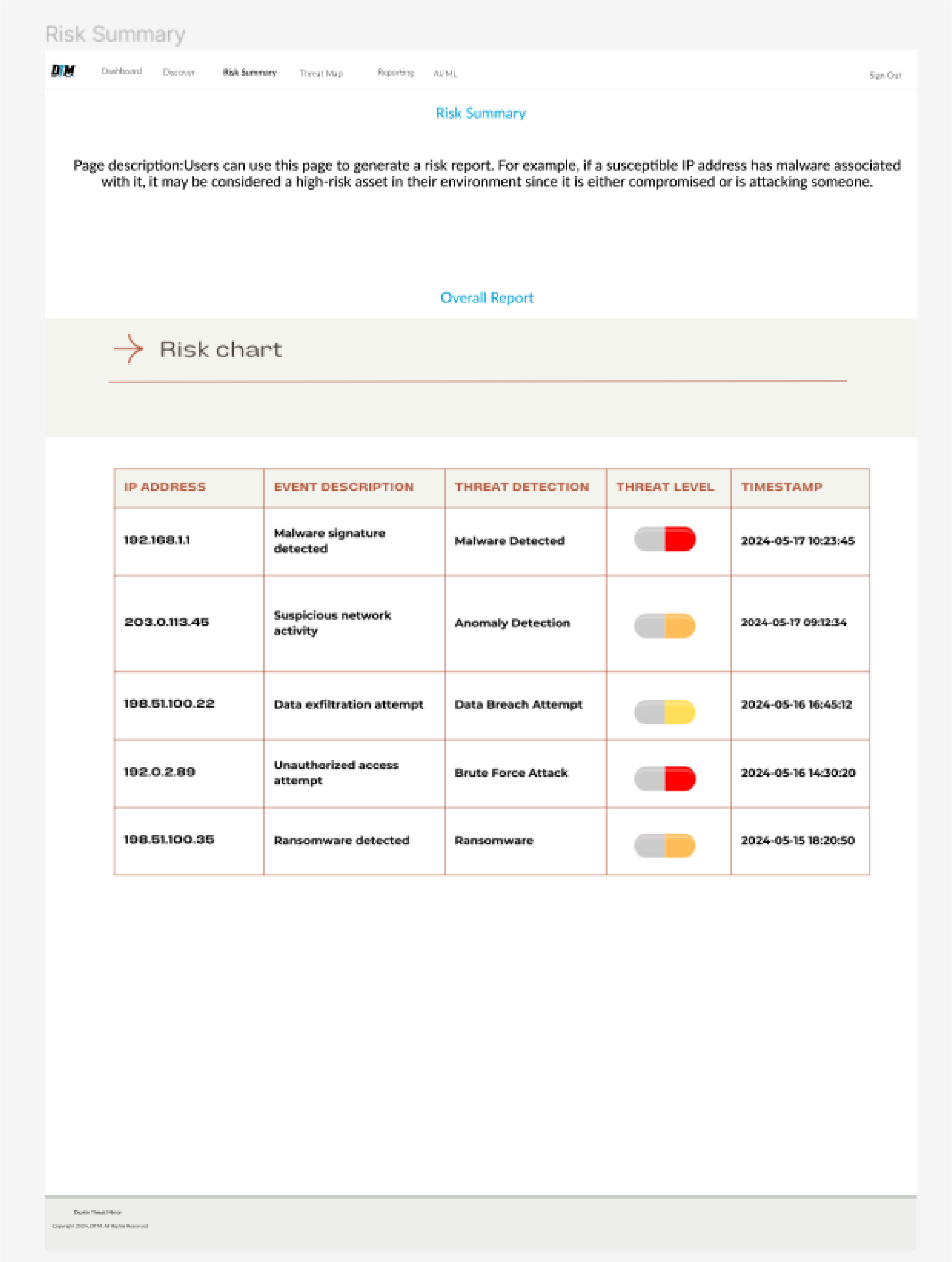
UI Documentation

Figma Link: https://www.figma.com/design/ewk0QRyxAP6jbkdkuZtyWW/Deakin-Threat-Mirror-UI?m=dev&node-id=0%3A1&t=h5bRn5mPv3YaTOK6-1



