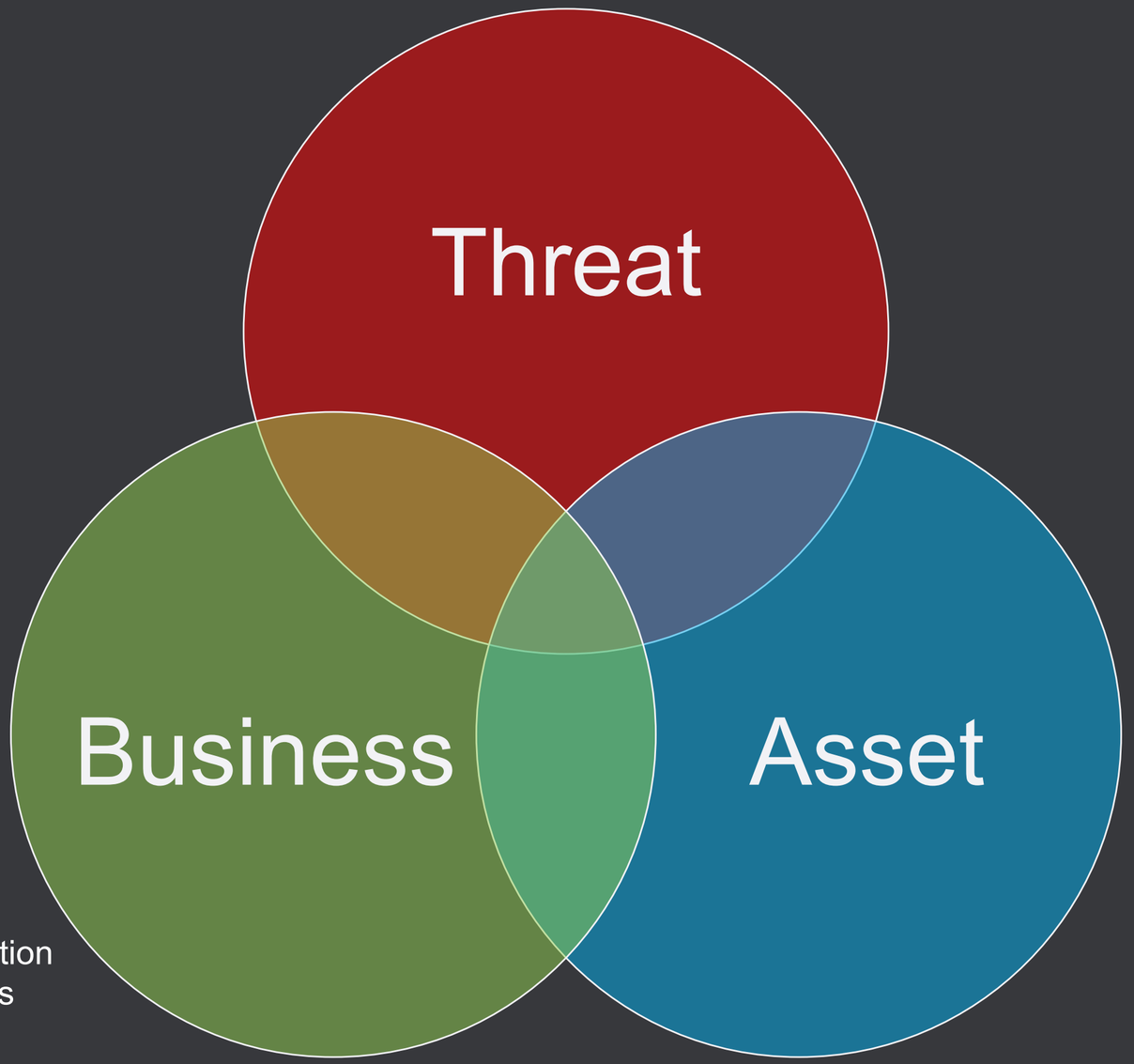
Power of Community for Evolution of Security Capabilities

