Capabilities and Limitations of Endpoint Security Solutions (CLESS)

IETF 104, Monday 25th of March 2019, Prague

Arnaud Taddei (Arnaud_Taddei@symantec.com)

Candid Wueest (Candid_Wueest@symantec.com)

Kevin Roundy (Kevin_Roundy@symantec.com)

Dominique Lazanski (dml@lastpresslabel.com)

Introduction to CLESS

- Why? A gap in the « codification » of endpoint security?
- Why now? Many « environmental » changes (technical, regulations, etc.)
- What?
  - In the long term, a full review of endpoint security in all its dimensions
  - Currently we started with
    - Endpoint Models
    - Threat Landscape
    - Endpoint security capabilities
    - An ideal endpoint security
    - Defence in depth
    - Endpoint security limitations
    - Example from production data
    - Regulatory aspects
- Status? An early draft on purpose, we seek feedback and future collaboration

Where to find it? Table of Content

https://github.com/smart-rg/drafts/blob/master/draft-taddei-cless-introduction-00.txt

Table of Contents

Lessons Learnt Already

- Much harder than initially thought
- Couldn’t find any satisfying:
  - Threat Landscape methodology for endpoint security
  - Capabilities list and methodology for endpoint security (not just 3rd party)
    - Good potential of work for SMART on both threat landscape and capabilities
- Production data from Managed Security Services
  - Interesting methodology
  - Study on the last 3 months on hundreds of enterprise customers
  - Endpoint only security gives a lot of results
  - Critical events not detected by endpoints

Questions for Future Development

- Endpoint modeling between ‘UEs’ and ‘Hosts’
  - Better uniformity across the document
- Threat Landscape Methodology
  - Align with or fork from MITRE ATT&CK?
  - Should it be done in this I-D?
- Intrinsic Capabilities
  - Need a much deeper inventory
- Other Aspects
  - Should we have an economic section?
  - Regulations and Human Rights sections – need a good neutral balance
    - New Requirements, New Limits, New Constraints
  - Other real production data?

QUESTIONS ?

THANK YOU