Automated Incident Response
Bring Your Own SOAR

GitLab Security Incident Response Team

Valentine Mairet
Manager, EMEA

Harjeet Sharma
Staff Security Engineer
In this workshop, you will learn about:

- The GitLab Security Incident Response Team
- Automation opportunities in incident response
- Integrating multiple platforms using Tines
- Creating your own automations to make your lives easier
But first...who are you?
Workshop Breakdown

30 min
Theory
A little bit of context

10 min
Break
Get yourself ready

30 min
Lab 1
Let’s build something together!

40 min
Lab 2
Let’s build something on your own!

10 min
Closing Notes
Conclusion, future work, Q&A
First Challenge

Let’s create your accounts!

- Tines
- GitLab
- Slack

http://bitly.ws/Sk4Y

(this is not a phishing domain)
Outline

● Who is GitLab SIRT
● A day at SIRT
● It’s not just incident response
● Automation opportunities
● A day at SIRT - walkthrough
Who are we?

VM
- Offensive security
- Coding
- Threat hunting
- Mountains
- Automation

Harjeet
- Detection engineering
- Monitoring
- Learning new things like AI
- Traveling
- Automation
Who is us?

- GitLab
- GitLab Security
- Security Operations
- Security Incident Response Team
When we think IR automation, we think about investigations:

How can I analyze faster?

- Filtering logs
- Gathering IoCs
- Enrichment
- Mundane tasks like blocking a user or leaked key revocation
Where to use automation?

**Detection Engineering**

- All alerts should uphold quality standards
- Team members review/approve alerts
- Deploy alerts automatically to our SIEM
- Generate metrics about alerts
- SIEM-agnostic solution
Where to use automation?

Incident Management

- Make it easy to report incidents
- Automate the initial Severity/Priority triage
- Keep ongoing incident documentation up to date
- Use GitLab as SSoT for incidents
- Smooth incident handovers available to the whole team
- High-quality and consistent incident reviews
- Metrics on our incidents
Where to use automation?

**Metrics Generation**

- Insights on most/least noisy alerts/incidents
- Identify trends
- To reduce alert fatigue
- Insights on most/least common alerts/incidents
- Make it easy for team members to provide feedback on alerts
- Insights on false/true positives alerts/incidents
- Metrics to justify necessary team growth
Why automate?

★ To make it easy
★ To standardize
★ To save time
★ To not forget
★ To scale better
And so, we automated:

- Alert creation
- Alert deployment
- Alert tuning
- Incident reporting
- Incident handling
- Incident handovers
- Incident reviews
- Metrics generation
Walkthrough

A typical scenario to show the entire pipeline
Walkthrough

- GitLab API tokens can be dangerous. We want to monitor their creation.
  - We create an alert as code
  - We deploy this alert on our SIEM through our pipeline
  - We wait...

- Alert triggers
  - Automation validates the creation of the token directly with the actor
  - Automation notifies SIRT
  - SIRT closes the alert and gives feedback.

- End of day
  - SIRT writes a handover for the next responder on call.
Alert as code

```json
{
    "name": "SecOps.gitlab.any_pat_created",
    "message": "{prod}-{BlackLab}- PAT created for blacklab.com account \$username",
    "description": "$parsed_json",
    "subcategory": "SecOps",
    "isActive": true,
    "alertCorrelationContext": {
        "querySourceCode": "from my.synthesis.railsprod.logs where controller = 'Profiles::PersonalAccessTokensController' and action='create' select username as entity_username",
        "correlationTrigger": {
            "kind": "each"
        }
    }
}
```
Deployment pipeline

<table>
<thead>
<tr>
<th>fetch</th>
<th>process</th>
<th>upload</th>
<th>scheduled</th>
</tr>
</thead>
<tbody>
<tr>
<td>fetch_changed_files</td>
<td>process_files</td>
<td>update_rules</td>
<td>on_schedule</td>
</tr>
</tbody>
</table>
User Attestation Module (UAM)

SIRT detected an event:
my.alert.gitlab_workshop.SecOps_gitlab_any_pat_created

Actor: gg
User Agent (if applicable):
Mozilla/5.0+%28Macintosh%3B+Intel
+Mac+OS+X+10_15_7%29+AppleWebKit
%2F537.36+%28KHTML%2C+like+Gecko
o%29+Chrome%2F116.0.0.0+Safari%2F537.36

