



network defense through collaboration

OFFER & PRICE LIST | JUNE 2003

IDS Deliverables

Attend IDS Sensor Configuration

OVERVIEW: APERIOS custom configures an Aperios Assess IDS Sensor appliance for Client's network. APERIOS ships the pre-configured Sensor to Client with installation instructions and APERIOS is available during normal business hours to provide installation support as needed. Upon installation of the Sensor on Client's network, APERIOS remotely tests and verifies proper communication between Sensor and backend systems in the 24/7 Monitoring Center. When testing is completed, 24/7 Monitoring can begin.

AVAILABILITY: XXXXX: Included
XXXXX: Included

Box Sensor Option

OVERVIEW: The Box Sensor is the default option for all Clients unless a rack-mountable appliance is required.

AVAILABILITY: X XXXX: Included
XXXXX: Included

Rack-Mountable Sensor Option

OVERVIEW: This option is available for Clients requiring a rack-mountable Sensor.

AVAILABILITY: XXXXX: Upgrade Fee
XXXXX: Included

Rack-Mountable Gigabit Sensor Option

OVERVIEW: This option is available for Clients requiring a rack-mountable Gigabit Sensor.

AVAILABILITY: XXXXX: Upgrade Fee
XXXXX: Upgrade Fee

24/7 Management of Attend Sensors

OVERVIEW: APERIOS provides complete management and administration of the Aperios Assess Sensors from our 24/7 Monitoring Center. Sensor management activities include:

- Monitoring health status of all deployed Sensors.
- Administering software upgrades and operating system updates.
- Updating signatures in the intrusion detection engine. (All signatures are reviewed and tested by our engineers prior to being released and deployed in a commercially reasonable timeframe.)

AVAILABILITY: XXXXX: Included
XXXXX: Included

24/7 Monitoring for Attack Alerts

OVERVIEW: APERIOS will provide 24/7/365 monitoring of Client's network specifically for the purpose of identifying and responding to network attack alerts generated by the Attend Sensor.

APERIOS's security analysts based on our 24/7 Monitoring Center immediately investigate each attack using our proprietary analysis and investigation tools. Investigation includes:

- Detailed examination of TCP packet data.
 - Contextual analysis of offending packets.
 - Historical queries of similar past activity.
 - Queries on source IP address.
- Examination of the targeted system on the Monitored Network.



network defense through collaboration

OFFER & PRICE LIST | JUNE 2003

IDS Deliverables cont...

AVAILABILITY: XXXXX: Included
XXXXXXXX: Included

Discovery Alert Monitoring

OVERVIEW: Monitoring for pre-attack probes and other exploratory traffic from external sources. This activity indicates attackers are gathering information about the target system(s).
AVAILABILITY: XXXXX: Not Available
XXXXXXXX: Included

Penetration Alert Monitoring

OVERVIEW: Monitoring for active attempts to take advantage of vulnerabilities and penetrate the target system(s).
AVAILABILITY: X XXXX: Included
XXXXXXXX: Included

Exploit Alert Monitoring

OVERVIEW: Monitoring for indications attacker has control over the target system(s).
AVAILABILITY: X XXXX: Included
XXXXXXXX: Included

24/7 Incident Notification & Support

OVERVIEW: In the event of threatening attacks against the client, APERIOS's 24/7 Monitoring Center notifies Client in accordance to customized incident response plan and delivers incident reports that outline the results of the investigation:
- The specific attack activity and progress of the attacker
- The source of the attack activity
- The particular systems targeted on Client's network
APERIOS's analysts are available 24/7/365 to assist Client in their response to intrusion incidents.
AVAILABILITY: XXXXX: Included
XXXXXXXX: Included

Weekly Summary Reporting

OVERVIEW: Electronic reports will be delivered to Client every week that includes a summary of the intrusion monitoring activities. The report will include:
- Alert trends and statistics.
- Summary of alerts investigated.
AVAILABILITY: XXXXX: Included
XXXXXXXX: Included

Intrusion Blocking

OVERVIEW: Intrusion attempts can be blocked at the packet level before they reach their intended target and cause serious damage.
AVAILABILITY: XXXXX: Included
XXXXXXXX: Included



network defense through collaboration

OFFER & PRICE LIST | JUNE 2003

IDS Deliverables cont...

Worm Blocking

OVERVIEW: Known Worm Attacks can be automatically blocked before they enter the client's network. This helps eliminate the bandwidth consumption caused by Worms.

AVAILABILITY: XXXXX: Not Available
XXXXX: Included

Source Nastygram

OVERVIEW: APERIOS's analysts will prepare and send an incident report to the source ISP for every attack detected against Client's network. These reports, called Nastygrams, notify the source ISP of the attack activity originating from their network and encourage them to investigate the matter on their end. This helps ISPs track down and put an end to malicious activity from the offending users.

AVAILABILITY: XXXXX: Not Available
XXXXX: Included

CERT Incident Reporting

OVERVIEW: APERIOS's analysts will report each incident to the CERT Coordination Center in accordance with CERT's published Incident Reporting Guidelines. The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. <http://www.cert.org>

There are several reasons to report an incident to the CERT Coordination Center. CERT may be able to provide technical assistance in responding to the incident, or put the Client in touch with other sites involved in the same activity.

AVAILABILITY: XXXXX: Not Available
XXXXX: Included

Rule Customization

OVERVIEW: APERIOS can customize the rule settings for Clients that want to monitor and detect specific types of misuse (external or internal).

AVAILABILITY: XXXXX: Not Available
XXXXX: Included

Custom Reporting

OVERVIEW: APERIOS analysts can custom create reports that meet Client's specific needs. This service option is best for organizations that have reporting needs above and beyond APERIOS's standard weekly reporting. Reports can be configured to contain the specific information required by Client and can be delivered on a weekly or monthly basis.

AVAILABILITY: XXXXX: Not Available
XXXXX: Included*

*Limited to one customized report per Client. Certain restrictions may apply.