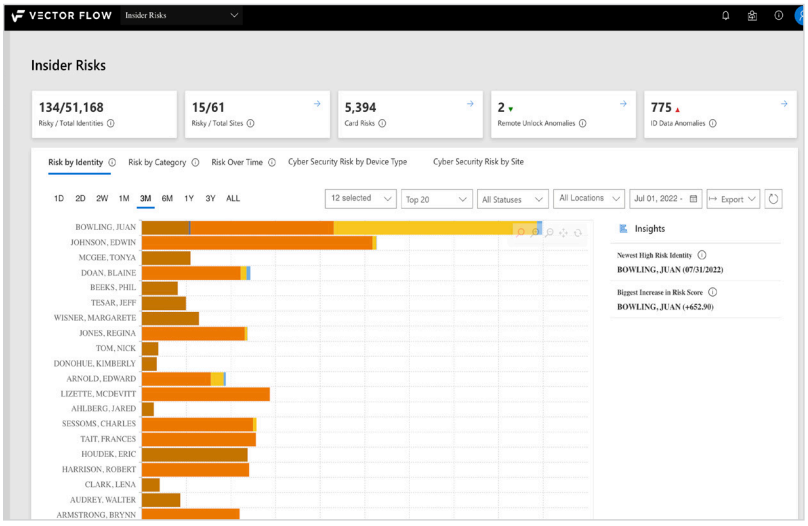
Physical Security Threat Intelligence

Physical Security Threat Intelligence has become a priority for CISOs and CSOs as Cyber Attacks and Workplace Violence incidents dominate the news. Insider attacks at large and small organizations have had consequences impacting those organizations' reputations and revenue negatively. According to the CISA[1] , FBI[2] , OSHA[3] , US Bureau of Justice[4], pre-attack behaviors of "insiders" could have been observed via technical means to mitigate these incidents. Vector Flow's Physical Security Threat Intelligence is built from the ground up leveraging lessons learned from real incidents and research on using technology to detect an insider's intent to cause harm. Vector Flow's approach integrates both people-centric and technology-centric approaches to help organizations identify and mitigate the risk of insider attacks.

Vector Flow's ID Risk Dashboard provides these unique benefits:

- Stay ahead of the security curve by proactively spotting risky or suspicious users and access anomalies that pose insider threats
- Discover misconfigured security access policies to help better maintain continuous compliance across the entire organization
- Enable sharing of KPIs to improve risk analysis and investigation between physical and cyber security teams
- Demonstrate the effectiveness of your PIAM program by utilizing highly accurate metrics with dashboards that are shared with other stakeholders, including executives
- Leverage experience from security practitioners, investigators, and 3,000+ real cases of insider threats with deep learning techniques that eliminate the need to create complex correlation rules

An insider threat is typically a current or former employee, contractor, third-party vendor, or visitor. In their present or former role, the person has or had access to an organization's systems, or facilities and misuses their access (knowingly or unknowingly). It can be negligence, greed, malicious intent, revenge, or making a profit. **It's estimated that up to 90% of insider threat activities go undetected for months or even years.** Historically, it has been challenging to identify patterns of anomalous physical access behavior to help predict insider threats. Current physical security solutions cannot correlate basic insider threat activities such as card sharing, cloning, tailgating, temporary card misuse, frequent access denials, and other red flags. In addition, many insider risks originate due to bad data within physical security systems such as active cards for terminated personnel, over-provisioning of access, no unique identifiers for each cardholder, etc. Also, physical security processes are often manual such as on/off-boarding of personnel, changes to physical access, and a high number of remote doors unlocking causing more risks.

