# Inside SOC: Triage Smarter, Not Harder

Tom DeJong

# About Me

### BHIS SOC

Triage Lead | DFIR

### Education

Information Technology Degree

### Hobbies

Snowboarding
Rock Climbing
Hiking

### Contact

tdejong@blackhillsinfosec.com

www.linkedin.com/in/dejongtom

# Today's Agenda

- Triage Fundamentals
- Anatomy Of An Alert
- Real Threat vs Noise
- Common Mistakes
- Live Demo
- Triage Mindset
- Triage Process
- Escalation vs Closure
- Real World Tips
- Q&A

# What Is Triage?

| Key Goals | What It Involves |
|---|---|
| • Determine severity & impact of an alert | • Reviewing alert metadata |
| • Identify real threats that need escalation or immediate action | • Judging if behavior is normal, suspicious, or malicious |
| • Document decisions & findings | • Make a decision: escalate, further investigation, or close |
| • Filtering out false positives | • Enriching data with threat intel or internal context |

# Why Triage Matters

- Becoming more efficient
- Reducing alert fatigue
- Improving threat detection
- Building trust in your decisions

# Triage Mindset

## Efficient & Decisive

- Efficient not rushed
- Decision oriented
- Calm under pressure

## Analytic & Context Aware

- Curious not complacent
- Context driven
- Pattern oriented
- Skeptical not paranoid

## Clear & Communicative

- Communicative
- Consistent documentation
- Ask questions

# Anatomy of an Alert

## Core Elements

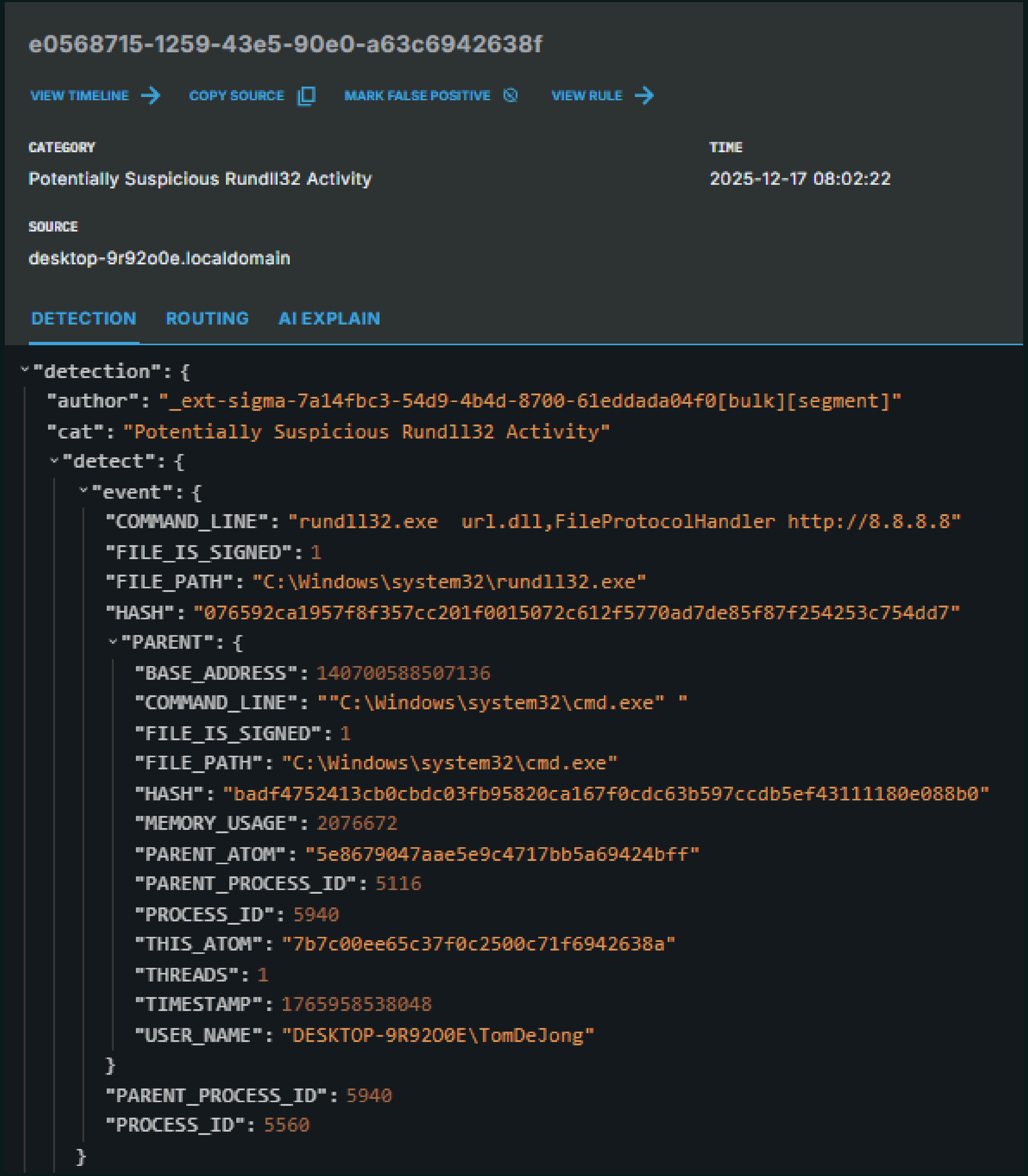
- Alert/Rule Name
- Detection Logic
- Timestamp
- Username
- Hostname
- Process ID
- Process Name
- Command Line
- File Path
- Hashes
- Domain
- Source IP/Port
- Destination IP/Port

