Sergey Polzunov

sergey@polzunov.com
+316 443-67-112
The Netherlands
Dutch citizen

https://polzunov.com
https://github.com/traut

Software engineer with more than 15 years of development experience, passionate about building novel technical solutions for cybersecurity, exploring the power of structured cyber threat intelligence, and prototyping advanced threat detection techniques.

WORK EXPERIENCE

Senior Software Engineer @ Threat Research And Detection Engineering (May 2024 - present)
Elastic, Global

Senior Security Data Engineer @ Threat Data Services team (Mar 2022 - May 2024)
Elastic, Global

- Technical ownership, design and implementation of Detonate, a scalable and fully automated malware detonation pipeline. See the Elastic Security Labs article for more details.
- Design and implementation of the internal security data services and telemetry pipelines.

Senior Software Engineer, Freelance (Jul 2021 - Feb 2022)
Fox-IT, Delft, The Netherlands

- Involved in the design and implementation of the internal DFIR tools.
- Worked on evolution and maintenance of Dissect – a digital forensics and incident response framework – https://github.com/fox-it/dissect

Engineering Manager, XDR Hunting Team (Oct 2020 - Jun 2021)
EclecticIQ, Amsterdam, The Netherlands

- Leading the conversation on scoping, design, and implementation of the core components of the EclecticIQ's XDR Platform: data normalization and processing pipeline, data storage architecture, threat detection, and hunting capabilities.
- Provided technical leadership in scoping and implementation discussions.
- Acted as a hiring manager for multiple open roles, seeking, selecting, and hiring new talent.

Lead R&D Engineer (2019 - 2020)
EclecticIQ, Amsterdam, The Netherlands

- Ran multiple R&D initiatives, focusing on advanced CTI processing and analysis use cases, that resulted in finished PoCs with the clear added value evaluation.
- Working closely with Fusion Center analysts, designed and implemented various PoCs, some of which were presented at FIRST Cyber Threat Intelligence Symposium 2019, FIRST Cyber Threat Intelligence Symposium 2020, and FS-ISAC Americas Spring Virtual Summit.
- Implemented experimental features in EclecticIQ Threat Intelligence Platform, contributing proposals to the Platform's development backlog.

Cyber Threat Intelligence Engineer (2018 - 2019)
EclecticIQ, Amsterdam, The Netherlands

- Being part of Fusion Center team — a team of Cyber Threat Intelligence (CTI) analysts with expertise in the public and private sectors, working on fusing streams of intelligence from multiple sources — designed, implemented, and supported of CTI data processing pipeline, delivering intelligence products to Fusion Center's customers, representing critical infrastructure, government, financial sector, and national security. The data pipeline accumulated more than 50M STIX entities in Fusion Center's knowledge database. I also participated in analysis and investigation work.
- Ran multiple Proof of Concept initiatives, developing the tools and solutions, helping the analysts to be more efficient by inventing novel ways for intelligence processing, visualization, and automated analysis.

Senior Software Engineer (2014 - 2018)
EclecticIQ, Amsterdam, The Netherlands

- As a member of the backend engineering team, I was involved in the design, implementation, and evolution of the EclecticIQ Threat Intelligence Platform (TIP).
- Author of open source TAXII server and client implementations in Python: OpenTAXII server and Cabby client library.
- As a member of OASIS Cyber Threat Intelligence Technical Committee (the group tasked with the design and evolution of STIX and TAXII standards), I participated and contributed to the development of STIX/TAXII. OpenTAXII server was one of the first open-source implementations of TAXII 1.0/1.1 server specifications.

Software Engineer (2011 – 2014)
RIPE NCC, Amsterdam, The Netherlands

- As a GII (Global Information Infrastructure) team member, was responsible for implementation and maintenance of the core data processing pipeline based on Hadoop. The pipeline handles daily, hourly and real-time processing of multiple data streams: BGP updates from RIS project, Atlas project's measurements, Maxmind GeoIP database dumps, etc.
- Designed and implemented various data views and derived datasets (in HBase) which are used to provide real-time results for RIPEstat service.

CONFERENCES

- Natural-Language Generation: Creating Intelligence Reports from Structured Data, FS-ISAC Americas Spring Virtual Summit, May 2020.
- Narrator: Generating Intelligence Reports from Structured Data, FIRST Cyber Threat Intelligence Symposium, March 2020.
- Fantastic Groups and Where To Find Them: Identifying the DNA TTPs of Nation-states, OneConference, The Hague, October 2019.
- Evaluate Or Die Trying - A Methodology for Qualitative Evaluation of Cyber Threat Intelligence Feeds, FIRST Cyber Threat Intelligence Symposium, London, March 2019.

OPEN-SOURCE

- **Stixview** — an embeddable JS library for visualizing CTI STIX2 graphs. https://github.com/traut/stixview
- **OpenTAXII** — robust Python implementation of TAXII Services that delivers a rich feature set and friendly Pythonic API. https://opentaxii.readthedocs.io/en/stable/
- **Cabby** — simple Python library for interacting with TAXII servers. https://cabby.readthedocs.io/en/stable/

EDUCATION

- **MEng Computer systems and networks** (2007-2009)
  The Faculty of Informatics and Computer Engineering,
  National Technical University of Ukraine “Kyiv Polytechnic Institute”.
- **BE Computer systems and networks** (2003-2007)
  The Faculty of Informatics and Computer Engineering,
  National Technical University of Ukraine “Kyiv Polytechnic Institute”.