SECURSHIELD | INTRUSION DETECTION AND PREVENTION

DataComm

Intrusion Detection & Prevention Monitoring (IDS/IPS)

DataComm's intrusion detection & prevention service, SecurShield, pairs a best-of-breed appliance with best-in-class service. Our proprietary SecurShield Sensing Unit has the ability to monitor activity on multiple network segments with real-time intelligent blocking of suspicious activity. DataComm's Secure Network Operations Center is staffed 24x7x365 with certified security technicians that interpret the suspicious activity and respond to threats in a customer-specified manner.

Service Features

- **Comprehensive monthly logs**: DataComm documents suspicious activity and resolution as reported by the IDS/IPS. The report includes an executive overview, raw data collected by your sensor throughout a month, and incident response logs which show how DataComm's technicians responded to all high-level alarms.
- **Updates (software, signature and rules)**: DataComm performs rigorous tests on the updates in a test environment before implementing them on your sensor. Updates are performed by the DataComm staff to make sure that all updates are current. Updates include the latest software releases, exploit signatures, and both anomaly and correlative rules.
- **Email Summary Reporting**: DataComm sends an overview of events (based on a customer specified period of time) via email as part of service, giving access to activity on the network daily. (Must have an in-house email server)
- **Real-Time Reporting and Management**: This graphical user interface provides customers with the ability to monitor their own network in real-time and create custom reports that can be used for board meetings, auditors or managers.

ALERT
ANALYZE
RESPOND
NOTIFY

SecurSHIELD Monthly Report | DATACOMM NETWORKS

CUSTOMER EVENT ANALYSIS

14

EVENTS BY TYPE

0.02% Virus 1	0.76% Spyware / Malware 41	Web Related
0.00% Log Monitoring 0	0.00% Denial of Service 0	Exploit
0.00% Remote Administration 0	91.20% Reconnaissance 4,912	Other

EVENTS BY SEVERITY

>0 % HIGH

% MEDIUM

7 % LOW

FOUR KEY PROCESSES

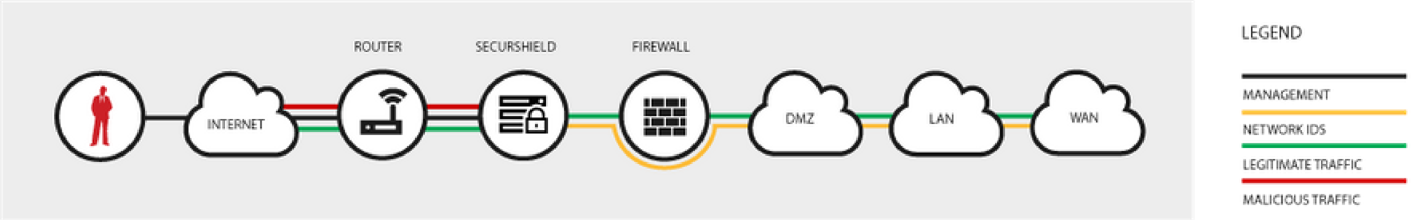
- **ALERT** – The SecurShield sensing unit examines all traffic flowing through its network interfaces. Event by event, the SecurShield is capable of immediately blocking the source of the activity then alerting the DataComm Network.
- **ANALYZE** – in addition to the sensor's analyzing capabilities alone, our Security Engineers then conduct further manual (human) analysis of all alerts.
- **RESPOND** – After our Network Security Engineers analyze alerted events, they immediately assess the potential threat, determine severity, and perform any necessary threat mitigation actions such as blocking activity, creating filters, contacting the client, and reporting the activity.
- **NOTIFY** – DataComm immediately notifies your organization of the threat and actions taken.

> *Quantifying financial losses from cyber-attacks is one of our major problems...But the real costs are the soft costs---lost business opportunities...for every hour you are down..*
>
> Richard Power | Editorial Director CSI (Computer Security Institute)

SECURSHIELD | INTRUSION DETECTION AND PREVENTION

DataComm

SecurShield | Intrusion Detection IDS/IPS



DataComm's SecurShield sensing unit is the best network security appliance on the market - a proactive, inline, scalable, network based IDPS that uses a powerful combination of signature, protocol, advanced information gathering, and correlative events-based inspection methods to achieve the maximum attack detection and prevention capability.

- Real-time Intrusion Detection/ Intrusion Prevention & Response
- Resistance to evasion techniques
- Secure website monitoring
- Signature & anomaly sensing
- Scalable internal sensing presence
- False Positive Reduction

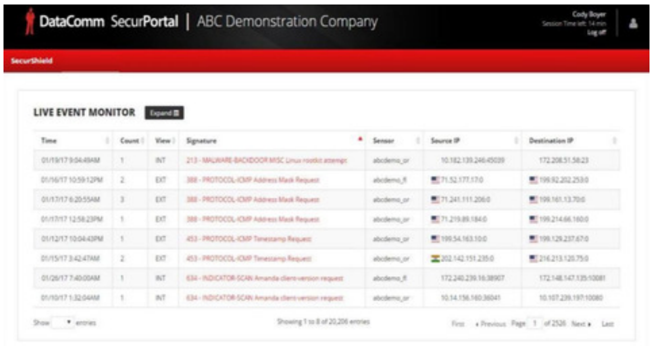
Monthly Sample Reports:

- Executive overview
- Events by type
- Events by severity
- Events classified by response
- Volume of events by day
- Top Concern Hosts
- Event analysis
- Detailed response log

SecurPortal:

The SecurPortal dashboard gives you a quick look at your live event monitor, security event interactive charts and tickets.

- Executive overview
- Expand the dashboard views
- View & download reports
- Manage trusted & blocked IPs
- Administer sub-user accounts


DataComm SecurPortal | ABC Demonstration Company
Cody Boyer
Session Time left: 14 min
Log off
SecurShield
Expand

LIVE EVENT MONITOR

Time	Count	View	Signature	Sensor	Source IP	Destination IP
01/19/17 9:04:49AM	1	INT	213 - MALWARE-BACKDOOR MISC Linux rootkit attempt	abcdemo_or	10.182.139.246:45039	172.208.51.58:23
01/16/17 10:59:12PM	2	EXT	388 - PROTOCOL-ICMP Address Mask Request	abcdemo_fl	71.52.177.17:0	199.92.202.253:0
01/17/17 6:20:55AM	3	EXT	388 - PROTOCOL-ICMP Address Mask Request	abcdemo_or	71.241.111.206:0	199.161.13.70:0
01/17/17 12:58:23PM	1	EXT	388 - PROTOCOL-ICMP Address Mask Request	abcdemo_or	71.219.89.184:0	199.214.66.160:0
01/12/17 10:04:43PM	1	EXT	453 - PROTOCOL-ICMP Timestamp Request	abcdemo_or	199.54.163.10:0	199.129.237.67:0
01/15/17 3:42:47AM	2	EXT	453 - PROTOCOL-ICMP Timestamp Request	abcdemo_or	202.142.151.235:0	216.213.120.75:0
01/26/17 7:40:00AM	1	INT	634 - INDICATOR-SCAN Amanda client-version request	abcdemo_fl	172.240.239.16:38907	172.148.147.135:10081
01/10/17 1:32:04AM	1	INT	634 - INDICATOR-SCAN Amanda client-version request	abcdemo_or	10.14.156.160:36041	10.107.239.197:10080

Show ▾ entries

Showing 1 to 8 of 20,206 entries

First ‹ Previous Page 1 of 2526 Next › Last