Secure Information Sharing Sensor Delivery event Network

Abstract

The *SISSDEN* project will improve the cyber security posture of EU entities and end users through the development of situational awareness and sharing of actionable information. SISSDEN builds on the experience of Shadowserver, a non-profit organisation well known in the security community for its efforts in mitigation of botnets and malware propagation. It will provide free of charge victim notification services, and close collaboration with Law Enforcement Agencies, national CERTs, and network owners and providers.

The core infrastructure element of *SISSDEN* is a worldwide sensor network, which will be deployed and operated by the project consortium. This passive threat data collection mechanism will be scalable and complemented by behavioural analysis of malware and multiple external data sources. Actionable information produced by *SISSDEN* will be used for the purposes of nocost victim notification and remediation via organisations such as National CERTs, ISPs, hosting providers and Law Enforcement Agencies such as EC3. It will especially benefit SMEs and citizens, who lack the capability to resist threats alone, allowing them to participate in this global effort. All will benefit from the improved information processing, analysis and exchange of security intelligence - significantly improving cybercrime prevention and ability to counter security breaches/threats.

SISSDEN will deliver multiple high-quality and trusted (free) feeds of salient actionable security information that will be used for remediation purposes and for proactive tightening of computer defences. These unique data feeds will be possible thanks to the development and deployment of a large distributed sensor network based on state-of-the-art honeypot/darknet technologies and the creation of a high-throughput automated data processing centre based in Europe. *SISSDEN* will not only provide in-depth analytics on the collected data but also develop metrics that will be used to establish the scale of some measurable security issues in the EU. Finally, a curated reference data set will be created and published to provide a high-value resource to Academia and researchers in the field, thereby encouraging future innovation.

Key objectives:

1. **Create a large distributed sensor network**. Over 100 passive sensors based on current and beyond state-of-the-art honeypot and darknet technologies will be deployed in multiple organisations, including all 28 EU member states and 6 candidate countries, and will be used to observe malicious activities on an unprecedented scale, without intercepting any legitimate traffic.
2. **Advancements in attack detection**. New types of honeypots, darknets and probes will be deployed to detect, analyse and alert on types of attacks not widely detected today, such as reflective DDoS amplification or attacks against Internet of Things (IoT) devices, which are expected to increase significantly in the coming years as a range of new network-centric technologies are embraced by consumers and SMEs globally.
3. **Advancements in malware analysis and botnet tracking.** The large sensor network will be augmented by an innovative new generation of enhanced sandbox technologies designed for long running monitoring of malware specimen execution and behavioural clustering, to provide even more information on current threats.
4. **Improving the fight against botnets**. Sensor and sandbox data collected will be used for detailed studies of botnet infrastructures. Long term observation of multiple families of current botnets will support anti-botnet research and law enforcement activities. Output will closely align with existing European anti-botnet and anti-cybercrime strategies, as well as providing support to proven strong LEA partnerships, such as with Europol's European Cybercrime Center (EC3).
5. **Collect, store, analyse and reliably process Internet scale security data sets.** The inherent challenges of building and continuously operating reliable data collection, storage, exchange, analysis and reporting systems at high volumes will be solved by multiple innovations in sensor and backend packaging, deployment, integration and data searching, based on consortium members' extensive experience with "big data" approaches, high volume transactional and non-relational data systems.
6. **Share high-quality actionable information on a large scale.** SISSDEN will produce large amounts of intelligence on current threats and all of it will be shared with stakeholders and the larger community, at no cost to them, for the purposes of remediation or for early warning. The project will distribute high-quality data feeds to the majority of the National CERTs in Europe, as well as worldwide, along with Law Enforcement Agencies, Internet providers, network owners and other vetted organisations fighting to defend their networks, SME customers, EU citizens and Internet users against continuous attacks.
7. **Provide objective situational awareness through metrics.** The consortium will have access to huge amounts of high-quality data on cyber threats: primarily obtained by the sensor network but also contributed by the members of the consortium. This unprecedented visibility will enable metrics developed as part of SISSDEN to offer a truly objective, non-vendor

biased overview of the threat landscape in the EU and individual member states.

8. **Create and publish a large scale curated reference data set.** A significant subset of the data produced by *SISSDEN* will be made available to vetted researchers and Academia, addressing the clear and urgent need for large scale, high quality, recent security datasets in order to improve or test defensive solutions. This should become a valuable new resource for powering security research excellence in Europe.

All of these goals, including large scale information collection and dissemination, will be realised in the course of the *SISSDEN* pilot. The TRL 9 pilot will not only demonstrate the technical viability of the underlying concepts and technologies, but also provide actionable, timely, free of charge data and intelligence that will have a positive impact on the security posture of the member states, their citizens and the EU as a whole.

Project Partners

The *SISSDEN* consortium consists of:

Naukowa i Akademicka Sieć Komputerowa	Coordinator	Poland
Montimage EURL	Principal Contractor	France
CyberDefcon Limited	Principal Contractor	United Kingdom
Universitaet des Saarlandes	Principal Contractor	Germany
Deutsche Telekom AG	Principal Contractor	Germany
Eclexys SAGL	Principal Contractor	Switzerland
Poste Italiane – Sozieta per Azioni	Principal Contractor	Italy
Stichting the Shadowserver Foundation Europe	Principal Contractor	Netherlands

Project funding

The *SISSDEN* project has received funding from the European Union Horizon 2020 Programme (H2020-DS-2015-1) under grant agreement n° 700176.

Duration: **From** 1st May 2016 **to** 30th April 2019.
Total project cost: 6 341 775 Euros.
Total EU Contribution: 4 912 692,5 Euros.