



## Internet Protocol Threat Analysis Program (IPTAP)



Quantar's Internet Protocol Threat Analysis Program acquires threat and risk data specific to your organization, utilizing our patented methodologies, to ensure accuracy and appropriateness of data for effective operational risk management.

### Business Process & Technology Risk Assessment

Operational risks derived from corporate network connectivity cannot be managed successfully using simplistic models and spreadsheets due to the specificity of these types of attack.

In establishing effective network operational risk management, your organization needs to understand both the interdependency between business operations and technology, and the continual threat evolution created by the internet.

With compliance and risk management a key aspect of managerial requirements, IPTAP provides oversight and increases transparency of value at risk methodologies to satisfy regulatory bodies.

IPTAP provides effective and accurate analysis and threat identification for network operational risks. It enables your risk and compliance teams to ensure your organization meets transparency criteria for risk quantification, both now and in the future.

### Rapid Deployment & Ease of Use

Deploying IPTAP within your organization is quick, simple, with a low training requirement, meaning low implementation and ongoing ownership costs. Once installed, IPTAP runs and updates automatically, with limited administration required.

IPTAP's output acts as one of the critical inputs for both n-ORM and PAE in delivering actual threat data for your organization.

With the ability to export to xml, IPTAP integrates with any third party vendor products, as well as having the capability of saving to a local file such as a spreadsheet.

Managing, assessing and valuing risks derived from technology and business process integration has increased in priority. IPTAP gives your organization the capability to capture risk data to ensure valuations and predictions are based upon actual organization-specific threats posed.

Business process optimization relies upon an in-depth understanding of each key operation within your organization and its' interaction with technology and systems. IPTAP assists in understanding the platforms upon which you rely for continuity, for the enhancement of organizational resilience.

## Benefits

Determines risk exposure of critical assets and business process vulnerability.

Acquires actual organization-specific threat data from your organization for risk modelling.

Rapid deployment and intuitive user-friendly interface ensuring low cost of implementation and ownership.

Automates the risk quantification process, providing a unified operational risk calculation for network and technology dependency.

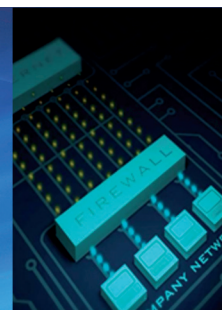
Risk Reporting & Compliance

Risk Management & Enterprise Resilience

Organization-specific Risk Data Acquisition

Managerial Oversight

Fig 1. IP TAP Assists in both GRC and OpRisk Segments



## IPTAP Recommended Specifications

IPTAP captures inbound traffic at up to 1Gb/s and detects and stores attack information.

Temporal profiles of stored attacks are created and exported in xml file format via fileserver or web for use by n-ORM; PAE or third party applications as inputs. It can also be used for fine-tuning perimeter defences & as historic OpRisk data for audit and compliance.

## Hardware Requirements

Server hardware must have dual CPU's; hard drives to RAID0; network interface card minimum 1Mb/s capacity. NOTE: server specifications are minimums.

### Monitoring Device:

2 x 3.4GHz Xeon (2MB Cache) Hyper-Threading  
 3GB 400MHz DDR2 PC3200 ECC RAM (as 2 DIMMS)  
 2 x 80GB Pluggable U320 SCSI 15000rpm HDD RAID 0  
 Hardware PCI-X RAID Controller  
 2 x Onboard Broadcom 1Gb/s Ethernet NIC  
 Intel Pro 1000 PCI-X133 NIC

### Database & File Server:

3GHz Xeon (2MB Cache)  
 3GB 400MHz RAM  
 3 x 140GB HDD

## Software Requirements

To ensure superior performance, ease of installation with high-speed network capacity and low cost of ownership, off-the shelf operating systems and ancillary software is utilized for stability, support for various hardware options, and configuration and administration.

### Monitoring Device:

FreeBSD 8.1 and above

### Database & File Server:

GNU/Linux Ubuntu 6.06 or above

### Ancillary Software:

SNORT 2.8.3 and above  
 MySQL 5.1.49 and above  
 Apache 2.0.63 and above (for web-based file swap)  
 SAMBA 3.5.0 and above (for fileserver swap)

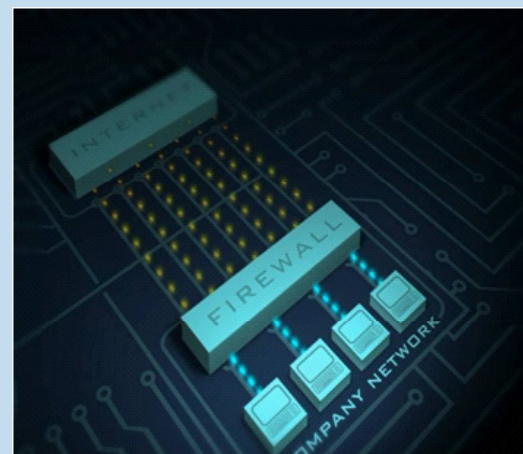


Fig 1. Data Flows In and Out of Organization

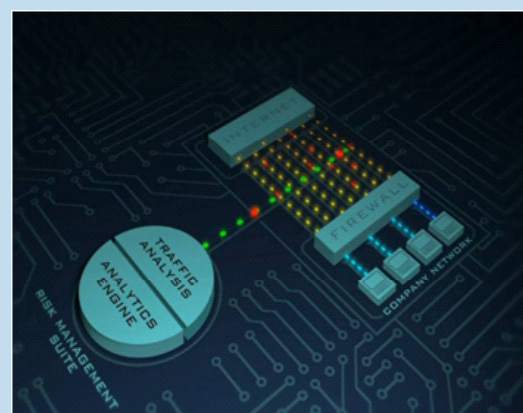


Fig 2. IPTAP Acquires Actual Organizational Data for Accuracy & Appropriateness

```
<Crimson Version="1">
<ObservedThreats ObservationStart="2010-07-19T00:00:00"
ObservationEnd="2010-07-26T00:00:00">
  <Threat ID="1408" Category="Indiscriminate" Target="Unknown"
SeverityScore="7">
    <Observation Day="Monday" From="00:00:00" To="00:59:59"
Count="50" />
    <Observation Day="Monday" From="01:00:00" To="01:59:59"
Count="95" />
    <Observation Day="Monday" From="02:00:00" To="02:59:59"
Count="60" />
    <Observation Day="Monday" From="03:00:00" To="03:59:59"
Count="35" />
  </Threat ID="1408" Category="Indiscriminate" Target="Unknown"
SeverityScore="7">
</ObservedThreats ObservationStart="2010-07-19T00:00:00"
ObservationEnd="2010-07-26T00:00:00">
</Crimson Version="1">
```

Fig 3. Actual Organization-Specific Threat Data