## Snort Database Schema v1.06 Standard Snort Table Diagram created Sept 10, 2004 chris.reid@codecraftconsultants.com SnortDB Extra Table Bold fields are "not null" sig\_reference reference reference\_system schema PK,FK2 PK sig id ref id ref\_id PΚ ref system id PK,FK1 PK vseq FK1 ref\_system\_id ref\_system\_name ref\_seq ref\_tag ctime signature sig\_class PΚ sig\_id sig class id sig\_name sig\_class\_name detail encoding FK1 sig\_class\_id sig\_priority PK detail type encoding type sig\_rev sig\_sid detail\_text encoding\_text sensor event PΚ sid PK,FK2 sid PK <u>cid</u> hostname interface FK1 signature filter timestamp FK2 detail FK1 encoding last\_cid data iphdr PK,FK1 cid PK,FK1 <u>cid</u> PK,FK1 sid protocols PK,FK1 <u>sid</u> protocol data\_payload ip\_src ip\_dst description ip\_ver ip\_hlen opt ip\_tos PK,FK1 PK,FK1 PK <u>cid</u> ip\_len ip\_id sid optid ip\_flags ip\_off opt\_proto ip\_ttl opt\_code FK2 ip\_proto ip\_csum opt\_len opt\_data icmphdr udphdr tcphdr flags PK,FK1 cid PK,FK1 sid PK,FK2 cid PK,FK2 sid PK,FK1 <u>cid</u> number PK,FK1 <u>sid</u> <u>sid</u> <u>sid</u> RES1 FK2 FK3 udp\_sport udp\_dport FK3 tcp\_sport RES2 icmp\_type URG icmp\_code FK4 tcp\_dport ACK PSH icmp\_csum udp\_len tcp\_seq icmp\_id udp\_csum tcp\_ack tcp\_off RST icmp\_seq SYN tcp\_res FK1 tcp\_flags FIN tcp\_win valid tcp\_csum description tcp urp services port protocol name description