



How OKENA Is Positioned Favorably vs. IDS

Intrusion Detection Systems, such as Symantec ESM, ISS RealSecure, and Cisco Secure IDS monitor network activity for attacks, analyzing logged data and reporting suspicious activity. Network IDS systems promiscuously inspect network fragments for an entire subnet; Host IDS systems reside on servers and desktops. Both flavors of IDS provide

appropriate forensic evidence of those activities that violate established network security policies. These technologies are entirely reliant on a database of known signatures.

IDS strengths:






- ?? A single network based IDS may catch network attacks for an entire subnet within the enterprise.
- ?? IDS systems can detect failed access attempts, alerting IT to a potential future intrusion.
- ?? IDS systems correlate evidence of attacks across a range of log files to assess system vulnerabilities.

IDS limitations:

- ?? Totally reactive – attacks are only detected after they occur. HIDS can only claim to be ‘near real-time’ and only when a signature is recognized
- ?? A high volume of network traffic can overload a network based IDS. Encryption also prevents effective Network Intrusion Detection, as do switched environments
- ?? Intrusion Detection Systems are network based – they do not look for attacks contained within files.
- ?? High administrative overhead required for monitoring activity and analyzing log data.

OKENA StormWatch strengths:

- ?? Okena is proactive and able to prevent new and evolving attacks. Not reliant on a set of signatures
- ?? Recognizes sequences of file and network activity to proactively block inappropriate behavior before damage can be inflicted.
- ?? OKENA understanding of application behavior provides for a finer granularity of Intrusion Prevention security.
- ?? Doesn't have to scan high volume of network traffic – monitors activity for abhorrent behavior, based on established rules

Lifecycle of an Attack		Okena	IDS
Probe			
	Ping Addresses	Yes	Yes
	Scan Ports	Yes	Yes
	Guess Passwords	X	X
	Guess Mail Users	X	X
Penetrate			
	Mail Attachments	Yes	X
	Buffer Overflows	Yes	Yes
	ActiveX Controls	Yes	X
	Network Installs	Yes	Yes
	Compressed Messages	Yes	X
	Backdoors	Yes	X
Persist			
	Create New Files	Yes	Yes
	Modify Existing Files	Yes	Yes
	Weaken Registry Security Settings	Yes	X
	Install New Services	Yes	Yes
	Register Trap Doors	Yes	X
Propagate			
	Mail Copy of Attack	Yes	X
	Web Connection	Yes	X
	IRC	Yes	X
	FTP	Yes	X
	Infect File Shares	Yes	X
Paralyze			
	Delete Files	Yes	Yes
	Modify Files	Yes	Yes
	Drill Security Hole	Yes	X
	Crash Computer	Yes	X
	Denial of Service	Yes	X
	Steal Secrets	Yes	X

Preventative Security Provided During an Attack

Bottom Line message:

Intrusion Detection Systems, with vulnerability assessment, are good for audit and forensic analysis of an attack – but they do not prevent damage!

Only behavior enforcement technology from OKENA **prevents** damage from attacks.