## Questions to Ask

1. Is this normal for the user/host?
2. Does the command/ domain look suspicious?
3. Have I seen this pattern before?
4. Do I have enough context?
5. What logs or tools can verify this?

## Work Smarter

- Spot red flags early
- Focus on key data fields
- Check for enrichments
- Correlate with other alerts or logs
- Refer to internal documentation



CATEGORY
Potentially Suspicious Rundll32 Activity

TIME
2025-12-17 08:02:22

SOURCE
desktop-9r92o0e.localdomain

```
"detection": {
  "author": "_ext-sigma-7a14fbc3-54d9-4b4d-8700-61eddada04f0[bulk][segment]"
  "cat": "Potentially Suspicious Rundll32 Activity"
  "detect": {
    "event": {
      "COMMAND_LINE": "rundll32.exe  url.dll,FileProtocolHandler http://8.8.8.8"
      "FILE_IS_SIGNED": 1
      "FILE_PATH": "C:\Windows\system32\rundll32.exe"
      "HASH": "076592ca1957f8f357cc201f0015072c612f5770ad7de85f87f254253c754dd7"
      "PARENT": {
        "BASE_ADDRESS": 140700588507136
        "COMMAND_LINE": ""C:\Windows\system32\cmd.exe" "
        "FILE_IS_SIGNED": 1
        "FILE_PATH": "C:\Windows\system32\cmd.exe"
        "HASH": "badf4752413cb0cbdc03fb95820ca167f0cdc63b597ccdb5ef43111180e088b0"
        "MEMORY_USAGE": 2076672
        "PARENT_ATOM": "5e8679047aae5e9c4717bb5a69424bff"
        "PARENT_PROCESS_ID": 5116
        "PROCESS_ID": 5940
        "THIS_ATOM": "7b7c00ee65c37f0c2500c71f6942638a"
        "THREADS": 1
        "TIMESTAMP": 1765958538048
        "USER_NAME": "DESKTOP-9R92O0E\TomDeJong"
      }
      "PARENT_PROCESS_ID": 5940
      "PROCESS_ID": 5560
    }
```

https://github.com/refractionPOINT/sigma-limacharlie/blob/rules/latest/windows_process_creation/proc_creation_win_rundll32_susp_activity.yml

# The Triage Process

## Review The Alert

- Carefully read the alert
- Check severity, rule name, detection logic, and key metadata
- Ask What triggered the alert? What behavior was flagged?

## Gather Context

- Check the users role and behavior history
- Check the asset involved such as the endpoint or server
- Enrich the alert with threat intel
- Review relevant logs or previous alerts

## Make a Decision

- Based on the alert and context decide one of the following
  - **Escalate**: Malicious or highly suspicious
  - **Investigate Further**: Still unclear or potentially important
  - **Close**: Benign, false positive, or known behavior

## Document Outcome

- Document a note saying
  - What you reviewed
  - What context you found
  - Why you chose to escalate, close, or investigate further
- Include URLs or screenshots
- Follow internal documentation standards

# Real Threat or Just Noise

## Real Threat

Identify red flags that spark a deeper investigation

- Behavior that is abnormal for the user/host
- Hacking tools (e.g. mimikatz, metasploit)
- Sequence of alerts showing multi-step activity (e.g. execution → lateral movement → exfiltration)

## Tools & Techniques

- SIEM/EDR enrichment
- Threat intelligence platforms (e.g. VirusTotal, URLScan)
- Internal playbooks (What’s the SOP for this alert type)
- Host/user baselining (What’s normal for this environment)

## Just Noise

Identify benign patterns that are expected in the environment

- Scheduled PowerShell Backups
- Admins using RMM tools (e.g. PsExec, RDP)
- Known good external domains (e.g. Microsoft Telemetry)
- Vulnerability scanners hitting systems

## When in Doubt

- Search for past occurrences of the alert
- Default to “Investigate More” instead of blindly escalating
- Ask a senior analyst for help
- Document what you tried, even if you’re still unsure

