Only Seeing Stars: Enabling the Open Source Scripting Community with OCSF

Mike Bunner (REI Co-Op,)

Your Speaker

Mike Bunner (he/him)
Sr. Security Automation Engineer, REI Co-Op

https://www.linkedin.com/in/mikedba/

This deck, examples and resources:
https://github.com/PaddlingCode/FIRSTCON25

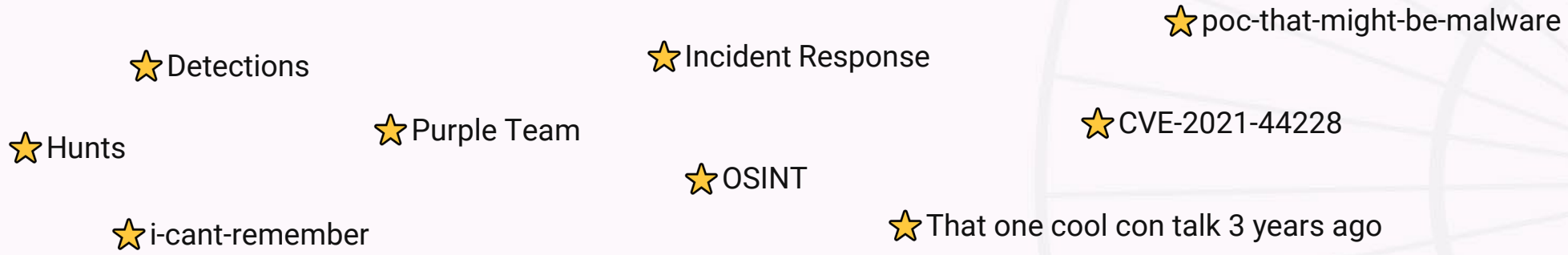
North Cascades National Park, US

Open Source Security is Awesome!

But I find myself..

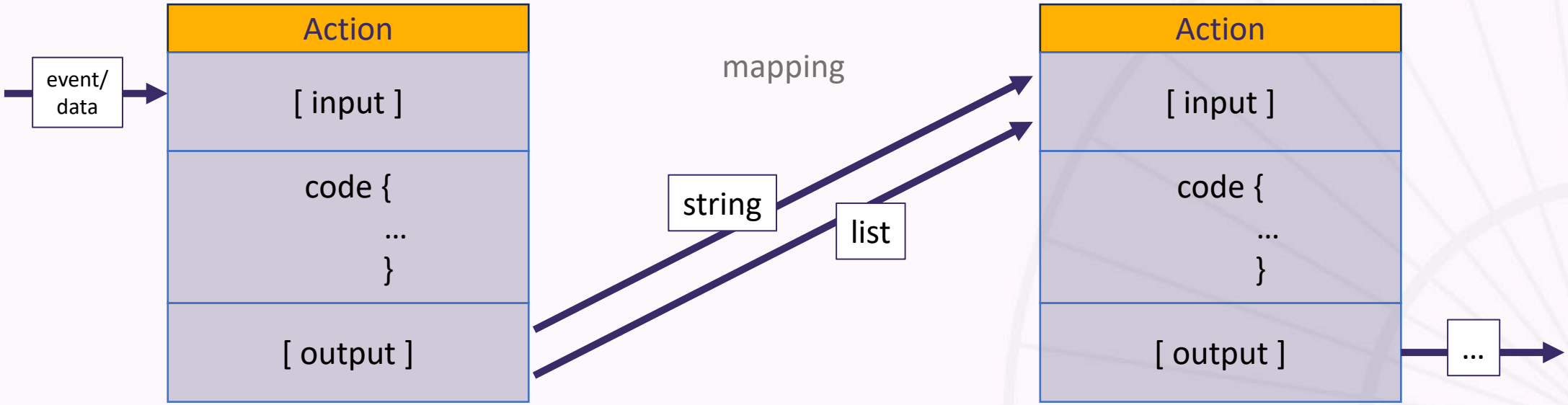
- Running scripts ad-hoc; not CI/CD or SOAR
- Manually building data transforms
- Reverse engineering point-solutions
- Searching multiple repos to complete objects

Yet my GitHub grows..



