Certificate in Threat Assessment and Management

Types of Threats

Active Shooter: An individual actively engaged in killing or attempting to kill people in a confined and populated area. In the context of threat assessment and management, an active shooter situation requires a swift and decisive response from law enforcement and other first responders.

Behavioral Threat Assessment: A structured process of information gathering, analysis, and management to identify, assess, and manage individuals who may pose a threat to themselves or others. This approach is grounded in the understanding that threats are often communicated through behavior, and that early intervention can prevent violence.

Campus Violence: Any behavior or act that is violent in nature, including but not limited to, physical assault, sexual misconduct, threats, intimidation, stalking, and hate crimes. Campus violence can have a profound impact on the safety and well-being of students, faculty, and staff, and requires a comprehensive approach to threat assessment and management.

Community Threat Assessment: A collaborative process that involves multiple agencies and stakeholders in the assessment and management of threats to a community. This approach recognizes that threats to a community often transcend the boundaries of any single agency or organization, and requires a coordinated response.

Critical Incident: An event that has the potential to cause significant harm or disruption to an organization or community. Critical incidents can include natural disasters, technological failures, and human-caused events such as active shooter situations or terrorist attacks.

Cyberstalking: The use of the internet, email, or other electronic communications to stalk, harass, or threaten an individual. Cyberstalking can have serious consequences for the victim, and requires a comprehensive approach to threat assessment and management.

De-escalation: The process of reducing the intensity of a conflict or crisis situation. De-escalation techniques can include active listening, empathy, and the use of non-threatening body language.

Domestic Violence: A pattern of abusive behavior in any relationship that is used by one partner to gain or maintain power and control over another intimate partner. Domestic violence can take many forms, including physical, sexual, emotional, and financial abuse.

Hate Crime: A criminal offense committed against a person or property that is motivated, in whole or in part, by the offender's bias against a race, religion, disability, sexual orientation, ethnicity, gender, or gender identity.

High-risk Behavior: Behavior that poses a significant threat to the safety or well-being of an individual or others. High-risk behavior can include substance abuse, reckless driving, and violent or threatening

behavior.

Insider Threat: A threat that originates from within an organization, often from an employee, contractor, or other trusted individual. Insider threats can include theft of proprietary information, sabotage, and acts of violence.

Mass Casualty Incident: An event that results in a large number of injuries or fatalities. Mass casualty incidents can include natural disasters, transportation accidents, and human-caused events such as active shooter situations or terrorist attacks.

Risk Assessment: The process of evaluating the likelihood and potential impact of a threat. Risk assessments can inform decision-making around threat management, and help organizations prioritize resources and responses.

Stalking: A pattern of behavior directed at a specific person that would cause a reasonable person to feel fear. Stalking can take many forms, including following, monitoring, and harassing the victim.

Suicide by Cop: A situation in which an individual intentionally engages in behavior that leads a law enforcement officer to use deadly force. Suicide by cop is a complex phenomenon that requires a comprehensive approach to threat assessment and management.

Targeted Violence: Violence that is directed at a specific individual, group, or location. Targeted violence can include acts of terrorism, active shooter situations, and workplace violence.

Threat Assessment: The process of identifying, assessing, and managing individuals who may pose a threat to themselves or others. Threat assessments can inform decision-making around threat management, and help organizations prevent violence.

Threat Management: The process of responding to and mitigating threats to an individual, group, or organization. Threat management can include a range of interventions, from counseling and monitoring to law enforcement intervention and criminal prosecution.

Threatening Behavior: Behavior that is intended to intimidate, harass, or threaten an individual or group. Threatening behavior can include verbal threats, written threats, and gestures.

Workplace Violence: Violence or the threat of violence that occurs in the workplace. Workplace violence can include physical assault, sexual harassment, and intimidation.

Written Threat: A threat that is communicated in writing, including letters, emails, and social media posts. Written threats can be a serious indication of intent to do harm, and require a comprehensive approach to threat assessment and management.

Example: A student posts a message on social media threatening to shoot up the school. The threat is reported to law enforcement, who conduct a threat assessment and determine that the student poses a serious threat. The student is removed from school and receives counseling and monitoring.

Practical Application: Threat assessment and management teams can use this glossary to ensure that all members are using common terminology and have a shared understanding of key concepts. This can help facilitate effective communication and collaboration, and ensure that threats are managed in a timely and effective manner.

Challenges: Threat assessment and management can be complex and challenging, particularly in situations involving multiple agencies and stakeholders. It is important for teams to have a clear understanding of roles and responsibilities, and to communicate effectively to ensure that threats are managed effectively. Additionally, teams must be mindful of privacy and confidentiality concerns, and ensure that all actions are taken in compliance with relevant laws and regulations.