DATA SHEET

CISCO SECURITY MONITORING, ANALYSIS, AND RESPONSE SYSTEM: DISTRIBUTED THREAT MITIGATION WITH INTRUSION PREVENTION SYSTEM

The Cisco® Security Monitoring, Analysis, and Response System (CS-MARS) Distributed Threat Mitigation with Intrusion Prevention System (IPS) is a collaborative solution that proactively identifies active network threats and distributes IPS signatures to mitigate them. Thus, it provides distributed and rapid threat mitigation utilizing a Cisco IOS® Software IPS and 42xx IPS Sensors.

PURPOSE

The main goal of this document is to describe a solution for faster mitigation of intrusion attempts or attacks, including worm or virus outbreaks, primarily in branch office networks in a dynamic and highly automated fashion.

SCOPE OF THE DISTRIBUTED THREAT MITIGATION WITH INTRUSION PREVENTION SYSTEM SOLUTION

When attacks are identified, either by signature or by anomaly-based systems, no scalable way to prevent further attacks or attempts to other network domains or elements exists. There is no economically feasible model based on a distributed architecture model to mitigate system or companywide alerts. Identifying or correlating discrete events in the network such as successful attacks (ones that damaged the target station) or innocent-looking reconnaissance (actually preparing the groundwork for an attack) so that other parts of the network are quickly prevented from similar incidents is desirable.

Usually, all the facts are not well connected for the user. Various pieces of information are derived from signature-based IPS sensors, and new families of security routers can send large amounts of data of any type: signature alerts, firewall syslogs, device health information, and so on. Before the MARS appliance, these inputs were not tightly coupled to correlate and validate the actual presence and damage of intrusion attacks scattered through the network. However MARS is capable of collecting and correlating this information, and now can automatically enable IPS signatures on IOS routers to help prevent attacks from spreading. This is an important factor in making inline intrusion protection effective and valuable on routers.

BUSINESS JUSTIFICATION

- Ability to use IOS router infrastructure to quarantine outbreaks
- Lowest-cost method of deploying an intelligent inline IPS solution
- Cisco IOS Software security coupled with MARS to provide a high-fidelity IPS solution
- Allows IOS router IPS to be kept dormant until needed to mitigate an attack, freeing up router resources until needed
- Additional return on investment (ROI) for existing IPS/intrusion detection system (IDS) deployments

ARCHITECTURE OVERVIEW

Distributed Threat Mitigation is a collaborative solution that proactively identifies and distributes IPS signatures for the most active threats detected on the network. Thus, it provides distributed and rapid threat mitigation utilizing a Cisco IOS Software IPS.

The primary values offered by this solution are:

- Collaborative utilization of MARS by extending event correlation and anomalous traffic detection to mitigation with a Cisco IOS Software IPS
- Uses a Cisco IOS Software IPS for a widely distributed threat defense system

- Identifies the most triggered signatures from a strategically placed Cisco IPS router or sensor
- Facilitates networkwide signature activation to mitigate the most active threats
- Completes the lifecycle of accurate detection, quarantine by dropping malicious traffic inline, and finally identifying and removing the offending device from the network

In today's complex networks, when threats are identified, they must be mitigated quickly. MARS Distributed Threat Mitigation with IPS provides a distributed architecture model to mitigate networkwide alerts. MARS collaborates by extending correlation capabilities and analyzing the alarm information received from Cisco IPS sensors. Cisco IOS Software IPS routers would have their base (default) signature files loaded depending on their capacity. Amendments to the signature database, based on the most active threats, are carried out by MARS, and those active threats are mitigated on the networkwide scale.

