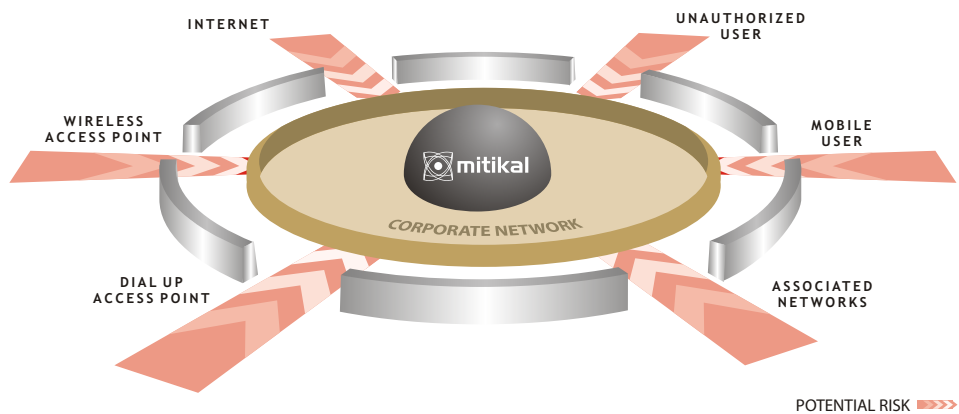


## Vulnerability Management

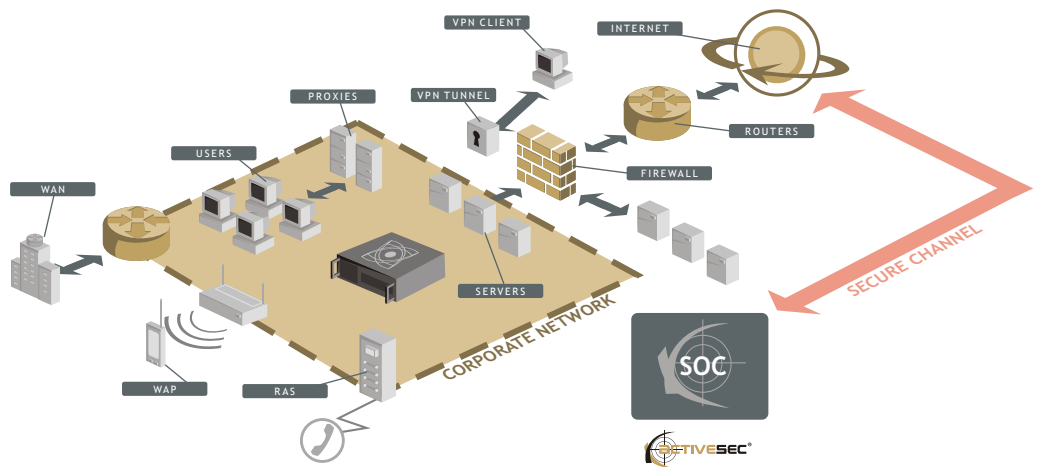
*In today's rapid changing environment where vulnerabilities are discovered every week, companies need to protect their critical IT assets from attacks and non-authorized intrusions.*

**mitikal**'s main goal is to help our customers to effectively control the complex process of Vulnerability Management. Many potential risk points are present in corporate networks where vulnerabilities allow intruders access to critical IT assets and information.



Activasec believes in a 360 degree security vision. There are no more internal LAN and external Internet connections. It is necessary to think of a whole network, where critical IT assets that support strategic business processes need to be protected.


**mitikal** works on a dedicated server appliance, installed in the internal LAN that allows both an assessment of internal assets and the request of external assessment to Activasec SOC (Security Operation Center).




An automated vulnerability assessment of internal networks and Internet-connected hosts is run, identifying high risk vulnerabilities.

Through detailed information of the evolution of hosts risk exposure, MITIKAL helps IT professionals in the design of a focused action plan.

Detailed reports with security information and solutions for target hosts hardening are issued. Vulnerabilities are ordered by severity to quickly identify risk exposures.

 **Name:** OpenSSH < 3.7.1

<b>ID</b> 11837	<b>Family</b> Gain root remotely	<b>Port:</b> unknown/tcp
--------------------	-------------------------------------	-----------------------------

 CAN-2003-0693, CAN-2003-0695

---

**Abstract** OpenSSH < 3.7.1

---


**Description**

You are running a version of OpenSSH which is older than 3.7.1

Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.


Network discovery capability provides an effective tool to detect active components in a network, offering IT staff control over the network's visibility.


MITIKAL offers "trend reports" to help both IT Managers and Network Administrators to measure and control corrective actions plans.


 **Trend Summary**

	High Risk	Warning	Notes	Ports	Test Database
<b>New</b>	5	5	16	0	<b>Total</b> 1620
<b>Persistent</b>	0	0	0	9	<b>Added</b> 14
<b>Closed</b>	0	0	0	0	<b>Updated</b> 217

---

 **New Vulnerabilities**

 **Security High Risk**

 **tcp/4876** **Abstract**  
 Portable SSH OpenSSH < 3.7.1p2  
 You are running OpenSSH 3.7p1 or 3.7.1p1.

For information on **mitikal**<sup>®</sup> contact ActiveSec by email  [sales@activesec.biz](mailto:sales@activesec.biz)

- **Comprehensive**  
A full updated database of vulnerability tests
- **Clear and concise fix information**  
Describing fixes and sources of related information
- **Automated scans**  
Customers can set frequency of scans to keep security level over time
- **Non disruptive**  
Denial of Service (DoS) exploits are reported, but not executed except for special requests
- **Service mapping**  
Shows services unintentionally exposed by maintenance or configuration errors
- **International Standards**  
Identification of Common Vulnerabilities and Exposure (CVE) is detailed on reports using international standard names
- **Trend Reports**  
Allows to effectively measure the progress of remediation tasks
- **Network Discovery**  
Vulnerability tests are run over IPs ranges to discover assets visibility from outside and inside