Defentect

Intelligent Threat Awarness

RAPIDSOFT SYSTEMS

Technologies for Homeland Security - Advanced CBRN Threat Detection System

Contact: **Brijesh Kumar, Ph.D.**
CSO/COO
Rapidsoft Systems Inc.
Princeton, NJ 08550
Direct Line: +1 609 -439 -4775
bkumar@rapidsoftsystems.com

Defentect

- **Our Mission**
  - the discovery and deployment of advanced technologies for physical and homeland security
  - **Intelligent Threat Awareness**

NUCLEAR AND RADIOLOGICAL TERRORISM THREATS FOR INDIA: RISK POTENTIAL AND COUNTERMEASURES

by

Rajesh M. Basrur, Director, Centre for Global Studies, Mumbai ;
Friedrich Steinhäusler, Professor, Institute of Physics and Biophysics, University of Salzburg, Austria

- This report by two learned scholars in the field describes quite well the threats that India faces.

- We will use this report to specify precisely where the Defentect Team can aid India

From the Report, page 2. Section 2.1 Radiological Terrorism. "**It is questionable whether initially Indian authorities would even be aware of the fact that a terror act..has occurred, since most first responders are neither trained, nor technically equipped to detect..**"

- Defentect can deploy to First Responders inexpensive mobile radiological sensors, like those currently used in New York City.
- The individual First Responder need NOT read the sensor. DM3 sensor analytics software can detect the pattern of radiological dispersion and determine the extent and lethality of any radiation exposure.
- Authoritative announcements from the government setting out with accuracy the limits of the radiological exposure will eliminate panic far more effectively than any propaganda.
- Sensors can continue to provide information during the critical 72 hours of a crisis.

Page 3. Section 2.2 Terrorist attacks on the nuclear infrastructure in India. **“A small team of trained saboteurs gains access to a nuclear power plant, possibly with an insider’s assistance…”**

The advantage of **P**erimeter **S**ecurity **I**nformation **M**anagement (“PSIM”):

•Combined with sensors, closed-circuit television, fiber-optic cable motion detectors, sensor analytics and video analytics,

•Eliminates the uncertainty of relying on the awareness, training, and loyalty of any individual security guard.

•Established procedures and notifications, well-thought out in advance, can be assured of being implemented through PSIM.

Page 5 Section 3.1 Illegal Acquisition of Nuclear and Other Radioactive Material from India and Abroad. **“There are multiple possibilities for terrorists to obtain radioactive material in India suitable for an Radiological Dispersal Device, such as hospitals..;research facilities..; oil-and-gas explorations industry; road construction industry; and steel manufacture…over 10,000 [locations]...” “Typically, physical protection at these sites is rather lax, at best comparable to the protection provided at a jeweler shop, i.e., not a real logistical problem for a trained team of adversaries.”**

- India’s Atomic Energy Commission (AEC) should assume total control of monitoring all radiological material at the borders and within the country, legal and outlaw, not just to protect "targets".
- Every single square inch of the country is NOT at risk and does NOT have to be sensored.
- The number of targets are manageable and the number of legitimate sources are limited.
- Sensors can be inexpensively deployed at every licensed site.

Defentect

Page 7. Section 3.2 India's Nuclear Power Infrastructure.
Page 7. Section 3.3 Organizational Vulnerabilities**.** **"A serious potential threat to nuclear facilities..comes from insiders."**

Again, PSIM automates the response and lessens reliance on human training, loyalty, and awareness.

RAPIDSOFT SYSTEMS
IT Outsourcing Done Right!

What is to be done to protect the Nation?

- From the IAEA: “a cardinal rule of radiological protection, namely that the security of the source is of paramount importance.”
- Our view is that a central agency should set standards and custodial responsibilities for radioactive materials, assume total control of monitoring all radiological material at the borders and within the country, legal and outlaw, not just to protect "targets".
- Security is a matter of taking control of the locations of likely activity - both sources of dangerous materials and locations which are considered targets. It is not necessary to cover every inch of the country with detectors to provide an effective overall system

The Solution

- Intelligent threat networks that monitor movement can reduce or eliminate misappropriation.
- Defentect's DM3™ software is the only management, monitoring and messaging component that networks to any third party sensors, providing administrative and configuration services for a variety of threat-event detection demands.
- Defentect has unique, low cost, integrated, networked, ubiquitous, wide area, unmanned software architecture and sensor technologies that meet this need.
- Our intellectual property is built upon readily available electro-optical devices.
- Defentect's products graft readily onto existing security systems, minimizing adoption costs and facilitating market penetration.

