

Key Features

Visual correlation and representation of wireless discovery data

Big picture overview; drill-down for details

Geographic visualization of location and movement of wireless devices

Visual tracks of threats moving inside a building

Historical analysis of wireless risks and remediation

Identification of same threat recurring across locations and time

Profiles of suspicious behavior patterns

Built-in reporting

Works on standard PC

Need

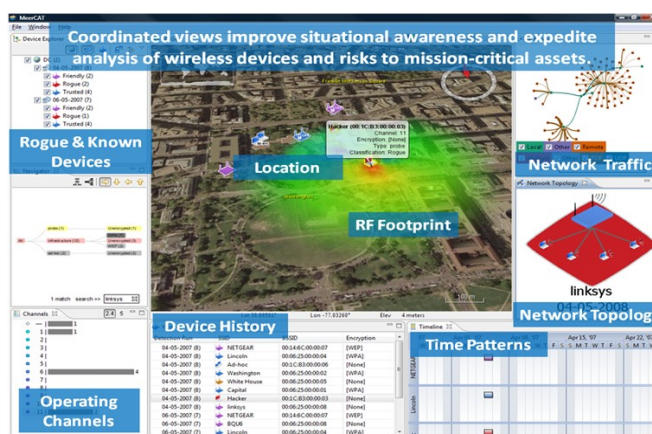
As a security professional tasked with protecting mission-critical fixed and mobile network assets, you need to locate and identify wireless security threats to these assets. Whether identifying risks to your authorized assets or discovering threats from unauthorized wireless devices, the task of collating, interpreting, and reporting on wireless data collections can be laborious. Despite this data overload, you must still:

Identify risks to your authorized wireless assets: non-compliance with security policy; behavior patterns inconsistent with the organization's mission or user's role; incorrectly positioned critical wireless assets.

Discover threats from unauthorized wireless devices: rogue devices in close proximity to your enterprise or high-value targets; suspicious devices that pop up repeatedly across disparate locations; unusual network connections from unknown devices

Solution

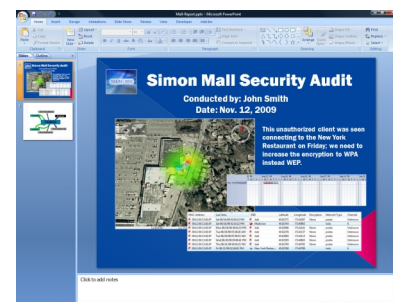
MeerCAT[®] is a patent-pending visual analytics and reporting tool that *simplifies the wireless audit risk assessment process* by unifying collected wireless data *with advanced visualization and report generation*. Wardriving tools such as Kismet and Flying Squirrel, and other wireless intrusion sensors, locate wireless devices and generate large quantities and varieties of data. MeerCAT's powerful visualization tools help you make sense of this wealth of data, "see" risks to critical assets, and turn it all into meaningful, actionable information.



MeerCAT visualizes location, network topology, device history, time patterns, and mission of wireless networks

MeerCAT's *built-in reporting tool* reduces your reporting burden by creating PowerPoint presentations and Word documents from your visual analysis with one click of your mouse. This simplifies production of compliance reports, and enhances their comprehension by non-experts.

MeerCAT presents *a unified picture of location, encryption levels, behavior patterns, time patterns, channel usage, and mission* of authorized and unauthorized wireless devices. Network traffic visualization shows communication patterns among wireless devices. Views of device movements help you assess the threat's intention and access to critical assets.





MeerCAT® – Pro

Uses

- Penetration testing
- Vulnerability analysis
- Wireless site survey
- External threat detection
- Insider threat detection
- Policy audits
- Wireless asset tracking
- Verification of remediation
- Mission readiness

Key Benefits

Expand risk assessment

Locate security risks to your enterprise from authorized & unauthorized wireless devices

Enhance threat detection

See rogue behavior and trends in massive volumes of data

Reduce workload

Rapidly analyze numerous wardrives across locations and time

Reveal non-compliance

Depict areas of non-compliance and results of intervention

Simplify reporting

Create documents and slides; email reports directly from MeerCAT

Cut cost

Eliminate dedicated hardware

Easy to use

Get up and running in minutes

Questions MeerCAT helps answer:

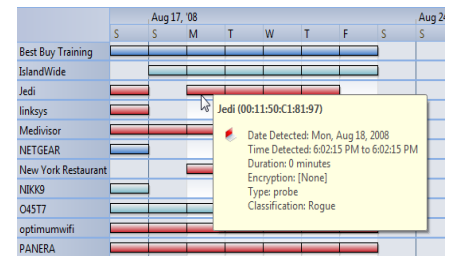
- ✓ Are there any unauthorized wireless access points detected within 1 km of the boundaries of the campus or base?
- ✓ Has that SSID been seen near the property within the past month?
- ✓ Has that same SSID been spotted at other, perhaps distant, government sites?
- ✓ Have unauthorized APs connected to the enterprise? To whom did they connect?
- ✓ Are they located within or outside the boundaries of the site?
- ✓ Are our wireless access points encrypted in accordance with our policy?

MeerCAT can be extended for management and tracking of mobile devices and people equipped with RFID tags, such as emergency equipment or sensitive cargo.

Users

- Info security professionals
- Penetration testers
- Vulnerability assessors
- Physical security teams
- Network administrators
- Compliance auditors

MeerCAT users can analyze the activity of suspicious wireless devices over time, and drill down for details. MeerCAT's **timeline view** shows wireless detections over days, weeks, or even months to verify when remediating actions were made, and assist in forensic investigations.



System Specifications

Data sources – MeerCAT-Pro visualizes wireless discovery and packet capture data including Kismet, NetStumbler, Flying Squirrel, AirPcap, and Wireshark. Other versions visualize WIDS/WIPS data, and combine wired and wireless data.

Geographic sources – MeerCAT-Pro displays imagery using NASA's World Wind or cached imagery. Versions for ESRI ArcGIS and Microsoft Virtual Earth are available.

Platforms – Windows XP, Vista, Windows 7. Future Linux version. No special hardware.

About Secure Decisions

Secure Decisions, a division of Applied Visions, Inc. (AVI), performs cyber security research and develops software products for government and commercial customers.

About MeerCAT-Pro

MeerCAT was developed under DARPA SBIR Phase II contract W31P4Q-07-C-0022. SBIR Data Rights (DFARS 252.227-7018 (June 1995)) apply.

MeerCAT® is a registered trademark of AVI. All rights reserved. All other trademarks are the property of their respective owners. Patent pending.

For Additional Information

Secure Decisions Division of AVI
6 Bayview Ave.
Northport, NY 11768
Phone: 631-754-4920

SecureDecisions.avi.com/MeerCAT
MeerCAT@SecureDecisions.avi.com