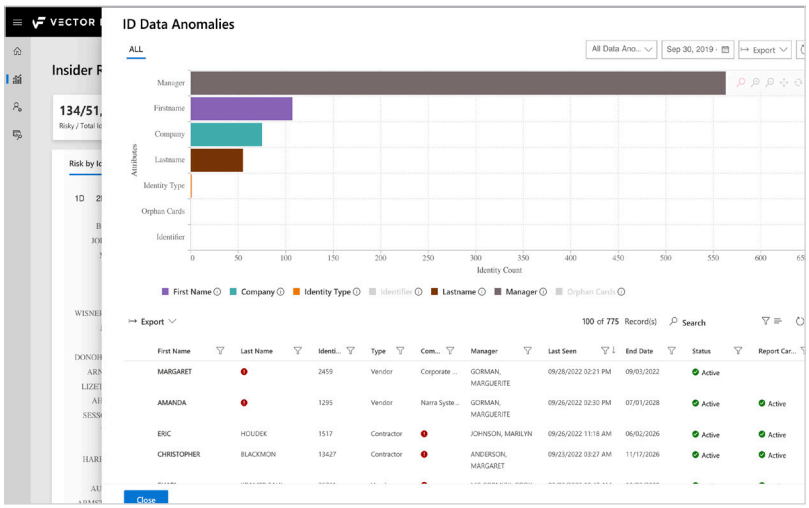


With the right tools in place, Physical Security Threat Intelligence provides security personnel with a proactive way to monitor the entire ecosystem of physical security systems to scan for breaches, insider threat behavior, data quality, and security process issues that would otherwise go undetected. While organizations want to proactively identify insider threats, knowing what to look for and where presents a significant challenge when dealing with such vast amounts of data.

Vector Flow's Physical Security Threat Intelligence solution employs advanced AI and machine learning to autonomously analyze and correlate myriad sources of data from

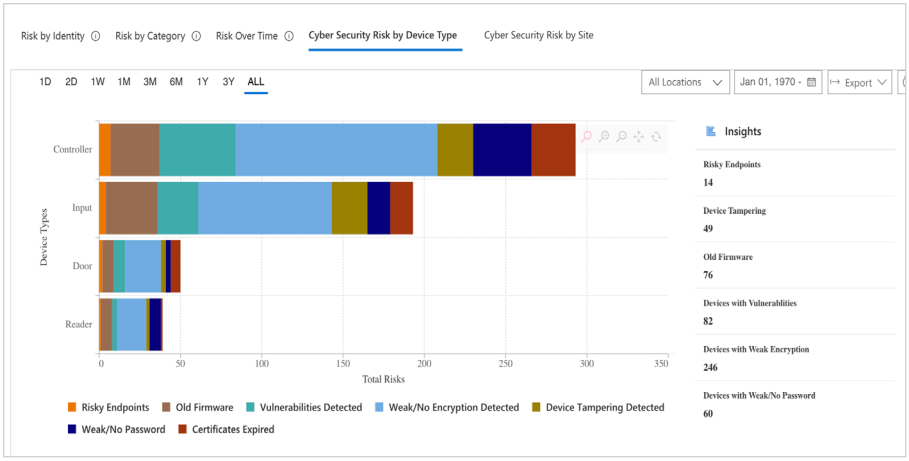
[1] Per CISA, https://www.cisa.gov/insider-threat-cyber
[2] Per FBI, https://www.fbi.gov/file-repository/stats-services-publications-workplace-violence-workplace-violence/view
[3] Per OSHA, https://www.osha.gov/workplace-violence
[4] Per U.S. Bureau of Justice https://www.ojp.gov/news/news-release/joint-study-workplace-violence

system logs, physical security access control systems, and Wi-Fi systems to uncover anomalies and abnormalities in real time that pose potential threats. Vector Flow helps quickly spot risky Identities, Sites, devices, doors, etc. across the entire enterprise to discover suspicious anomalies that pose insider threats, effectively alleviating risks and liabilities to your organization.



Intuitive *Physical Security Risk Dashboards* provide insights into operational and security risks on an individual user, device, or facility-level basis, along with recommendations for remediation or action. The dashboards simplify details, list key risk indicators with simple visuals, and highlight which controls are working and which are redundant.

Vector Flow's powerful and insightful Physical Security Risk Dashboards are already proving effective in helping customers discover anomalous access patterns and identities, compromised access credentials, compromised doors, tailgating, and other incidents that compromise security. Customers are also using the dashboards to share KPIs and risk analysis by Business Units, or departments, further improving collaboration between physical and cyber security teams.



Physical access and security irregularities no longer need to languish without detection and remedial action. Vector Flow's Physical Security Threat Intelligence solution continuously applies intelligent algorithms to analyze and correlate real operational data on who has access to restricted doors and where, when, and how they access these areas, with the ability to automatically issue alerts to management when irregularities are detected.

With Vector Flow's innovative Threat Intelligence solution, physical and cyber security teams can stay ahead of the security curve by proactively detecting and analyzing potential insider threats.

Contact us to learn more about how Vector Flow's Physical Security Threat Intelligence can help you quickly spot risky identities, sites, IoT edge devices, doors, etc. across the entire enterprise to discover suspicious access anomalies that pose as insider threats, effectively alleviating risks and liabilities to your organization

Learn more at vectorflow.com