Defentect DM3

Proven threat awareness solution

- Developed under Chairman Paul Bremer, Ambassador-at-Large for Counterterrorism and U.S. Administrator of Coalition Provisional Authority in Iraq.
- Installed, operational and proven in “high value” target facilities in the US.
- Gathers data from virtually any sensor which can live on a data network.
- Seeks and identifies anomalies in the data.
- Forwards the new information to an unlimited number of devices on any platform capable of receiving messages: SMS, email, smartphones, voicemail, XML.
- Automatically forwards any digitized information—such as floor plans and the names and photographs of authorized personnel—to first responders.
- All instantaneously and independent of operating personnel.
- Continuous information delivered during the first 72 hours of an attack—without relying on First Responders.

PROVEN IN THE US

- Participant in Operation Golden Phoenix Federal terrorism response laboratory, San Diego, with :
  - U.S. Department of Homeland Security
  - Customs and Border Protection,
  - U.S. Marine Corps Aircraft Group 46,
  - Department of Defense
  - Drug Enforcement Agency
  - Federal Bureau of Investigation
  - Department of Justice,
  - Department of Energy
- At Golden Phoenix, Defentect monitored threat-level radiation at Brown Field Airport and Scripps Memorial Hospital La Jolla

Among US installations:

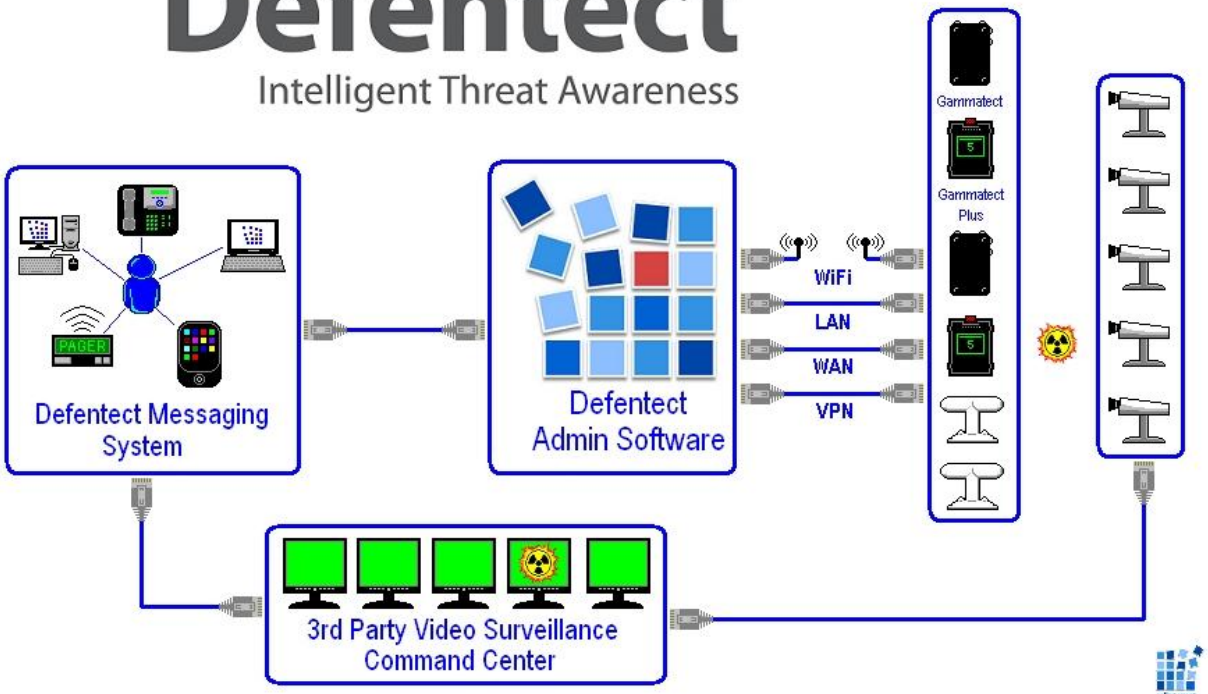
- AIT Worldwide Logistics, a global transportation provider
- Walter Reed National Military Medical Center,premier Washington D.C. are Hospital Center for all senior civilian/military.

Defentect Difference

- IP-based interface to legacy systems
- Web-based management, monitoring, and messaging system
- IP-based sensors at commercial prices
- Commercial distribution channel
- Existing pilots in operation
- Wisdom of our advisors

