ANOMALI

USE CASE

Applying Copilot to Mitigate Employee-Related Geopolitical and Cybersecurity Risks

ANOMALI

USE CASE

Applying Copilot to Mitigate Employee-Related Geopolitical and Cybersecurity Risks

In an era of heightened geopolitical tensions and sophisticated cybersecurity threats, CIOs and risk managers need to quickly understand and address the risks to their employees. This includes identifying employees in high-risk or conflict zones, understanding their roles and access levels, and protecting against targeted cyberattacks. Anomali Copilot can provide powerful tools for analyzing employee data, assessing risks, and implementing proactive measures.

Here's how Copilot manages these risks effectively:

1. Identifying Employees in High-Risk Areas and Assessing Operational Impact

Context

Companies must be aware of employees in high-risk areas or war zones. Understanding where these employees are, their responsibilities, and the potential impact on operations if they become unavailable is crucial for risk management and business continuity.

Copilot Application

Anomali Copilot can automate the identification of employees in high-risk regions and analyze the potential impact on operations in the following ways:

Implementation:

1. **Gather a Comprehensive View of Geographic Exposure Data:** Integrate employee location data with geopolitical risk databases and conflict zone maps. Copilot can use geospatial analytics to cross-reference employee locations with current geopolitical risk levels.
2. **Develop Risk Assessment Models:** Use Copilot to develop models that evaluate the operational impact based on employee roles and responsibilities. For example, Copilot can analyze the criticality of employees' roles in high-risk areas, allowing the business to predict potential disruptions to business operations if they become unavailable.
3. **Deploy Alert System:** Implement an AI-based alert system that notifies risk managers when employees enter or are located in high-risk zones, providing real-time updates and assessments of potential impacts.

Outcome

Using Copilot to identify and assess employees in high-risk areas better prepares companies for potential disruptions, develop contingency plans, and minimize operational impacts. This ensures business continuity and effective management of geopolitical risk.

2. Proactive Protection Against Targeted Cyber Attacks

Context:

Cybercriminals may target employees in specific regions, particularly in politically unstable areas. Understanding which employees might be at risk and what information they have access to is crucial for proactively defending against potential cyberattacks..

Copilot Application:

Here's how Anomali Copilot can be used to analyze and mitigate risks associated with targeted cyberattacks:

Implementation:

1. **Perform Geo-based Access Level Analysis:** Copilot can analyze employee access levels and permissions to identify those with access to sensitive or critical information. This analysis helps in understanding the potential impact of a cyberattack on different regions.
2. **Integrate Threat Intelligence:** Copilot includes the industry's most robust threat intelligence capability (ThreatStream), which provides threat intelligence feeds to monitor for emerging cyber threats specific to regions where employees are located. Copilot can be used to analyze patterns in attack data and predict potential threats to employees in specific locations.
3. **Leverage Comprehensive Risk Profiling:** Use Copilot-driven risk profiling to evaluate the cybersecurity risks associated with employees based on geographic location, role, and access to sensitive information. Copilot can predict which employees might be targeted and prioritize protective measures accordingly.
4. **Implement Adaptive Security Measures:** Implement Copilot to adjust protection mechanisms based on employees' risk profiles. For instance, if an employee is identified as being in a high-risk region, Copilot can automatically enforce additional security measures, such as enhanced authentication protocols and network monitoring.

Outcome

Copilot can help identify and protect employees at higher risk of being targeted by cyberattacks. This proactive approach ensures that sensitive information is safeguarded and that security measures are adapted to the specific risks associated with different regions.

3. Monitoring and Responding to Regional Cybersecurity Threats

Context

Ongoing conflicts or regional tensions may increase cybersecurity threats targeting specific areas. Monitoring and responding to these threats is essential to protect employees and organizational assets.

Copilot Application

Here's how Anomali Copilot can monitor regional cybersecurity threats and respond to them effectively:

Implementation:

1. **Perform Geo-based Threat Monitoring:** Deploy Copilot to continuously monitor cybersecurity threats in specific regions Copilot's threat detection capabilities can analyze network traffic, logs, and security events to identify signs of attacks or breaches.
2. **Detect Anomalies with Behavioral Analytics:** Use Copilot's behavioral analytics to detect anomalies in network activity that may indicate targeted attacks. For example, it can flag unusual login patterns, data access attempts, or communication with known malicious entities for investigation.

3. **Automate Incident Response:** Implement Copilot-enabled incident response systems that automate responses to detected threats. Copilot and Anomali Security Analytics can execute predefined security protocols, such as isolating affected systems, blocking malicious IP addresses, or alerting IT security teams.
4. **Share Regional Threat Intelligence:** Leverage Copilot and ThreatStream/Integrator to share threat intelligence across organizations or industry groups, particularly for regions experiencing heightened threats. AI can aggregate and analyze threat data from multiple sources to view regional risks comprehensively.

Outcome

Copilot enhances the ability to monitor and respond effectively to regional cybersecurity threats. By automating threat detection and response, companies can quickly address potential security incidents, protect their assets, and ensure the safety of employees in high-risk regions.

Conclusion

Copilot provides critical capabilities for managing employee-related geopolitical and cybersecurity risks. CIOs can effectively mitigate risks and ensure business continuity by using Copilot to identify employees in high-risk areas, protect against targeted cyberattacks, and monitor regional threats. Copilot's approach enables proactive risk management, safeguarding sensitive information, and maintaining operational stability in an increasingly complex risk environment.

Security Operations Done Differently.

Anomali is the leading AI-Powered Security Operations Platform that delivers mind-blowing speed, scale and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, NG SIEM, XDR, UEBA, SOAR, and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about the Anomali AI-Powered Security Operations Platform.

ANOMALI