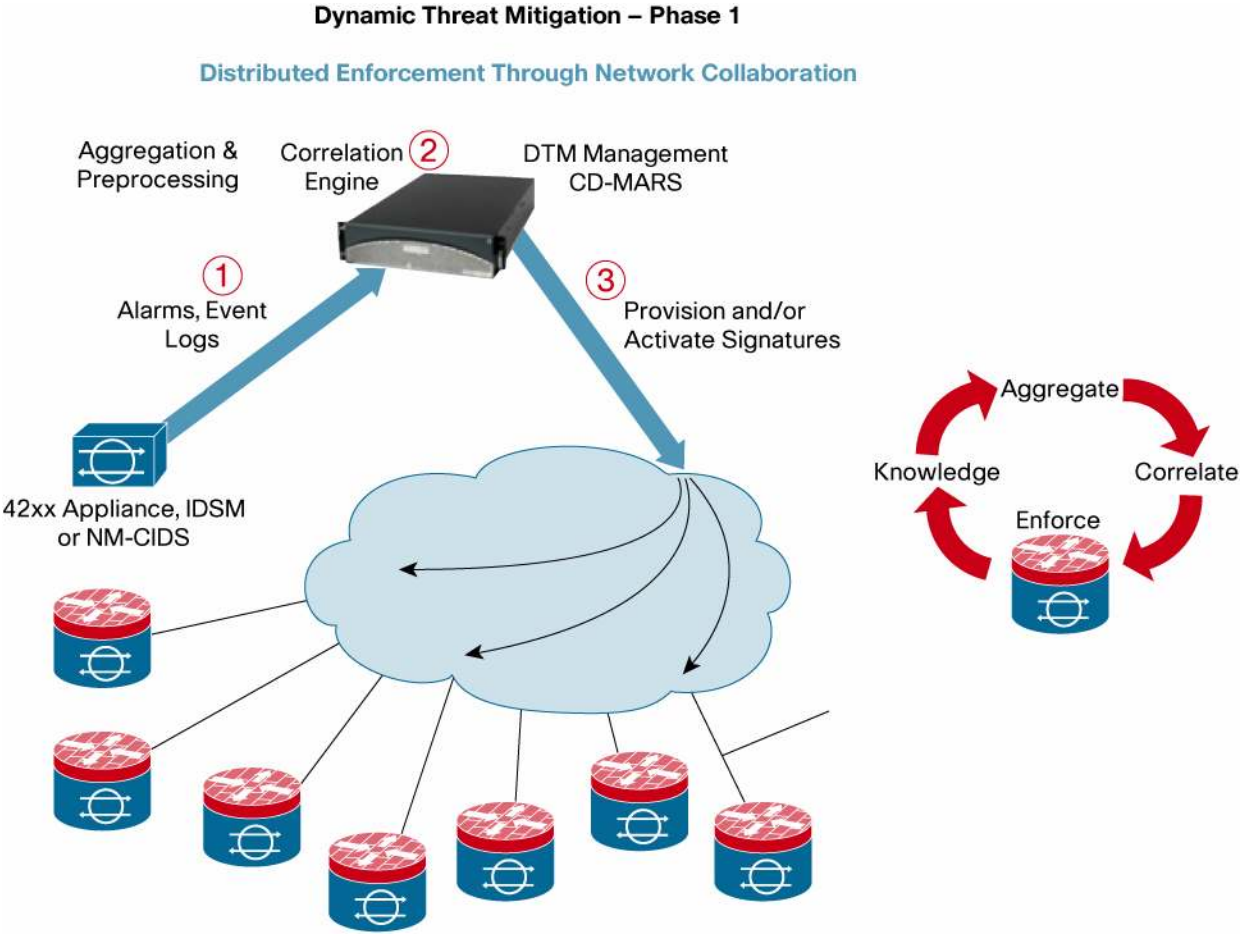
The main advantage of MARS Distributed Threat Mitigation with IPS is facilitating signature tuning in dynamic fashion. It also helps reduce the number of false alarms.

DISTRIBUTED THREAT MITIGATION STEP BY STEP

This section describes the sequence and the flow of Distributed Threat Mitigation.

