## **Cisco IPS Architecture**

## Intelligent Detection and Precision Response

Network Cisco Threat Context Signature Engine Context Intelligence Services **Updates** Updates Data Information **Normalizer** Modular Risk-Based On-Box Module Correlation Inspection **Policy Control Engines Engine**  Vulnerability Laver 3–7 Meta event Calibrated "risk rating" normalization of generator for computed for each event Exploit traffic to remove event correlation Event action policy Behavioral anomaly attempts to hide based on risk levels · Protocol anomaly an attack · Filters for known · Universal engines benign triggers Virtual Sensor Mitigation **Forensics** Selection and Alarm Capture · Traffic directed to · "Threat rating" of event · Before attack appropriate virtual indicates level of sensor by interface residual risk · During attack or VLAN After attack Out ln

# 1 day of "crud" seen at ICSI (155K times)

active-connection- reuse	DNS-label-len-gt-pkt	HTTP-chunked- multipart	possible-split-routing
bad-Ident-reply	DNS-label-too-long	HTTP-version- mismatch	SYN-after-close
bad-RPC	DNS-RR-length- mismatch	illegal-%-at-end-of- URI	SYN-after-reset
bad-SYN-ack	DNS-RR-unknown- type	inappropriate-FIN	SYN-inside- connection
bad-TCP-header-len	DNS-truncated- answer	IRC-invalid-line	SYN-seq-jump
base64-illegal- encoding	DNS-len-lt-hdr-len	line-terminated-with- single-CR	truncated-NTP
connection- originator-SYN-ack	DNS-truncated-RR-rdlength	malformed-SSH- identification	unescaped-%-in-URI
data-after-reset	double-%-in-URI	no-login-prompt	unescaped-special- URI-char
data-before- established	excess-RPC	NUL-in-line	unmatched-HTTP- reply
too-many-DNS- queries	FIN-advanced-last- seq	POP3-server- sending-client- commands	window-recision
DNS-label-forward- compress-offset	fragment-with-DF		

### The New York Times

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers, please click here or use the "Reprints" tool that appears next to any article. Visit www.nytreprints.com for samples and additional information. Order a reprint of this article now. »

December 16, 2010

## Ohio State Says Hackers Breached Data on 760,000

By TAMAR LEWIN

Ohio State University is notifying about 760,000 people whose personal information was stored in the university's computer server that a data breach could put them at risk for identity theft.

The university, located in Columbus, began sending letters on Wednesday to current and former faculty and staff members, students and applicants, telling them that hackers had broken into the server that stored their names, <u>Social Security</u> numbers, dates of birth and addresses.

The university said that although there was no evidence that the information had been used for identity theft, it was nonetheless offering a year of free credit protection to everyone whose data was on the server.

"We regret that this has occurred and are exercising an abundance of caution in choosing to notify those affected," Joseph A. Alutto, the university provost, said in a news release.