VIAVI Solutions

Product Brief

VIAVI
TeraVM
Cybersecurity Database

Agile and Progressive Security Validation.

Cybersecurity threats are evolving at a pace, that it has now become extremely difficult, to continuously assess and validate the effectiveness of security against the latest exploits. In many cases, it has become so complex and costly that many security defences simply go unvalidated. At the rate that new vulnerabilities are being exposed, there is a real worry that security defences are lagging behind.

TeraVM's Cybersecurity Threat Database provides the capability to analyze security with a comprehensive repository of traffic signatures, enabling assessment with the Good, the Bad and your Own. The TeraVM threat database includes known Common Vulnerability and Exposures (CVE), unknown (researched threats) and the ability to include your own traffic profiles, providing the maximum coverage possible for threat assessment.

With TeraVM, you can be assured that you will have the most up to date assessment capability, as and when the threat-scape changes. This not only helps to ensure that you have the right level of security but your investment in threat assessment is protected for the future.

Efficient and Reliable Assessment of Security Counter Measures

Security Hardening

By emulating the latest CVE security threat and exploit profiles, users of TeraVM can quickly assess security vulnerabilities in a safe and contained manner. TeraVM enables users to quickly pinpoint where the weaknesses are in their security counter measures ensuring the appliance or application is patched for any vulnerabilities.

Performance Under Duress

Determine with precision the effectiveness of security counter measures against scaled and targeted attacks. Assess what the impact is on normal network operations in a safe and contained manner. Use TeraVM to emulate common distributed denial of service attacks with known exploits and device vulnerabilities.

Exploit Recovery

Use TeraVM's security threat and exploit application library to assess how effective planned procedures are in recovering from a breached security defence. TeraVM delivers a safe contained environment in which to build knowledge and skills for pragmatic recovery plans.

Evolve with the Threat-scape

TeraVM's security threat and exploit application database is updated on a regular basis, ensuring you have the right defenses as and when needed. Assess with the latest vulnerabilities, protocol attacks and malware. TeraVM enables users to store up to a terabyte of additional traffic signatures. Future proof your investment in security assessment by choosing TeraVM.

TeraVM – Security Assessment with the Good, Bad and your Own

TeraVM is an IP traffic emulation and performance measurement solution used to validate the performance of networks and applications. Using TeraVM, emulate the most realistic attack scenarios by delivering mixed flows of legal and malicious content. TeraVM enables users to use a mix of known (CVE), unknown (researched threats) and your own traffic signatures, with the ability to store up to a terabyte of traffic signatures.

Assess a range of security counter measures such as appliances, applications and policies to ensure that the most robust security principles are applied. TeraVM's evolving threat database ensures that any future changes in the threat-scape or security counter measure e.g. a security appliance upgrade, does not diminish or expose the secure environment to vulnerabilities and exploits.

Common Vulnerability and Exposure (CVE) profiles

The TeraVM threat database includes known threats that target network user devices and applications, but more importantly also includes malicious traffic destined for server-side appliances and applications. Enabling users to assess for the lowest exploit risk.

The database includes many of the known vulnerabilities for vendors of security appliances and software applications. In addition, the repository includes vulnerabilities of the common open source server side applications. A sample of the CVE related threats and exploits contained in the TeraVM threat database include:

Network Users
• Network Services, Servers & Infrastructure
• Adobe: Acrobat and Reader, Flash Player, Photoshop
• Apple: Safari, QuickTime Player
• Cisco: IP Phone
• Facebook: ImageUploader
• Google: Chrome
• McAfee: VirusScan
• Mozilla: Firefox, Seamonkey, Thunderbird
• Microsoft: Windows, Internet Explorer, Powerpoint, Outlook, etc
• Sun Microsystems: Java Runtime Environment, JDK

Network Users
• Citrix: XenCenterWeb
• Cisco: ACS, Catalyst, IOS
• McAfee: SecurityCenter, E-Business Server
• Microsoft: IIS, Exchange Server, SQL server
• Oracle: Hyperion Financial Management
• Sun Microsystems: Web Server
• Symantec: Veritas NetBackup
• WordPress: Numerous themes and plugins
• Joomla: VirtueMart
• Zope: Application Web Server

For a complete overview of the latest threats and exploits visit: https://www.viavisolutions.com/en-us/node/60199

TeraVM Capability Overview	
General	Real-time isolation of problem flows
Data	TCP / UDP
	HTTP (headers, substitution, attachments)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
Address	MAC, VxLAN
	DHCP, PPPoE (IPv4 & IPv6)
	Dual Stack (6RD, DS Lite)
Ethernet Switch	VLAN and Double VLAN Tagging (Q-in-Q)
	ACL, 802.1p, DSCP
Replay	Replay large PCAP files - TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunelling (AMT)
	Video on Demand (RTSP)
	Adaptive Bit Rate Video (HLS, HDS, Smooth)
	Video conferencing
Secure VPN	SSL/TLS/DTLS, IPsec (IKE v1/v2)
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN Client
	Juniper Pulse, Juniper Network Connect
	802.1x EAP-MD5
Security attack mitigation	Spam / viruses / DDoS
Voice	VoIP: SIP & RTP (secure & unsecure), H.323
	Dual Hosted UACs, SIP Trunking
	Voice & video quality metric (MOS)
LTE/4G	GTP tunnel support
SLA	TWAMP
Automation	CLI, Perl, TCL, XML, Java API

VIAVI Solutions

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-cybersecurity-pb-wir-nse-ae
30187517 900 0918