Threat & Risk Information Sharing and Federation

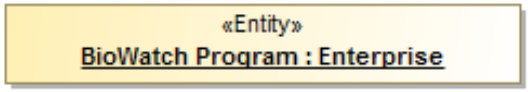
BioWatch Pathogen of Interest Use-Case & Scenario

Background and context

BioWatch is a United States Federal Government program to prepare state and local governments to prepare a response for and to provide detection of the release of pathogens into the air as part of a terrorist attack on major American cities. more than 30 major metropolitan areas nationwide. The BioWatch program was created in 2001 in response to the increased threat of bioterrorism sparked by the terrorist attacks on Sept 11 2001 and was announced in President George W. Bush's State of the Union Address of 2003.
The program, described as "the nation's first early warning network of sensors to detect biological attack" operates via a system of collectors located within Selected cities Nationwide.
The context of this scenario is the risk of and subsequent fictitious biological attack in Selina County, CA

Model Mappings

Throughout this document we will show examples of how concepts in this scenario are represented using the threat/risk model. These mappings will be shown in a box, as demonstrated below. Note that to manage size, only examples are shown – not all possible elements.



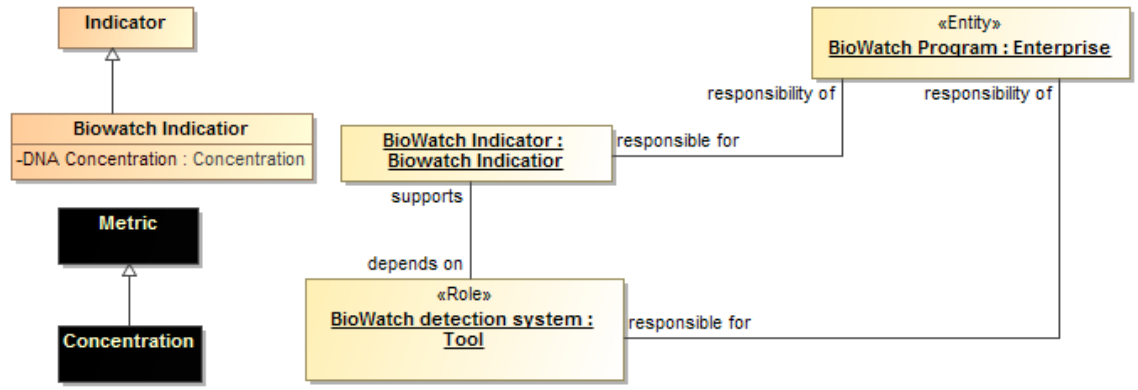
Biowatch is an enterprise: An enterprise is a stakeholder organization with a mission, members and authority over resources to accomplish its mission(s). An enterprise provides context for operations and analysis.

Threat indicators

BioWatch Indicators

A sighting from a BioWatch detection system detects the presence of a pathogen or multiple pathogens in a particular location at a particular time that indicates the possibility of a terrorist attack, accidental release of pathogens or natural outbreak. The detection systems report pathogens based on the concentration of the DNA for a pathogen which is rated as low, medium or high. The BioWatch detectors can also provide

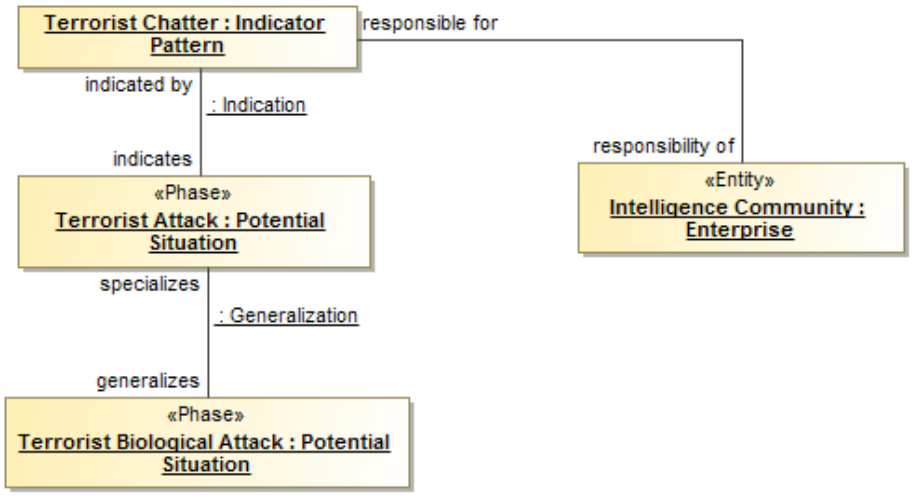
information about location of the event (indoor vs outdoor) and potentially any geographical patterns.