@LiorKolnik

Demisto

Information domains



- VIP Accounts
- CRM / ERP
- Travel activity
- Customer geolocation
- Downtime windows

- IT (+Cloud)
- Security tools

Attackers have no boundaries

SOAR Community

- CISO
- Technical Director
- Analyst
- Security Vendor
- SOAR Vendor
- Researcher

CISO

- Business risk – map, measure, reduce
- Strategies
- Budgets
- Vendor relations
- Threats (Strategic view)

Tech Director

- Playbooks
- Tools - Choosing, Leveraging
- (Global) Team Collaboration
- Training

Analyst

- Playbook-aware Analysis Methods
- Threats (Tactical)
- Tools – Operation
- Reports & communication
- Case Collaboration
- Feedback loop

Before – Let’s buy/code another tool

After – let’s design a new playbook

Vendors

APIs

- REST
- Comprehensive
- Documented
- Reliable
- Current

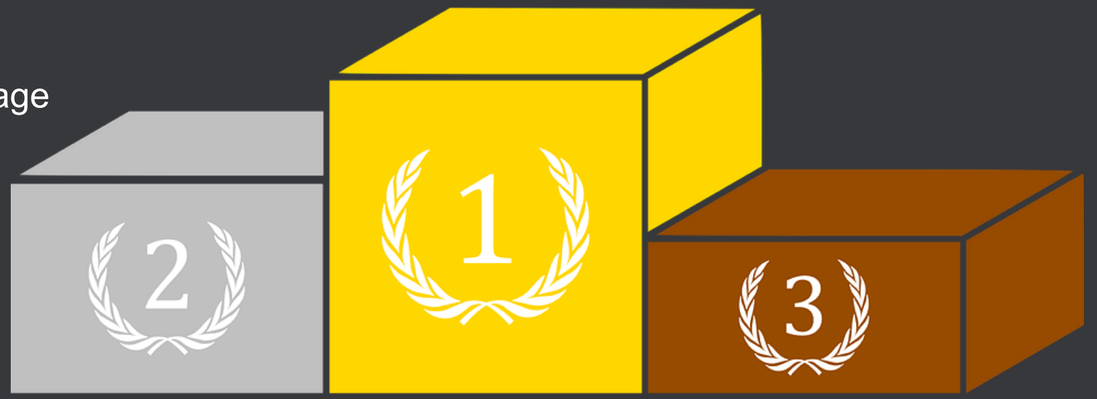
- Testing -> Feedback -> Responsiveness
- Customer-driven
- Interop is a strength!

Partnering with SOAR

1. API – Comprehensive, Documented
2. Here‘s a lab instance full of data that makes sense.
3. Here are use cases our customers care about the most.
4. Here’s where we think SOAR can best complement our product and provide value to the customer

Let’s build it together!