Commercial SOAR (does this for you)

- Mapping handled in a GUI
- Increased risk of vendor *lock-in*



Data Structure Standards

We need:

- To capture complex objects
- Extensibililty
- Mature and broad support
- Free & open source

Not quite:

- YARA, STIX & OpenIOC are threat based
- Elastic Common Schema (ECS) is limited
- Vendor specific & closed models

Open Cybersecurity Schema Framework (OCSF)

- Extensible & structured
- Community driven
- Vendor agnostic
- But backed and supported by large vendors
  - Cloud Service Providers
  - Enterprise security
  - Identity providers
  - Issue tracking software
  - Data pipelines
- Open source community?

Landscape Shift: **Legitmate**, but **abused** software

- Not outright malicious
- Hides in legitmate traffic
- Full blocks could have business impact
- Org-specific solutions
- Often missed by expensive security solutions

⚠ **And critically important to address!**

The FOS Security Community Delivers

(Free & Open Source)

- Quick response
- Proof of Concepts, detections and scripts
- Free via git repos, Fediverse and other social channels

Automation Roadblocks

- Point solutions
- Disparate information
- Sporadic upkeep
- Unstructured data

Semi-Static Objects in OCSF: **RMMs**

(Remote Management & Monitoring)

- Requires multi-faceted solutions
- Poorly automated today
- No single FOS project or vendor has 100% coverage

OCSF Data Highlights

Domains
Protocols
Executables
Processes
Installation artifacts

Use Cases

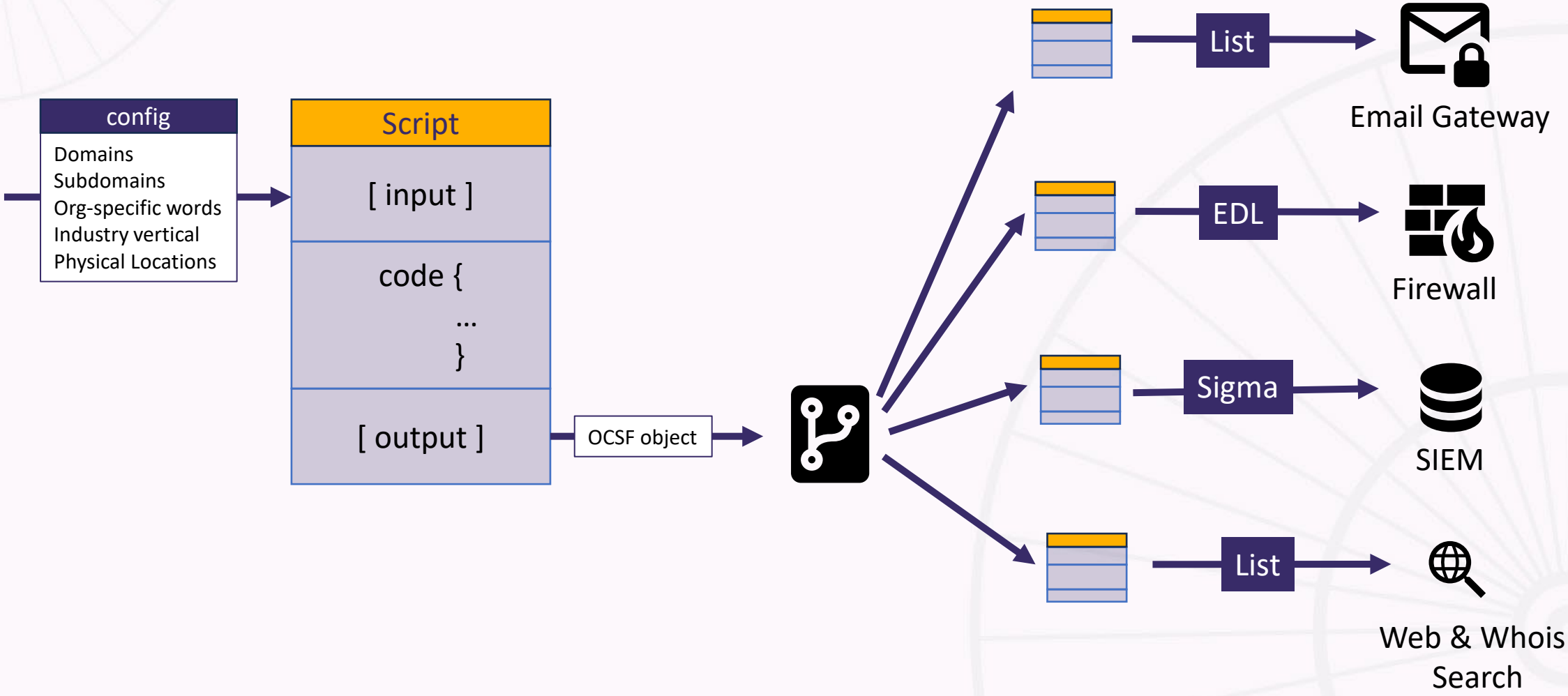
Firewall & Web Proxy – Block/Allow EDLs (External Dynamic List)
MDR & SIEM – Detections & IOAs
Endpoint Management – Removal Scripts