A Biowatch indicator has a specific metric – a DNA concentration. Such an indicator indicates a potential biological terrorist attack and depends on detection systems, the responsibility of the BioWatch program.

Intelligence Indicators:

The intelligence community releases notices of suspected terrorist activity from multiple sources, including the monitoring of social media and other classified sources. Such activity is an indicator of an ongoing or possible future attack.



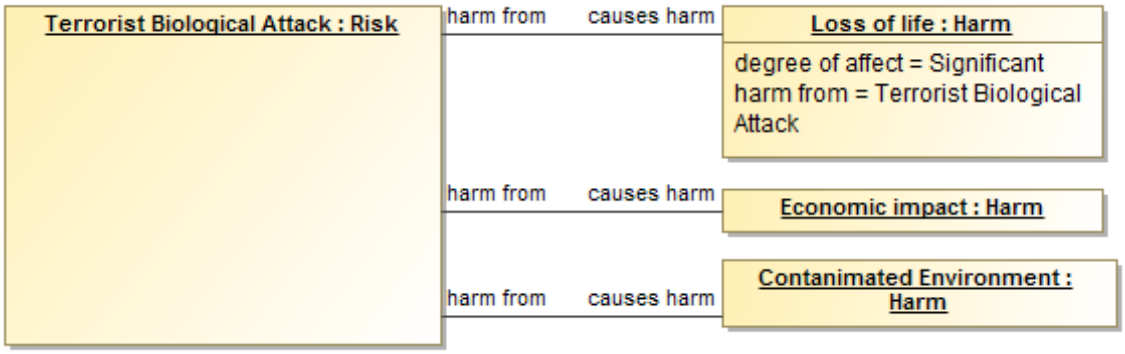
Terrorist chatter, an indicator which is the responsibility of the intelligence community, indicates a potential terrorist attack. A Terrorist Biological Attack is a kind of Terrorist attack.

Risks

The Risk of a potential bioterrorism attack is determined by: information from the intelligence community (fusion centers, FBI weapons of mass destruction experts, DHS Intelligence and Analysis Analysts, law enforcement, and others); results from BioWatch

detection system for pathogens of concern (e.g. anthrax or plague); and biosurveillance (e.g. public health reports of unusual syndromic surveillance activity (e.g. unusual spike of visits to the ER for fever) or unusually veterinary or agricultural data) or actual disease diagnosis of a disease of concern for bioterrorism. It would also be useful to know if there were any recent environmental disturbances such as: brush cutting or lawn mowing near the BioWatch collectors that could have disturbed carcasses thus aerosolizing the pathogen.

The potential Harm from such a bioterrorism attack is significant and includes: potential for significant life loss (approximately 10M plus people would need to be treated if all of LA County is affected), however it is not clear that this was an actual attack and or if people will become infected. If people are going to get infected they must be treated with antibiotics in order to recover. Potential for economic impact and loss of life; potential biohazard issue – contaminated environment; and more.



Specific Sightings (Fictional)

Biowatch indicators

Sightings: On July 4, 2014 two BioWatch collectors in Selina County detect moderate levels of the presence of a pathogen of concern – *Yersinia pestis*, (The cause of Bubonic plague).

BioWatch Sighting CA20140604-1:

Observer: Biowatch detector CA2387

Location: West Midland, CA.

Pathogen: *Yersinia pestis*

Date and time: July 4, 2014

DNA Concentration: Medium

BioWatch Sighting CA20140604-2:

Observer: Biowatch detector CA2392

Location: East Longview, CA.

Pathogen: *Yersinia pestis*

Date and time: July 4, 2014

DNA Concentration: High

Intelligence Community Sightings

The intelligence community has identified "chatter" online indicating the potential for non-state actor involvement in a biological attack in California.