1. API Docs
2. Partner account / install package

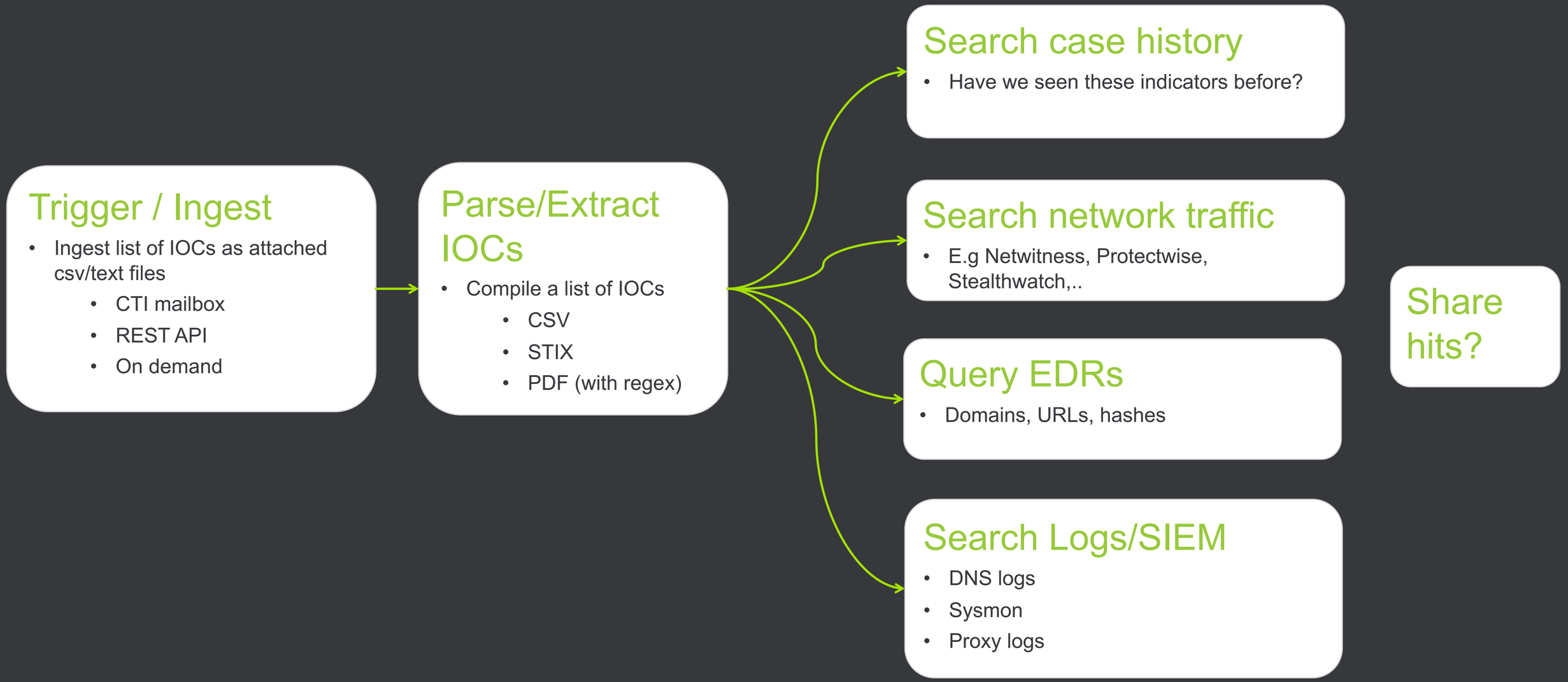


1. Immature APIs
2. Missing documentation

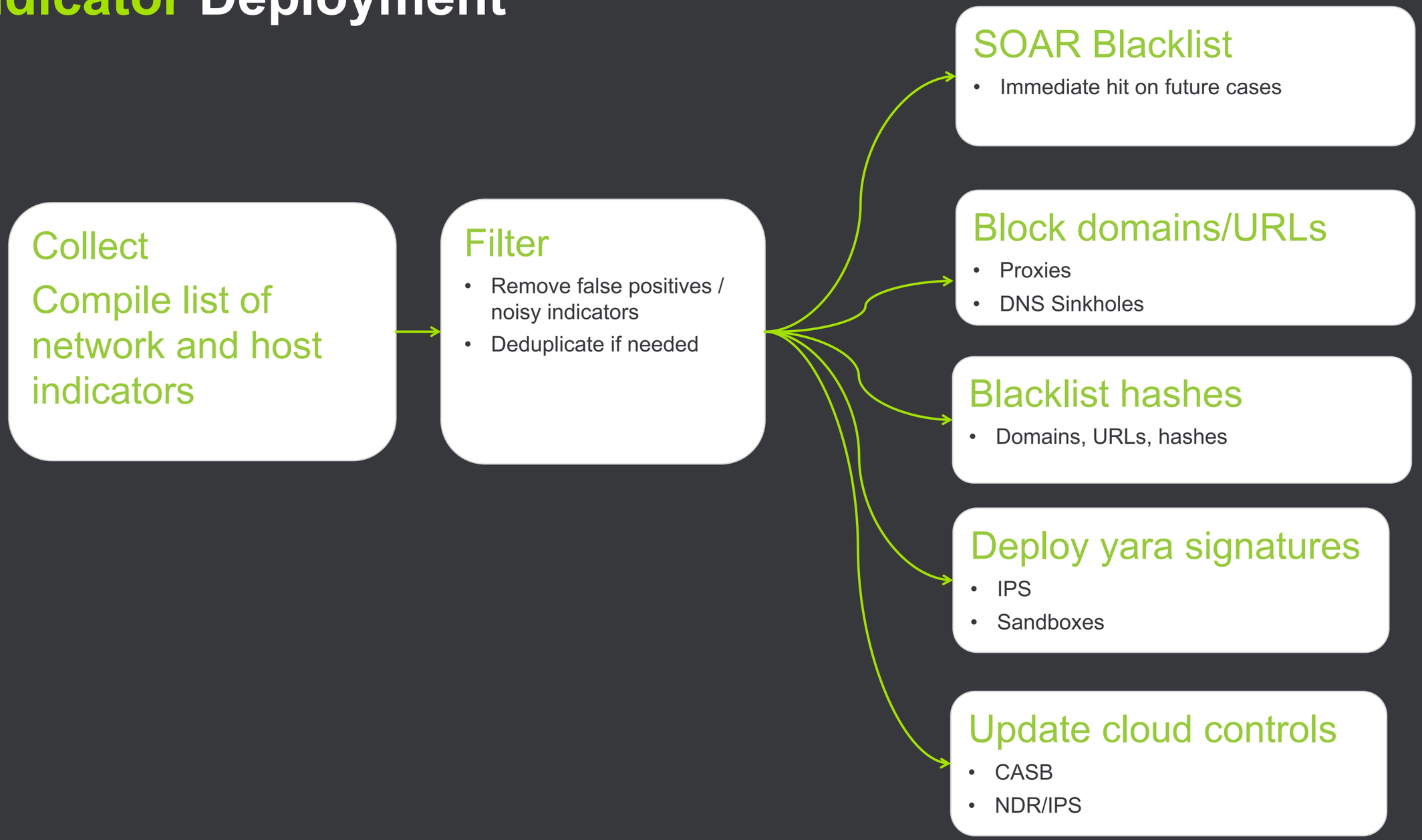
But – interested in improving!

Automation enables sharing

Indicator Hunting



Indicator Deployment



Common questions

- What are other teams doing?
- New to a tool - Tips / useful features?
- Vendor X is missing this API, do you know if it’s coming soon?
- Caveats of certain tools - what should I know before investing / deploying?
- I have this idea for a process/playbook to solve a problem - what do you think? Is there a better way to do this?

Partnership opportunities

- Integrated exercises – Share, receive hits
- Playbook development projects
- Hunting across the fence – well-defined, with approval on hits
- Playbook sharing seminar
  - Engage peer organizations
  - existing + wishlist
  - Divide the work
- Your SOAR Vendor
  - Design partnership for features you care about
  - Introduction to peers (other customers with similar interests)
  - Collaboration challenge!

Give back

- Code fixes & upgrades (connectors / integrations / apps)
- Playbook improvements
- Indicators (with relevant context)
- False positives
- Deployment lessons learned
- Metrics
  - Security (Risk reduction)
  - Efficiency (value)

- Trust and value

Free code, knowledge & Slack community

MIT-licensed Playbooks, Scripts, API client code (integrations)

https://github.com/demisto/content

https://DFIRCommunity.*Slack.com* (~4k users)

All discussions useful to defenders are welcome

Ping me for direct invite (or through our site)

Twitter - DM @LiorKolnik

lior@demisto.com

Thank You