Alert Time: 2023-08-24+06%3A31%3A11.396
IP Address: 212.30.60.1

This Was Me  I don't recognize this
**BlackLab Watchdog**

**BlackLab Watchdog**

[prod]-[BlackLab]- PAT created for blacklab.com account gg:

**Actor:**
- gg

**Runbook Link:**
- [Link](https://eu.devo.com/#/loxcope/alert/goToQuery?id=16640875)

**Alert_Name:**
- SecOps_gitlab_any_pat_created

**Event Time:**
- Thu Aug 24 06:31:18 UTC 2023

**Assign alert to other team member**
- Select a user

**SecOps Application default link**
- Link to SecOps Application

**TriageBot**

1:33 PM

User reported they are not aware of the activity related to the alert 16640875. Please investigate further.
Escalation

BlackLab Watchdog 1 minute ago

Awesome, I have opened an issue for you. You can access it by visiting http://34.66.143.75/gitlab-instance-2105a4c2/security-incident-response-team/incidents/-/issues/4
Hello team! It’s time for the handover! 🎉

Is there any work required to continue? Are there any high-severity/high-priority incidents where the investigation or mitigation process phase is still ongoing? Write a detailed handover message below so that the next SIRT engineer on-call can pick up from where you left off.

Nothing today—it was a quite day.

Do you have any additional information about lower-severity incidents that could be relevant in case of escalation? Notify the team below. You still retain ownership of this incident but, as long as it doesn’t escalate, it can wait for the next business day.

GG created an API key and forgot about it. We originally thought it was a hacker but turns out, it was one of her automations.

Send

Thanks for the handoff update. It’s been forwarded to the team. They all highly appreciate your work! 🥰
Handogotchi Lite 12:11 PM

(沌 o^v^o)  Hando has the warm handoff ready for the team: 🥰
Handoff 2023-08-24
by Greylag Goose

Work required to continue:
Nothing today—it was a quite day.

Additional information
GG created an API key and forgot about it. We originally thought it was a hacker but turns out, it was one of her automations.

Feed Pet Give us a fun fact!
Break

Validate that you have access to:

- Tines
- GitLab
- Slack

Shout if you don’t!
Lab 1

Let’s make teams!

- At least 1 laptop per team
- At least 1 technical person per team

Shout if you have questions.

If you don’t want to shout, you can DM us on Slack.

@Greylag Goose (VM)  @Harjeet
Lab 1

Tokenheimer - automatic token revocation
Lab 1

Open the **Tokenheimer** story

Open the **Lab 1** story

Copy/paste the Tokenheimer story into Lab 1

Rename the first action to “Tokenheimer - [your team’s name]”

Once everyone has their own Tokenheimer story, we’ll create /commands for each team.
Lab 1
Show off your Tokenheimer!
Lab 2
Tokenheimer Version 2
Lab 2

Build upon your Tokenheimer story

Need ideas?

- Tokenheimer also scopes a token (type, user, groups, etc)
- Tokenheimer accepts multiple tokens
- Tokenheimer creates an incident
Lab 2

Show off your Tokenheimer v2!
What we automated today

- Alert deployment pipeline
- Alert handling in Slack
- User attestations
- Team handovers
- Token revocation
What we’ve already automated at home

- Reporting incidents
- Assessing Severity and Priority
- Triaging incidents
- Keeping incidents up-to-date
- Incident review process
- Transferring Slack messages over to GitLab incidents
- Handogotchi++
- Collecting metrics on detections and incidents
The beast we’ve made

GitLab Universal Automated Response and Detection

- Alert deployment pipeline
- Slack-powered alert handling capabilities
- Alert feedback support
- UAM integrations
- Alert metrics collection
Future Work

GitLab Universal Automated Response and Detection

- MITRE ATT&CK expansion
- Risk scoring
- Dashboards!
- AI-integration
  - Enrichment
  - Assisted alert handling
  - Reporting
GUARD Publications

- Speaking at mWISE on September 18-20
- Blog series incoming

https://about.gitlab.com/blog/categories/security/
As promised...

All we’ve talked about today is opensourced here:

Automated Incident Response 🌐
Project ID: 48761321 🛠️


Because Transparency is one of our core values!
THANK YOU!