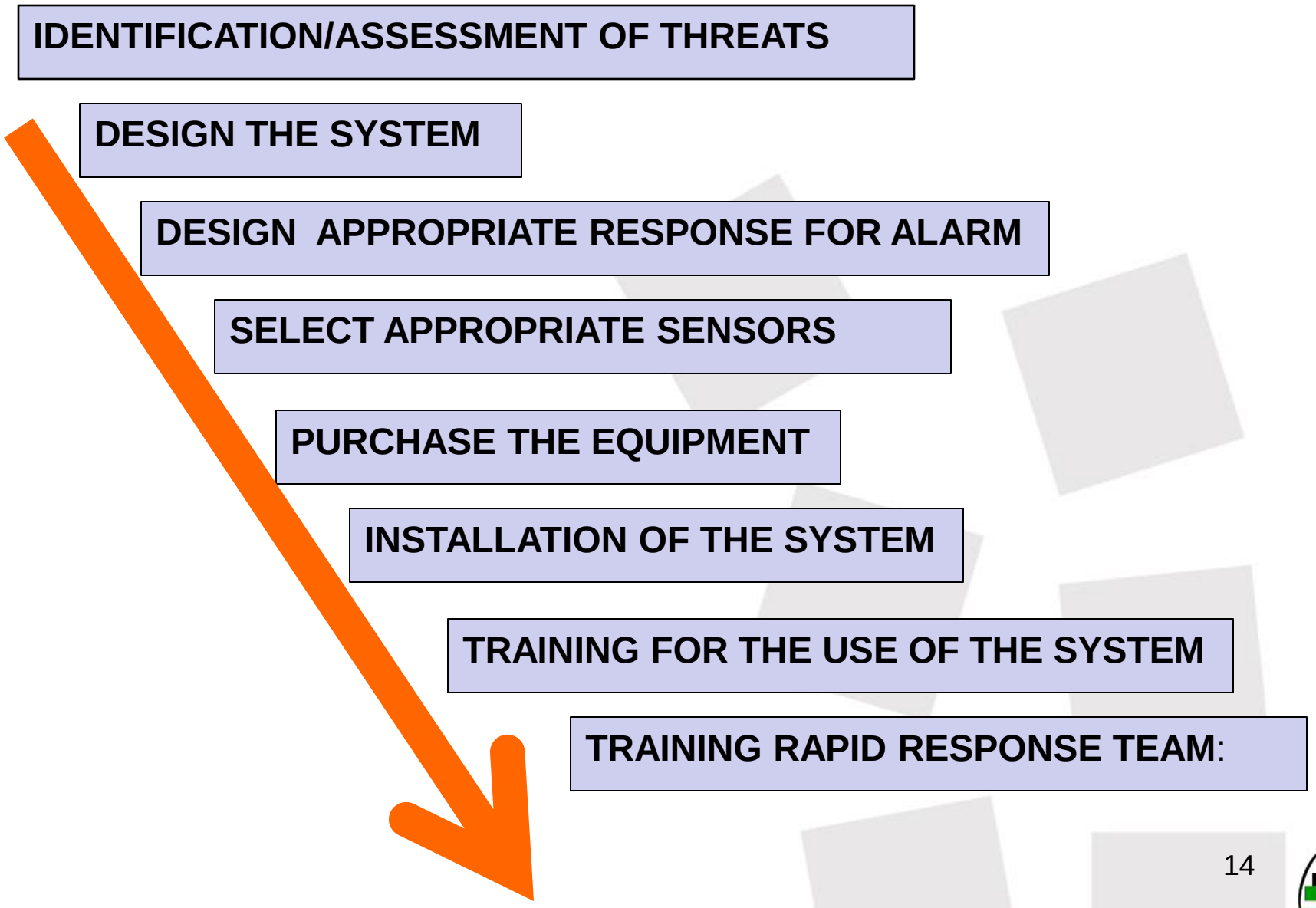
Defentect

Intelligent Threat Awareness



1-888-868-8386

DELIVERY OF THE TOTAL SECURITY PACKAGE

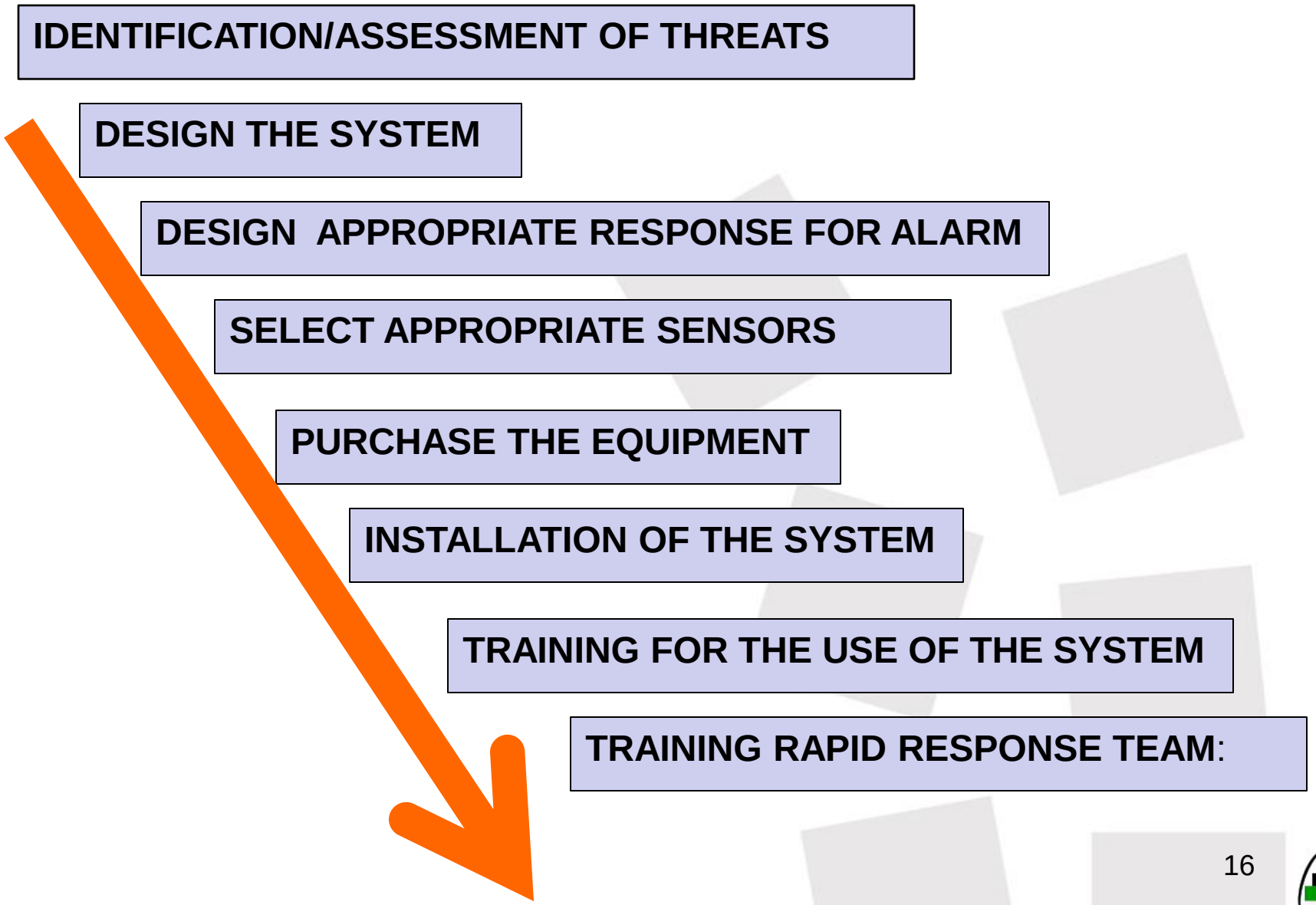


DELIVERY OF THE TOTAL SECURITY PACKAGE

1. **IDENTIFICATION/ASSESSMENT OF THREATS**: The Defentect Team will identify and assess the threats at each location that is specified. As this will be time-consuming and require site visits, travel costs and other out of pocket expenses, and subject matter experts ("SME's") charging a reasonable hourly rate to develop the plan, payment in advance of the estimated expenses plus half of the remaining cost to develop the plan. The Team will present the plan in an oral presentation. The remaining amount will be payable and due upon receipt of the written report, including any slides, of the Identification/Assessment of Threats.
2. **DESIGN THE SYSTEM**: The Team will design the layout and sensor/CCTV/detector locations for each site specified. The amount will be payable upon delivery of the written report.
3. **DESIGN THE APPROPRIATE RESPONSE FOR ALARM**: The Team will design the appropriate response, including who should be alerted and what messages should be sent out. The cost of designing the appropriate response and notification scheme will be due and payable upon delivery of the written report.
4. **SELECT APPROPRIATE SENSORS**: The Team, working with relevant vendors, will select the appropriate sensors/video analytics/CCTV/motion detectors. This cost will included into the total cost of purchasing the equipment from manufacturers and video analytics software developers.
5. **PURCHASE THE EQUIPMENT**. The Team will purchase the equipment upon receipt of the full purchase price in advance..
6. **INSTALLATION OF THE SYSTEM:** The Team will be responsible for the installation. Staged advance payments will be required.
7. **TRAINING FOR THE USE OF THE SYSTEM**: This should take no more than one week's time and will be built into the cost of installation .
8. **TRAINING RAPID RESPONSE TEAM**: This will be the responsibility of the Defentect Team , which will include options for Mobile Training Teams at the customer's training facility or training in the US. Payable in full in advance before any training can take effect.

Next step: meeting to discuss the scope of work, detailed analysis of security, pricing

Defentect



RAPIDSOFT SYSTEMS
IT Outsourcing Done Right!

Contact Information

Primary Contact:

Brijesh Kumar, Ph.D.

CSO/COO

bkumar@rapidsoftsystems.com

Rapidsoft Systems Inc.

Princeton, NJ 08550

Phone: +1 609-439-4775