Secure Decisions MeerCAT is a visual analytics tool designed to help users locate wireless assets and networks, and assess risks to their organization

MeerCAT®-Pro

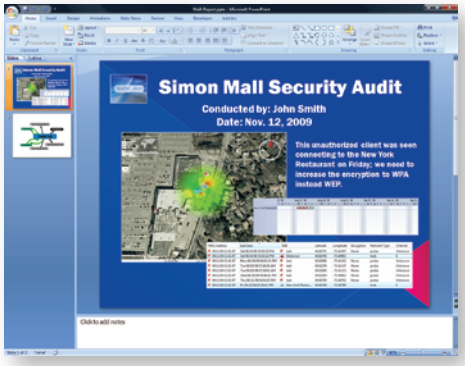
Visualizations that Help Make Sense of Wireless Security Data

The Need

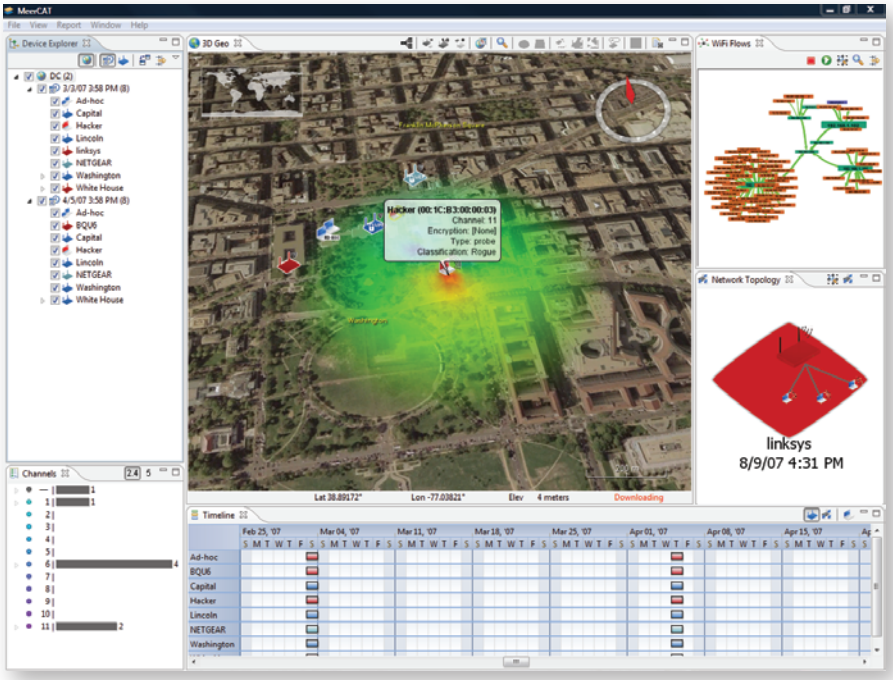
As a security professional tasked with protecting mission-critical fixed and mobile network assets, you need to locate and identify wireless security threats to these assets. Whether identifying risks to your authorized assets or discovering threats from unauthorized wireless devices, the task of collating, 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



Quickly generate professional looking, detailed reports



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

The 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 presents a unified picture of location, encryption levels, behavior patterns, time patterns, channel usage, and mission of authorized and un-authorized 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'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.

SECURE DECISIONS
A DIVISION OF APPLIED VISIONS, INC.

Secure Decisions performs cyber security research and develops software products for government and commercial customers

SECUREDECISIONS.COM
info@securedecisions.com
(631) 759-3988
6 Bayview Avenue
Northport, NY 11768

MeerCAT

Uses

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

Questions that MeerCAT helps answer:

- ✓ Are there any unauthorized wireless access points detected within 1 km of the boundaries of the facility?
- ✓ Has that SSID been seen near the property within the past month?
- ✓ Has that same SSID been spotted at other, perhaps distant, sites?
- ✓ Have unauthorized access points 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 policy?

Key Features

- ✓ Visual correlation and representation of wireless discovery data
- ✓ Big picture overview, filter, and 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

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.

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

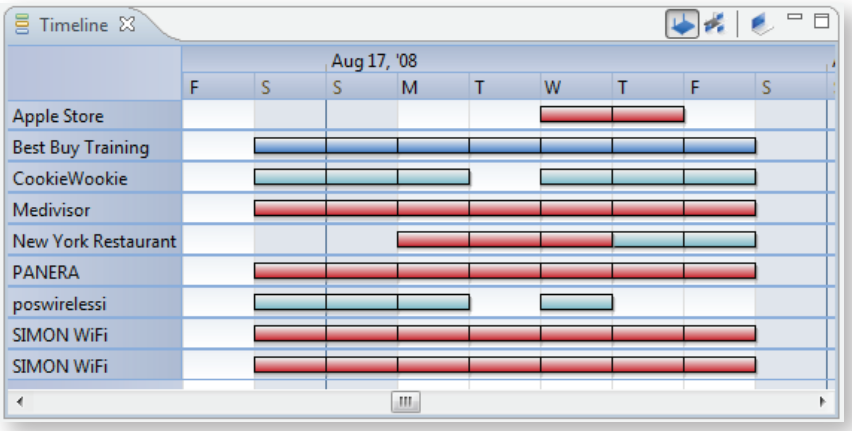
Reduce workload Rapidly analyze numerous wardrives across locations and time

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 Up and running in minutes



Analyze wireless activity over time

Visualize the location of wireless devices

About MeerCAT

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.

SECURE DECISIONS
A DIVISION OF APPLIED VISIONS, INC.

Secure Decisions performs cyber security research and develops software products for government and commercial customers

SECUREDECISIONS.COM
info@securedecisions.com
(631) 759-3988
6 Bayview Avenue
Northport, NY 11768