Figure 1 shows the overall solution workflow, followed by a step-by-step description of Distributed Threat Mitigation deployment in a network.

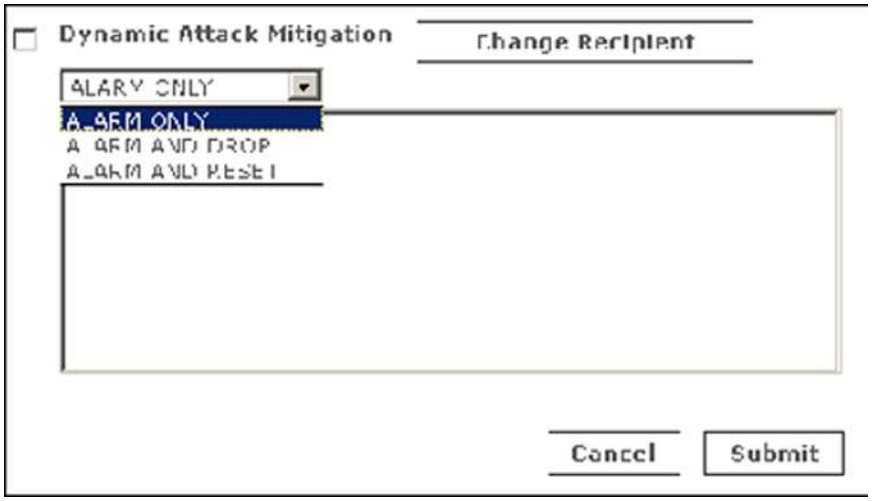
Figure 1. Distributed Threat Mitigation Workflow



1. The Distributed Threat Mitigation feature of MARS works in conjunction with a Cisco IPS device to generate and publish current signature definition files (SDFs) to the IPS function on IOS routers. The SDF is an Extensible Markup Language (XML) file that a Cisco IOS Software IPS device reads, and based on the parsed data it then populates its internal tables with the signatures against which it has to inspect each packet.

To use Distributed Threat Mitigation, you must define MARS IPS signatures-based inspection rules and use the newly added action Distributed Threat Mitigation notification. (See Figure 2.)