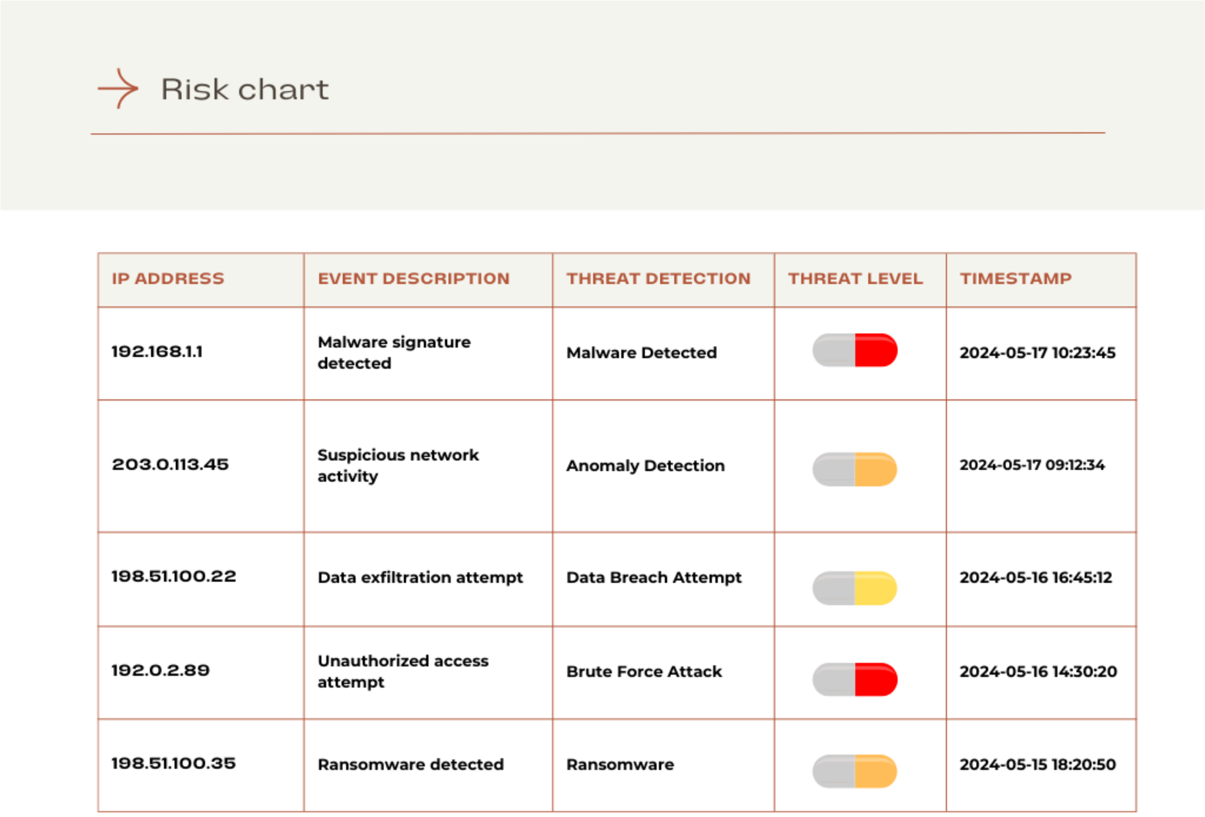
Risk Summary

Page description:Users can use this page to generate a risk report. For example, if a susceptible IP address has malware associated with it, it may be considered a high-risk asset in their environment since it is either compromised or is attacking someone.

Overall Report

Risk chart

IP ADDRESS	EVENT DESCRIPTION	THREAT DETECTION	THREAT LEVEL	TIMESTAMP
192.168.1.1	Malware signature detected	Malware Detected	🟥	2024-05-17 10:23:45
203.0.113.45	Suspicious network activity	Anomaly Detection	🟧	2024-05-17 09:12:34
198.51.100.22	Data exfiltration attempt	Data Breach Attempt	🟨	2024-05-16 16:45:12
192.0.2.89	Unauthorized access attempt	Brute Force Attack	🟥	2024-05-16 14:30:20
198.51.100.35	Ransomware detected	Ransomware	🟧	2024-05-15 18:20:50



Risk chart

IP ADDRESS	EVENT DESCRIPTION	THREAT DETECTION	THREAT LEVEL	TIMESTAMP
192.168.1.1	Malware signature detected	Malware Detected	🟥	2024-05-17 10:23:45
203.0.113.45	Suspicious network activity	Anomaly Detection	🟧	2024-05-17 09:12:34
198.51.100.22	Data exfiltration attempt	Data Breach Attempt	🟨	2024-05-16 16:45:12
192.0.2.89	Unauthorized access attempt	Brute Force Attack	🟥	2024-05-16 14:30:20
198.51.100.35	Ransomware detected	Ransomware	🟧	2024-05-15 18:20:50

The Risk Summary Page table provides a comprehensive overview of security events within the network, detailing critical information to help users understand and respond to potential threats. The table includes the following columns:

IP Address: This column lists the specific IP addresses associated with each security event. Each entry represents a unique device or endpoint within the network that has been monitored and flagged for suspicious activity or potential threats.

Event Description: The Event Description column provides a brief summary of the security event that has been detected. Examples of events include Unauthorized Access, Suspicious Login, Malware Alert, Anomalous Traffic, and Data Exfiltration. This description helps users quickly identify the nature of the incident.

Threat Detection: This column specifies the type of threat detected in each event. The possible threats include:

- Malware Detected: Indicates that malicious software was identified on the device.
- Anomaly Detection: Highlights unusual or abnormal behaviour that deviates from the norm, suggesting potential compromise.
- Data Breach Attempt: Signifies an attempt to steal or exfiltrate sensitive data from the network.
- Brute Force Attack: Denotes multiple failed login attempts, indicating an effort to gain unauthorized access.
- Ransomware: Refers to the detection of ransomware, which can encrypt files and demand payment for their release.

Threat Level: The Threat Level column categorizes the severity of each detected threat. Levels include Low (yellow), Medium (orange), High (red). This classification helps users prioritize their response based on the potential impact of the threat.

Timestamp: This column records the exact date and time when the security event was detected. The timestamp provides context for when the incident occurred, which is crucial for tracking the sequence of events and responding promptly.

Summary:

When users navigate to the Risk Summary Page, they will see a table displaying each IP address involved in security events, along with a description of the event, the specific threat detected, the assessed threat level, and the timestamp of detection. This structured format allows users to quickly assess the security posture of their network, understand the types of threats they are facing, and take appropriate actions to mitigate risks. The table's design emphasizes clarity and usability, ensuring that users can efficiently interpret and respond to security incidents.