BUILDING AND OPERATING A LARGE SCALE SECURITY OPERATIONS CENTER

LIVIU VĂLSAN
FOR THE CERN COMPUTER SECURITY TEAM
SPRING 2017 HEPIX, BUDAPEST
WHAT IS A SECURITY OPERATIONS CENTER?

- Centralized system for the detection, containment and remediation of IT threats
- Ensures that security incidents are properly
  - Identified
  - Analysed
  - Reported
  - Acted upon
SYSTEM DESIGN

- Unified platform for:
  - Data ingress
  - Storage
  - Analytics
- Multiple data access / view patterns:
  - Web based dynamic dashboards for querying and reporting
  - Command line interface that can be easily scripted
- Extensible, pluggable, modular architecture
- Unified data access control policies
LOG COLLECTION

- Progressively scaling up
- Started with Bro, fully in our control
- Currently adding syslog: partial control
- Other 3rd party logs will be added at a later stage
LOG TRANSPORT: KAFKA & FLUME

- Kafka used as a central data backbone
- Flume for ingress, log parsing and normalisation
- Log gateways using Flume as well
- Currently migrating to the centralized Kafka service
- Aiming for having the last 24 hours of data in Kafka
THREAT INTELLIGENCE

- MISP as the sole threat intelligence platform at CERN
- CERN is operating 3 different instance:
  - Main CERN instance with close to half a million IoCs
  - WLCG central MISP instance with more than 160,000 IoCs
  - Development MISP instance used for MISP development (CERN is an active contributor) and for validating new MISP releases
DETECTION

- Detection at the network level offloaded to Bro and Snort.
- Detection in all other types of logs performed using Spark streaming.
  - Space-efficient Bloom filter used for matching the various data fields against IoCs from MISP.
NETWORK TRAFFIC AGGREGATOR AND SPLITTER
LIGHTWEIGHT ENRICHMENT WITH SPARK

- For all data sources
- Must be light to add / quick to obtain
- May not be 100% accurate
- Used in web dashboard & further analysis
- Example: forward and reverse DNS resolution
ADDITIONAL ENRICHMENT

- For malicious activity only
- Increased accuracy (100%)
- Aggregation & correlation
- Used by the Computer Security team for user notifications and follow-up
LESSONS LEARNED

- Lots and lots of bottlenecks encountered.
- Many thanks to our colleagues in the IT department for the support.
- Expect dedicated talks regarding those in future HEPiX meetings.
private String readLine() throws IOException {
    ByteArrayDataOutput out = ByteStreams.newDataOutput(300);
    int i = 0;
    int c;
    while ((c = raf.read()) != -1) {
        i++;
        out.write((byte) c);
        if (c == LINE_SEP.charAt(0)) {
            break;
        }
    }
    if (i == 0) {
        return null;
    }
    return new String(out.toByteArray(),Charsets.UTF_8);
}
WLCG SOC WORKING GROUP

- Mandate to investigate different models for SOCs and advise the WLCG / sites on best practice from the experience of the group.
- Initially focussed around the development of a minimum viable product:
  - Bro IDS & MISP
- Additional components to add to the SOC stack will be investigated next.
- If you’re interested to participate please contact David Crooks or myself.
  - Mailing list: wlcg-soc-wg@cern.ch