Figure 2. Distributed Threat Mitigation Alert on MARS

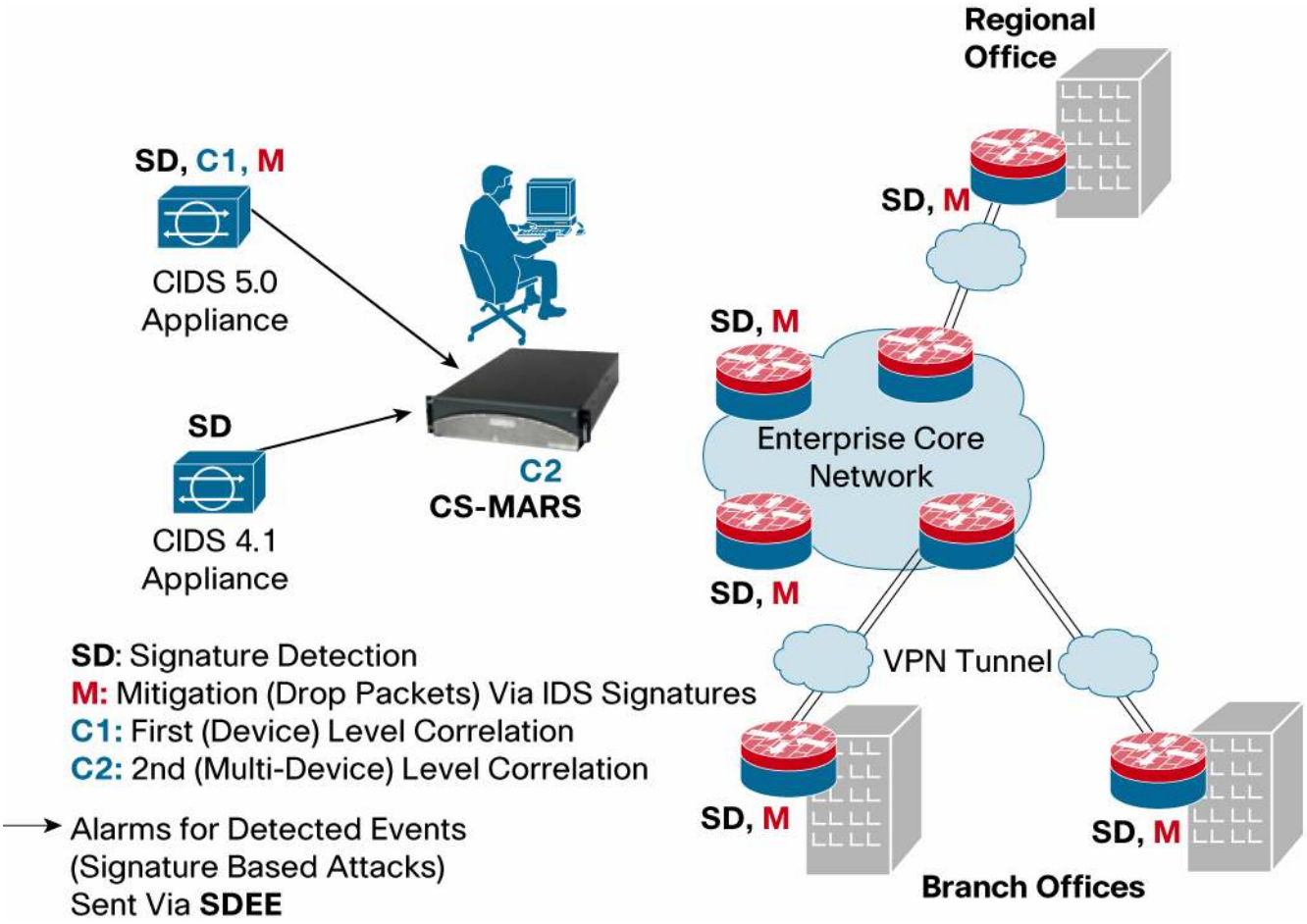


For such rules, the SDF for those signatures is generated and stored on the MARS appliance when the rules are fired. Selecting the Distributed Threat Mitigation notification method means that if that rule fires, then MARS pushes the associated SDF to any Cisco IOS Software IPS devices that are in the recipient list for that notification (here you can specify a list of static devices, or a group of devices for each notification, and have different set of devices for different rules). The Distributed Threat Mitigation notification method also includes an IPS alert action: alarm, alarm and drop, or alarm and reset (if it is a TCP session). This IPS alert action enables new or existing signatures and configures the signature to respond accordingly when it fires. The alarm action refers to sending a syslog or Security Device Event Exchange (SDEE) notification to target monitoring devices, such as MARS and syslog servers.

Together with the rule action, the user can also specify how often the MARS box has to schedule Distributed Threat Mitigation updates.

2. The Cisco IOS Software IPS router or IPS appliance detects one or more signatures and sends an alarm to MARS for event correlation and monitoring. (See Figure 3.)

