Detection Rules Explorer - Quick Reference

🚀 Quick Start Commands

Initial Setup


bash

```
# Configure Git
git config --global user.name "Your Name"
git config --global user.email "your.email@company.com"

# Setup SSH (optional but recommended)
ssh-keygen -t ed25519 -C "your.email@company.com"
cat ~/.ssh/id_ed25519.pub  # Add this to GitHub

# Test SSH
ssh -T git@github.com
```

Create Detection Rules Repo


bash

```
git clone git@github.com:YOUR-USERNAME/detection-rules.git
cd detection-rules
mkdir -p rules/windows/execution rules/linux/execution rules/cloud/aws
# Add your first rule (see example-rule.yml)
git add .
git commit -m "Initial rules structure"
git push -u origin main
```

Create Explorer Repo


bash

```
npx create-next-app@latest detection-rules-explorer
cd detection-rules-explorer
npm install lucide-react js-yaml
git init
# Copy all config files from artifacts
git submodule add https://github.com/YOUR-USERNAME/detection-rules.git rules
git submodule init && git submodule update
npm run prebuild
npm run dev  # Test locally
git add .
git commit -m "Initial commit"
git remote add origin git@github.com:YOUR-USERNAME/detection-rules-explorer.git
git push -u origin main
```

📝 Daily Workflow

Add a New Rule

bash

```
cd ~/detection-rules
cat > rules/category/new-rule.yml << 'EOF'
id: rule-2024-XXX
name: Rule Name
description: What it detects
severity: high
type: query
domain: endpoint
# ... (see example-rule.yml for full template)
EOF
git add .
git commit -m "Add [rule name]"
git push
```

Update Explorer Locally

bash

```
cd ~/detection-rules-explorer
git submodule update --remote
npm run prebuild
npm run dev
```

Deploy Changes

bash

```
git add .
git commit -m "Update submodule"
git push
# Or manually trigger in GitHub Actions
```

🔧 Configuration Files Checklist

Copy these files from the artifacts to your project:

detection-rules repository

- [ ] `rules/windows/execution/suspicious_powershell_encoded.yml` - Example rule
- [ ] `README.md` - Documentation

detection-rules-explorer repository

- [ ] `.gitignore` - Git ignore rules
- [ ] `next.config.js` - Next.js config
- [ ] `package.json` - Update scripts section
- [ ] `postcss.config.mjs` - PostCSS config
- [ ] `tailwind.config.js` - Tailwind config
- [ ] `app/globals.css` - CSS styles
- [ ] `app/layout.js` - Root layout
- [ ] `app/page.js` - Main component
- [ ] `scripts/prebuild.js` - YAML converter
- [ ] `.github/workflows/deploy.yml` - CI/CD workflow
- [ ] `README.md` - Documentation

🌐 URLs to Remember

Replace `YOUR-USERNAME` with your GitHub username:

- **Explorer Site**: `https://YOUR-USERNAME.github.io/detection-rules-explorer`
- **Rules Repo**: `https://github.com/YOUR-USERNAME/detection-rules`
- **Explorer Repo**: `https://github.com/YOUR-USERNAME/detection-rules-explorer`
- **GitHub Actions**: `https://github.com/YOUR-USERNAME/detection-rules-explorer/actions`

- **GitHub Pages Settings**: `https://github.com/YOUR-USERNAME/detection-rules-explorer/settings/pages`

⚙️ package.json Scripts

Update your `package.json` scripts section:


json

```
{
  "scripts": {
    "prebuild": "node scripts/prebuild.js",
    "dev": "npm run prebuild && next dev",
    "build": "npm run prebuild && next build",
    "start": "next start",
    "lint": "next lint"
  }
}
```

🎯 Rule YAML Template


yaml

```yaml
id: rule-2024-XXX
name: Rule Name
description: Detailed description
author: Security Team
created: 2024-10-19
updated: 2024-10-19
severity: high  # low, medium, high, critical
type: query     # query, threshold, eql, ml
domain: endpoint  # endpoint, network, cloud, web
language: kuery   # kuery, kql, lucene, eql
tactics:
  - execution
  - defense_evasion
techniques:
  - T1059.001
os:
  - windows
data_sources:
  - process
  - command_line
use_cases:
  - threat_detection
enabled: true
query: |
  process where event.type == "start"
false_positives:
  - Known legitimate scenarios
risk_score: 73
```

🐛 Common Issues & Fixes

Issue: "Repository not found" during build

Fix: Make detection-rules repository **Public**

Settings → Danger Zone → Change visibility → Public

Issue: "404 Not Found" on GitHub Pages

Fix: Enable GitHub Pages

Settings → Pages → Source → GitHub Actions

Issue: Submodule not updating

Fix: Update manually

bash

```
cd ~/detection-rules-explorer
git submodule update --remote
git add rules
git commit -m "Update submodule"
git push
```

Issue: Font errors in development

Fix: Use simple layout.js (already in artifacts)

Issue: Rules not loading in production

Fix: Check basePath in next.config.js matches repo name

📦 Dependencies

detection-rules-explorer

json

```
{
  "dependencies": {
    "js-yaml": "^4.1.0",
    "lucide-react": "^0.263.1",
    "next": "14.2.0",
    "react": "^18.2.0",
    "react-dom": "^18.2.0"
  }
}
```

✅ Pre-Deployment Checklist

- [ ] Git configured with name and email
- [ ] SSH key added to GitHub (recommended)
- [ ] detection-rules repo created and **PUBLIC**
- [ ] At least one example rule added
- [ ] detection-rules-explorer repo created and **PUBLIC**
- [ ] All config files copied from artifacts
- [ ] Submodule added with HTTPS URL
- [ ] `npm run prebuild` works locally
- [ ] `npm run dev` shows rules correctly
- [ ] GitHub Pages enabled (Source: GitHub Actions)
- [ ] First deployment completed successfully

🎓 Learning Resources

- **MITRE ATT&CK**: https://attack.mitre.org/
- **Next.js Docs**: https://nextjs.org/docs
- **Tailwind CSS**: https://tailwindcss.com/docs
- **GitHub Actions**: https://docs.github.com/en/actions
- **Elastic Detection Rules**: https://github.com/elastic/detection-rules

---

💡 Pro Tips

1. **Version Control**: Tag rule releases (e.g., v1.0.0)
2. **Documentation**: Keep rule descriptions detailed
3. **Testing**: Validate rules before merging
4. **Collaboration**: Use PR templates for rule submissions
5. **Monitoring**: Watch GitHub Actions for build failures
6. **Backup**: Export rules.json periodically
7. **Performance**: Keep rule files under 100KB each
8. **Organization**: Use consistent naming conventions

📧 Email Template Content

Subject: Detection Rules Explorer - Implementation Guide

Body:

Hi Team,

Please find attached the complete implementation guide for the Detection Rules Explorer project.

What's Included:

- Complete setup guide (PDF/Markdown)
- All configuration files as code artifacts
- Example rule template
- Quick reference guide
- Troubleshooting section

Key Features:

- ✅ Web-based rule explorer with search and filtering
- ✅ Automatic daily updates via GitHub Actions
- ✅ Free hosting on GitHub Pages
- ✅ Version-controlled YAML rule storage
- ✅ Mobile-responsive design

Getting Started:

1. Follow the "Complete Setup Guide" document
2. Copy configuration files from artifacts
3. Deploy to your GitHub organization
4. Start adding detection rules

Live Demo: https://mcpacket.github.io/detection-rules-explorer

Estimated Setup Time: 1-2 hours

Please let me know if you have any questions!

Best regards, [Your Name]

Document Version: 1.0
Last Updated: October 2024