Intelligence sighting:

Target Location: California

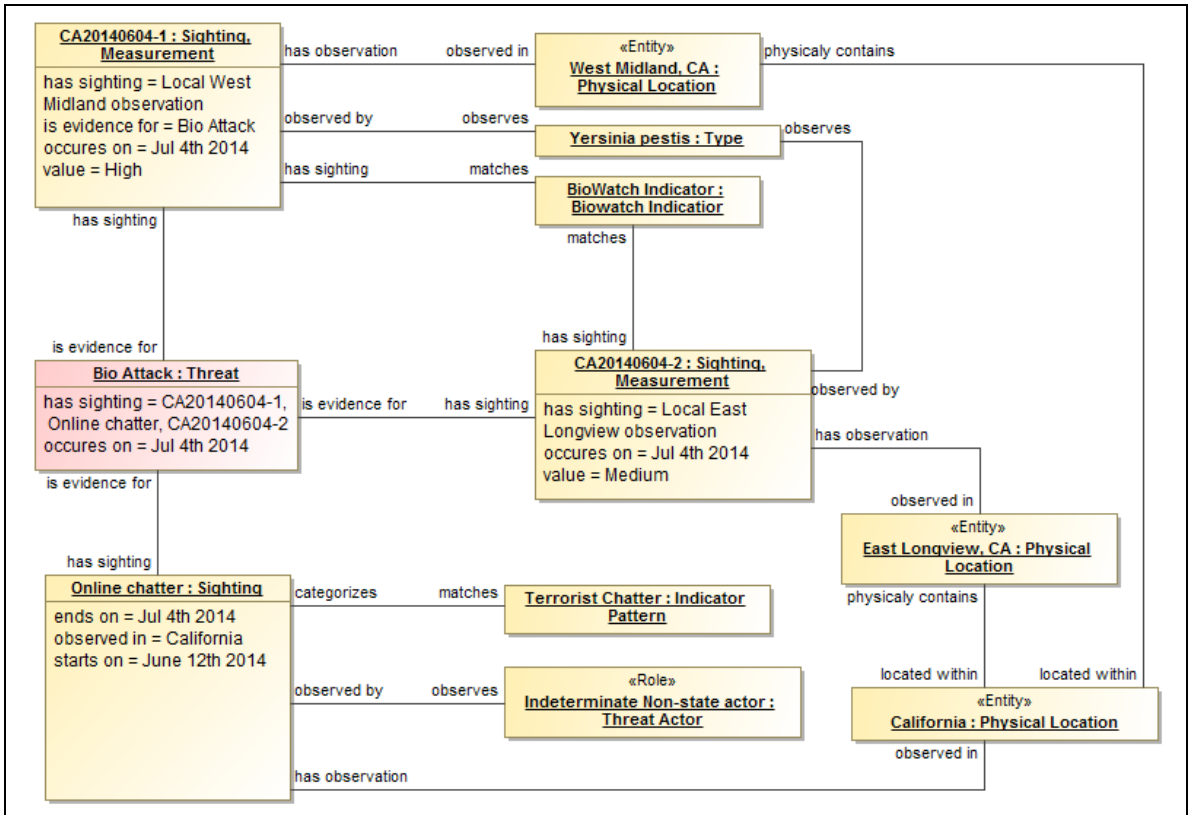
Threat actor: Indeterminate Non-state actor

Indicator Type: Online chatter

Date range: June 12th 2014 – July 4th 2014

Attack type: Biological attack

Risk Indicator: Medium



Example of how multiple sightings, based on indicators, can come together as evidence for threat of biological attack.

Law enforcement sightings

Based on the above local law enforcement was asked to see if there were any recent environmental disturbances such as: brush cutting or lawn mowing near the BioWatch collectors. No unusual activity was reported.

Local West Midland observation:

Observer: Longview County police

Location: West Midland, CA.