Figure 3. Distributed Threat Mitigation Operation: Step 2



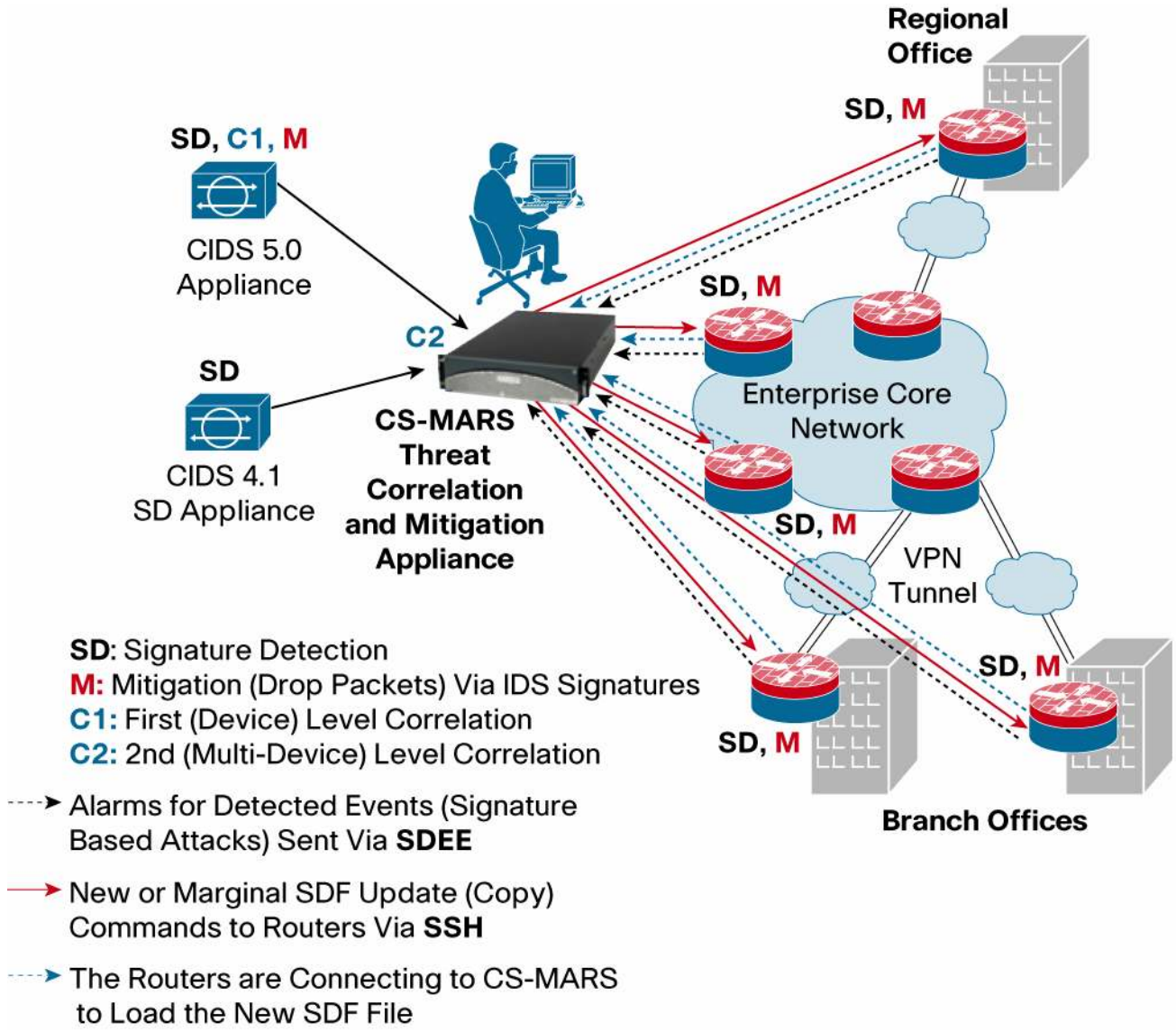
3. Following the intelligent analysis and correlation of signature detection events, and based on default and/or user-defined rules on MARS, signatures to be added to routers are identified, depending on when the last signature file update was sent.

MARS keeps track of the signature running on the routers and from there compiles the new .sdf file. To this file it adds the new signatures, depending on how the appliance has been configured and on what is firing. It checks the amount of memory that each signature needs and the free memory on the router.

4. MARS sends the update to all or a group of branch routers (as configured). It is important to note that signatures can be added in “alarm only” mode at this stage.