# Escalate or Close

| Criteria For Escalation | Criteria For Closure |
|---|---|
| • Confirmed malicious behavior<br>• Behavior matches known attack patterns | • Alert from a noisy or broad rule<br>• Expected behavior of a known business process |
| • Abnormal behavior for the user/host<br>• Connections to suspicious/malicious IP/domain | • Activity covered by existing tuning/ allowlist<br>• Benign network behavior |
| • Use of unauthorized tools<br>• Activity on critical system | • Alerts triggered by internal tools<br>• No indicators of compromise |
| • Persistence mechanism or signs of backdoor<br>• Requires containment or isolation | • Alert in test or lab environment<br>• Repeated alert that is already escalated or handled |

# Common Mistakes To Avoid

### Escalating Without Evidence

**Why it's harmful:** Wastes time, erodes trust, & creates unnecessary alert noise

**What to do instead:** Investigate, enrich, & document. Escalate with proper justification

### Over Investigating Low Risk Alerts

**Why it's harmful:** Reduces time for higher priority work & increases burnout

**What to do instead:** Use internal resources & context to confidently close benign alerts

### Skipping Context Checks

**Why it's harmful:** Can lead to false positives or missed threats

**What to do instead:** Check internal documentation befre fully digging into an alert

### Weak or Missing Documentation

**Why it's harmful:** Creates gaps for audit & leads to repeated triage of the same alert

**What to do instead:** Clearly document what was investigated, what you found, & what decision you made

### Not Asking For Help When Needed

**Why it's harmful:** Can slow analyst growth, increases risk of mistakes, & leads to burnout

**What to do instead:** Ask questions to your team

### Treating All Alerts The Same

**Why it's harmful:** Leads to alert fatigue, burnout, & can be a misallocation of time

**What to do instead:** Prioritize high value assets, suspicious behavior or known threat patterns.

# Tips For Making The Right Call

### → Don’t escalate out of fear

- Escalation should be evidence based not an emotionally driven decision
- If you feel unsure investigate more until you have the evidence you need

### → Use a checklist

Before escalating or closing an alert ask yourself

- Is this activity abnormal?
- Does this activity pose a risk to the business?
- Is there enough context to justify an action?
- Can I describe why this is suspicious/malicious?

### → Know your environment

- What looks suspicious in one company may be totally normal in another
- Build familiarity with asset roles, user behavior, and common processes & procedures

# Smart Documentation Tips

## What To Include In a Good Triage Note

- **Summary**
  Description of what triggered the alert
- **Actions Taken**
  Checks performed during investigation
- **Findings**
  Key details found during investiagtion
- **Decisions**
  Why you chose to escalate, close, or investigate further

## Tips for Better Smarter Notes

- **Be Specific**
  Document detailed findings
- **Be Concise**
  Summarize findings
- **Be Consistent**
  Use the same structure across investigations
- **References**
  Include links to resources used/found

# Basic Documentation Template

[Summary]
Brief description of the alert and what triggered it

[Actions Taken]
Checks you performed (tools, logs, enrichment sources)

[Findings]
Key context, suspicious or benign behavior, notable evidence

[Decision]
Escalated, closed, Investigate further | Document your reasoning for this decision

- Use bullet points for clarity
- Keep it short but meaningful
- Link to relevant tools or logs if allowed

# Soft Skills
# That Make A Difference

### Communication

- Write concise & clear notes
- Asking good questions
- Sharing relevant updates

### Active Listening

- Listening carefully before reacting
- Taking time to understand context
- Asking clarifying questions

### Collaboration

- Sharing findings or shortcuts with team
- Picking up slack when things get busy
- Giving & receiving feedback without ego

### Composure

- Using playbooks when its chaotic
- Think before you escalate
- Managing time and focus when busy

# Managing Alert Fatigue

## Alert Fatigue Symptoms

- Skimming alerts
- Escalating to be “safe”
- Closing alerts too quickly
- Feeling burnout

## Why It Happens

- Poorly tuned detections
- Pressure to act quickly on every alert
- Repetitive low-fidelity alerts
- Growing workload without automation or support

## Managing Fatigue

- Leverage internal documentation
- Use enrichment wisely
- Tune & improve detections
- Take mental breaks

## Shift Mindset

- Triage is about consistency
- Focus on progress
- Trust the process
- Lean on your team

# Live Demo

https://limacharlie.io/

https://obsidian.md/

# Rule Logic

- https://github.com/refractionPOINT/sigma-limacharlie/blob/rules/latest/windows_process_creation/proc_creation_win_powershell_non_interactive_execution.yml
- https://github.com/refractionPOINT/sigma-limacharlie/blob/rules/latest/windows_process_creation/proc_creation_win_powershell_encode.yml
- https://github.com/refractionPOINT/sigma-limacharlie/blob/rules/latest/windows_process_creation/proc_creation_win_powershell_base64_encoded_cmd.yml

https://limacharlie.io/

# Thank You

for Your Time and Attention

Present by Tom DeJong

tdejong@blackhillsinfosec.com
www.linkedin.com/in/dejongtom