Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

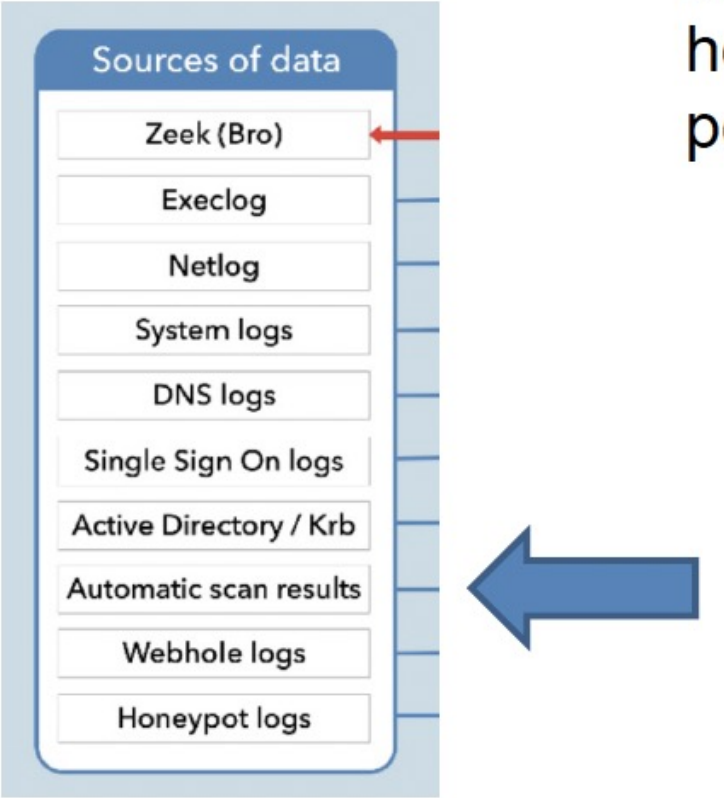
Strumenti per le strutture

Gianluca Peco

Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 - Padova

Public

Strumenti per le strutture



- *(in un mondo perfetto)* va indagata e definita dotazione *standard* (sulla quale sviluppare know-how per facilitarne installazione e manutenzione) per:
  - protezione rete/macchine (non potremo permetterci NGFW - e le relative signature aggiornate annualmemte - per tutte le strutture):
    - EDR, HIDS, NIDS, firewall, …
    - **DNS firewall** (prototipo in funzione);
  - generazione dati da elaborare centralmente:
    - network sniffer (argus), EDR, HIDS, NIDS (zeek), firewall, strumento per raccolta, selezione, normalizzazione log, …

TOOL

SURICATA (HIDS/NIDS)
SNORT (HIDS/NIDS)
ZEEK (NETMON/METADATA/NETFLOW)
ARGUS (NETFLOW)
NTOP&Co (NETMON,NETFLOW,PCAP)
SILK(NETFLOW)
YAF(NETFLOW)
ARKIME(PCAP)
YARA(MALWARE ANALYSIS)
OSQUERY(OSMON/OSANALYSIS)
OPNSENSE/PFSENSE (NGFW)
SECURITY ONION (ALL IN ONE)
ALIENVAULT (ALL IN ONE)

Public

SURICATA

SNORT

ZEEK

ARGUS

NTOP

SILK

YAF

ARKIME

Public

YARA

OSQUERY

OPNSENSE/PFSENSE

SECURITY ONION