Note: The action that you want to implement on the devices is defined by the user depending on the set of routers enforcing the signatures and on the topology of the network. In this example the first time MARS will push the signatures in "alarm only" mode, and the same signatures files again in "alarm/drop" mode. It is also possible to immediately deploy the signatures in drop mode or to take different action depending on the set of routers to which the user is deploying. (See Figure 4.)

Figure 4. Distributed Threat Mitigation Operation: Step 4



5. Following the update, the branch office routers will also detect the same signature(s), start sending alarms to MARS, and verify the occurrence of active threats. Those new alarms in turn trigger a new rule in MARS to have those signatures drop the suspicious packets, thus stopping the attack at the branch gateway. A new .sdf file will be pushed to the routers with the new action for those rules following the schema.

6. You can define queries and reports around any of the Distributed Threat Mitigation events, which are organized under the Misc/DTM event group. These events provide status around the Distributed Threat Mitigation updates that are published to the target devices. Alternatively, you can enter “dynamic attack” in the Description/CVE: field and click Search on the Management > Event Management page of the HTML interface.

The following Distributed Threat Mitigation reports are provided by MARS:

- Activity: Cisco IOS Software IPS Distributed Threat Mitigation Successful Signature Tuning—All Events
- Connectivity issues: Cisco IOS Software IPS Distributed Threat Mitigation—All Events
- Resource issues: Cisco IOS Software IPS Distributed Threat Mitigation—Top Devices

PRIMARY BENEFITS WITH DISTRIBUTED THREAT MITIGATION WITH INTRUSION PREVENTION SYSTEM SOLUTION

The primary benefits provided by Distributed Threat Mitigation with Cisco IOS Software IPS solution are:

- Attempts to utilize the router’s resources for intrusion detection and/or protection only when (and as much as) needed
- Provides (optionally) automated tuning of IPS signatures: customers will not have to worry about which IPS signature set has to be loaded and active on their branch routers; additional signatures will be loaded and/or activated as attacks are detected at other parts of the network
- Customers that turn on and use the IPS feature on their branch routers will not have to deal with too many (sometimes false) alarms, because a smaller set of signatures will be active, generating fewer alarms with a much lower ratio of false positives
- Uses networking and security features that are unique to Cisco Systems® routers and thus provides significant competitive advantage
- Has a major leadership security feature/solution that no competitor can offer today
- Increases the value of a company’s investment in network-based intrusion detection products
- Helps the user (operator) to narrow down or locate the source of the attack more quickly while dropping malicious traffic inline to protect other network segments
- Also helps the user to quickly identify the branch or regional offices that are already affected by the attack as well as those that have not seen the attack yet
- The only inline IPS system that evaluates network device and security device events and correlates that data with anomalous traffic flow analysis to determine the fidelity of an IPS device signature alert prior to applying that signature potentially enterprisewide to quarantine an outbreak

SPECIFICATIONS

Cisco Secure MARS Distributed Threat Mitigation with IPS supports the following Cisco mitigation products:

- Cisco IPS 4200 Series sensors with software v5.0 or greater
- Cisco ASA 5500 Series Adaptive Security Appliances with an AIP-SSM card with software v5.0 or greater
- Cisco Catalyst® 6500 Series Intrusion Detection System (IDSM-2) Services Module with software v5.0 or greater
- Cisco NM-CIDS Network Module (with software v5.0 or greater) for Cisco 2600XM series routers, Cisco 2800 and 3800 series integrated services routers, and Cisco 3700 Series multiservice access routers
- Cisco IOS Software routers with security features set and Release12.3(14)T or greater

MARS platform support includes the following:

- CS-MARS-20-K9
- CS-MARS-50-K9
- CS-MARS-100E-K9
- CS-MARS-100-K9
- CS-MARS-200-K9

SYSTEM REQUIREMENTS

Management Console requires the following Web browser: Internet Explorer 6.0 SP2 or greater.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205404.M_ETMG_KL_9.05

Printed in the USA