Semi-Static Objects in OCSF: **SaaS**

- Abuse via Living off Trusted Sites/Tunnels
- Difficult to fully block
- Shadow SaaS, PaaS, Cloud and DNS

Data Highlights	Use Cases
Web Domains	Firewall & Web Proxy – Block/Allow
Email Domains	Email Gateway Policy
ASNs, IP Ranges	MDR & SIEM – Usage, Detections
Login URLs	CASB & DLP
Abuse Reporting	Automated abuse reporting

OCSF Adoption in Scripting: {brand} Domain Gen



OCSF Adoption in Scripting: Software Removal

Difficulties

- Uninstall is unavailable or broken
- Persistent and changing artifacts
- Scripts target single PUPs for single point vendor solutions

OCSF Adoption

- Centralized community managed artifacts
- Reusable scripts
  - Iterative improvment
  - More oversight
- Migrate from single-point solutions

Same Object, More Use Cases

Security

- Abuse reporting (URL / email)
- Email policies (Domains)
- APIs (URL)

Governance & Risk

- 3rd Party & Vendor Management
- Licensing oversight
- Privacy Page (URL)
- Stock market ticker (8-K filings)

Operations

- CDN and IP lists (URL)
- Monitoring and outage links (URL)
- PSIRT and RSS feeds (URL)

Lessons Learned

- Directly creating objects was tough
- Some objects may not exist yet
- Steeper learning curve
- Lack of utility modules

Call to Action!

1

Join the Community!

- **https://ocsf.io**
- Slack Channel
- ⭐ the OCSF GitHub Repo

2

Retrofit / Implement OCSF

- Update a popular script
- Migrate RMM / LOTS / LOTT objects
- Release your next script with OCSF input / output

3

Build a Module

- PowerShell
- Python

Mike Bunner (he/him)
Sr. Security Automation Engineer, REI Co-Op

https://www.linkedin.com/in/mikedba/

This deck, examples and resources:
https://github.com/PaddlingCode/FIRSTCON25

Thank you!

Mount Rainier National Park, US

Resources, Attribution & Licensing

- Intro and Thank you slide photos of and owned by Mike Bunner (Limited Use Licensing for this Deck)
- OCSF logo (ocsf.io) (Apache 2.0 License, Linux Foundation)
- Icons on Domain Gen slide by pictogrammers.com (Apache 2.0 License)
- Elastic Common Schema (ECS) (Apache 2.0 License)