Observation: No unusual activity

Date and time: July 4, 2014, 3 PM PST

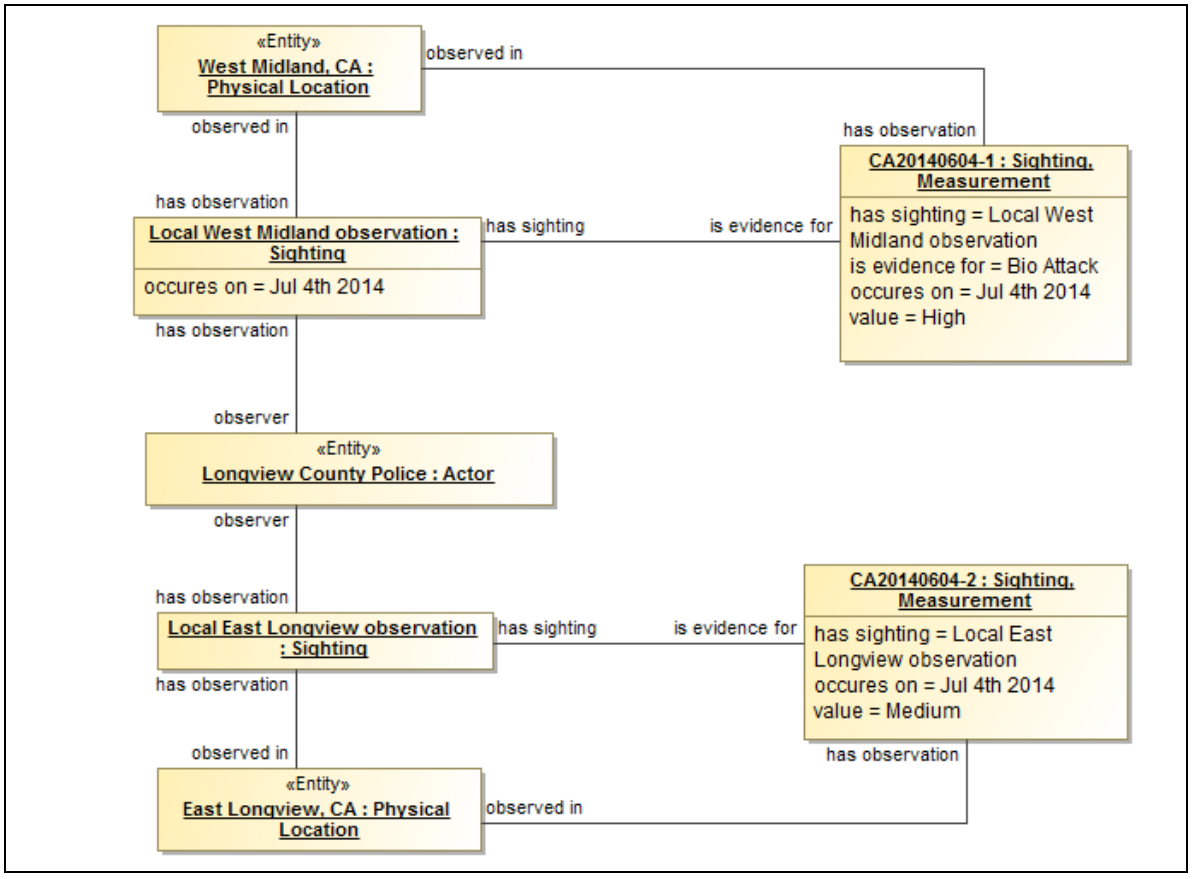
Local East Longview observation:

Observer: Longview County police

Location: East Longview, CA..

Observation: No unusual activity

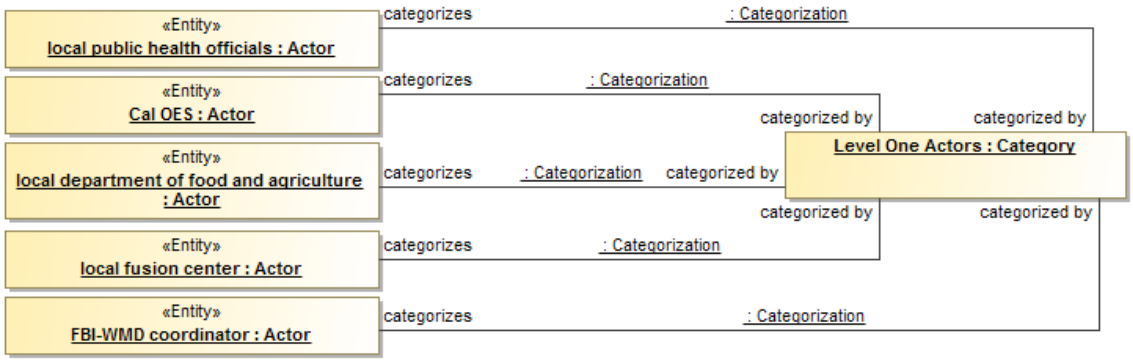
Date and time: July 4, 2014, 4 PM PST



The above shows that the local police inspection of the sites provides additional evidence for the validity of the measurements.

