TippingPoint
a division of 3Com

Custom Digital Vaccine® Service

DATASHEET

The TippingPoint Digital Vaccine team regularly develops filters to address vulnerabilities, viruses, Misuse and Abuse, and other applications and incorporates them into Digital Vaccines. Digital Vaccines are typically delivered to customers on a regular weekly release schedule, and can be deployed automatically with no user interaction required. The Custom Digital Vaccine (DV) Service is an extension of TippingPoint's standard Digital Vaccine service.

Selections

- The Custom Service is purchased on a credit system using credits as “currency”
- The Custom DV Service is purchased in units of 10 credits
- Credits are applied toward a request as follows:
  - Vulnerability: one (1) credit
  - Virus/Malware/Backdoor: one (1) credit
  - Application/P2P/Misc: two (2) credits

The Custom DV Service is available as a professional services arrangement to provide enhanced or extended filtering capability on an as-needed basis. Custom filter requests can serve multiple functions:

- Provide filter coverage for an issue not normally included in TippingPoint's Vulnerability, Malware, or Misuse and Abuse queue
- Provide filter coverage for an issue with more expediency than the scheduled DV release

Filters fall into one of three categories: Vulnerability, Virus or Application. The Digital Vaccine team will evaluate each filter request. If the Digital Vaccine team determines that the filter can be written, it will be delivered to the customer as promptly as possible after sufficient testing.

In order to help the customer make informed decisions on which Custom DV issues to request, the Digital Vaccine Team's filter queue and estimated delivery dates are available on the Threat Management Center. The customer may request that a particular filter be delivered before the estimated date or that an issue be added to the DV queue specifically for that customer.

Filters created by customer requests are exclusively owned by TippingPoint.

Service Definitions

Vulnerability – TippingPoint can write filters to prevent remote exploitation of vulnerabilities over the network. A vulnerability is typically acknowledged by the vendor or disclosed on a mailing list by a third party (e.g., Microsoft vulnerabilities, Oracle, etc.).

Virus – (including Malware and Backdoors) - TippingPoint can write filters to block e-mail viruses, worms, backdoor Trojans and Spyware.

Application – (including Misuse and Abuse/IM/Miscellaneous) - TippingPoint can write filters to block or rate limit P2P file transfers and IM communications. Additionally, TippingPoint can undertake special requests that do not fall into the Vulnerability or Virus categories (e.g. block IRC traffic, block Yahoo! Message Board, block Winamp Streaming Media, obscure P2P application, etc.).

Delivery

1.The customer makes a Custom DV filter request to the Technical Assistance Center (TAC).

2. A Digital Vaccine team member is assigned to the customer and may contact the customer to better understand the request and gather information.

3. The TAC notifies the customer within 12 hours if it is determined that the filter can be written. If so, an open ticket is established with an estimated timeline.

4. The DV team works with customer directly to deliver the Custom DV and answers any questions about its function or behavior.

5. The delivery timeline generally depends on request type, necessary research or exploitation replication, request complication and testing requirements.

6. Response time goal for Custom deliverable DV:

   - Virus: 12 hours - 36 hours
   - Vulnerability: 24 hours - three (3) days
   - P2P/Misc: two (2) days - one (1) week

3com