Actors

Important initial (level 1) Actors include: local public health officials; local emergency managers (Cal OES); local department of food and agriculture; local fusion center representative; FBI-WMD coordinator; and potentially others who are members of the BioWatch advisory committee.



The above identifies the level-one actors, the others are not shown in the interest of brevity and redundancy.

Important initial (level 2) Actors include: local and state, public health officials; local and state, emergency managers (Cal OES); local and state department of food and agriculture; fire and local and state police departments; state Homeland Security Advisor (which in California is the Director of Cal OES); state fusion centers (intelligence); Department of Homeland Security (Office of Health Affairs (BioWatch) and National Biosurveillance Integration Center); FBI-WMD coordinator(s); and potentially others

Important Actors (level 3) if this is declared an event that needs a public health response: local and state, public health officials; local and state, emergency managers (Cal OES); local and state department of food and agriculture; local, state, and federal EPA; fire and local and state police departments; state Governor; state Homeland Security Advisor (which in California is the Director of Cal OES); neighboring state agencies; National Guard; regional and state fusion centers (intelligence); Department of Homeland Security (FEMA, Office of Health Affairs (BioWatch), National Biosurveillance Integration Center, Intelligence and Analysis); FBI; Health and Human Services (Centers for Disease Control and Prevention (CDC) and Assistant Secretary for Preparedness and Response); White House; and others.

Treatment Strategies

Risk Treatment Strategies at a governmental level may include:

(i) Local, possibly regional, and possibly national calls regarding BioWatch detection of an agent of concern. (Impact mitigation)

(ii) Identifying in-state resources (antibiotics and vaccines), if necessary. (Impact mitigation)
(iii) Requesting MCM (antibiotics and vaccines) from the strategic national stockpile if the local, regional, and state supply cannot treat the number of infected individuals, if necessary. (Impact mitigation)
(iv) Coordinating and releasing appropriate risk communications messages (what to do and where to go for MCM) for the affected communities (need to identify the communities by looking at the timing of the event and the population present at the time of the attack – i.e. need to reach out to commuters as well as local residents). (Impact mitigation)
(v) Establishing points of distributions (PODs) for MCM with appropriate security, if necessary, depends on the size of the event. (Impact mitigation)
(vi) Possibly declaring martial law to reduce additional human harm. (Impact mitigation)
(vii) Distribution of MCM to the public, if necessary. (Impact mitigation)
(viii) Establishing treatment sites if necessary, depends on the size of the event. (Impact mitigation)
(ix) Establishing evacuation routes and capabilities for the affected communities if necessary, depends on the size of the event.
(x) Begin remediation efforts if necessary. (Impact mitigation)
(xi) Repatriation – if evacuations have occurred. (Impact mitigation)

Private parties and NGOs may prepare by:

(i) Identifying resources (privately held antibiotics and transportation capabilities to move MCMs). (Impact mitigation)
(ii) Helping to establish, stock (transporting MCMs from a centralized location to the PODs), and secure PODs. (Impact mitigation)
(iii) Setting up mass treatment facilities if necessary, depends on the size of the event. (Impact mitigation)

The attack

The Attack results in a Disaster that matches the predicted Threat, response Capabilities from public health and emergency management is determined by the available Resources, and the ability to request, receive, distribute, and communicate to and with decision makers and the public. In such a scenario the local public health official would determine (given the information presented on the local call) if the event needs to a public health response. If the event exceeds the ability of the local's response, the region and then the state would be requested to assist.

Further, if this is determined to be a bioterrorism attack, this would be decided during a BioWatch National Conference call consisting of members of all levels of government, representing major areas of response, including but not limited to the IC.Current Information Gaps

Current Information Gaps

The intelligence community would need to be aware of and recognize the potential Do It Yourself Bio (DIY Bio) threat or other potential similar threats (e.g. internet "chatter") and they would need to appropriately communicate these threats to the public health community. For example health care providers may need to be aware of a threat so that they do not misdiagnose someone during flu season with the flu instead of anthrax or another pathogen.

The intelligence community also needs an avenue to communicate this information to individuals in other domains, even if the information is sensitive or classified. Ideally, as much information needs to be de-classified as possible.

The public health community needs to be able to understand the intelligence information, meaning they need to understand the threat and the potential public health impact.

The biosurveillance networks need to be able to identify unusual health activity by performing syndromic surveillance and most importantly they need to be able to communicate with eachother. These networks need to have critical health relevant information (which has yet to be determined) feed the network to identify these unusual health relevant events.