Diamond in the SIEM

Improving the building blocks of Security Event Monitoring

PatH, CSides Monthly, 2022

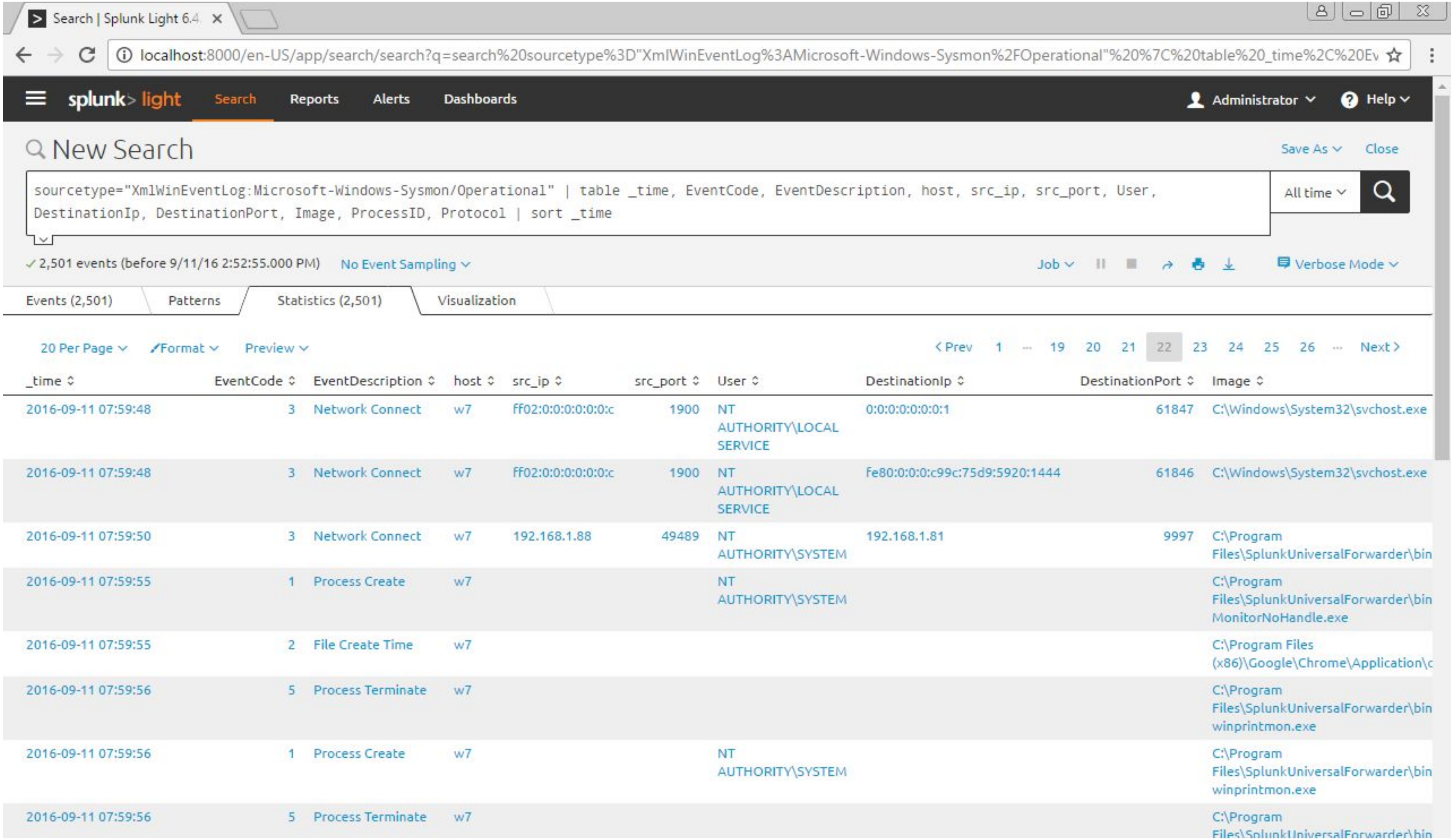
(otherwise known as)

The dumbest idea I ever had

PatH, CSides Monthly, 2022

Background

- Week of PTO
- Apocalypse cancelled planned events
- Kiddo at daycare, dog asleep
- Boredom
- Can I improve my Security Information and Event Monitoring experience (SIEM)?


Search | Splunk Light 6.4
localhost:8000/en-US/app/search/search?q=search%20sourcetype%3D"XmlWinEventLog%3AMicrosoft-Windows-Sysmon%2FOperational"%20%7C%20table%20_time%2C%20Ev
splunk> light
Search
Reports
Alerts
Dashboards
Administrator
Help
New Search
Save As
Close
All time
Job
Verbose Mode
Events (2,501)
Patterns
Statistics (2,501)
Visualization
20 Per Page
Format
Preview
‹ Prev 1 ... 19 20 21 22 23 24 25 26 ... Next ›

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" | table _time, EventCode, EventDescription, host, src_ip, src_port, User,
DestinationIp, DestinationPort, Image, ProcessID, Protocol | sort _time
```

✓ 2,501 events (before 9/11/16 2:52:55.000 PM) No Event Sampling

_time	EventCode	EventDescription	host	src_ip	src_port	User	DestinationIp	DestinationPort	Image
2016-09-11 07:59:48	3	Network Connect	w7	ff02:0:0:0:0:0:0:c	1900	NT AUTHORITY\LOCAL SERVICE	0:0:0:0:0:0:0:1	61847	C:\Windows\System32\svchost.exe
2016-09-11 07:59:48	3	Network Connect	w7	ff02:0:0:0:0:0:0:c	1900	NT AUTHORITY\LOCAL SERVICE	fe80:0:0:0:c99c:75d9:5920:1444	61846	C:\Windows\System32\svchost.exe
2016-09-11 07:59:50	3	Network Connect	w7	192.168.1.88	49489	NT AUTHORITY\SYSTEM	192.168.1.81	9997	C:\Program Files\SplunkUniversalForwarder\bin
2016-09-11 07:59:55	1	Process Create	w7			NT AUTHORITY\SYSTEM			C:\Program Files\SplunkUniversalForwarder\bin MonitorNoHandle.exe
2016-09-11 07:59:55	2	File Create Time	w7						C:\Program Files (x86)\Google\Chrome\Application\c
2016-09-11 07:59:56	5	Process Terminate	w7						C:\Program Files\SplunkUniversalForwarder\bin winprintmon.exe
2016-09-11 07:59:56	1	Process Create	w7			NT AUTHORITY\SYSTEM			C:\Program Files\SplunkUniversalForwarder\bin winprintmon.exe
2016-09-11 07:59:56	5	Process Terminate	w7						C:\Program Files\SplunkUniversalForwarder\bin

Project Requirements

Unix ELF parasites and virus

Silvio Cesare
October 1998

3 [Back to index] [Comments]

Introduction

This paper documents the algorithms and i
virus for Linux on x86 architecture is also s

1. Collect raw events
   - Windows only, CEOs don’t use Linux
   - *Stretch goal: Across an entire domain*

2. Generate detections based on events
   - Don’t flood UI with raw events

3. Display detections to the user
   - At-a-glance detection severity and event information
   - *Stretch goal: Multi-user*

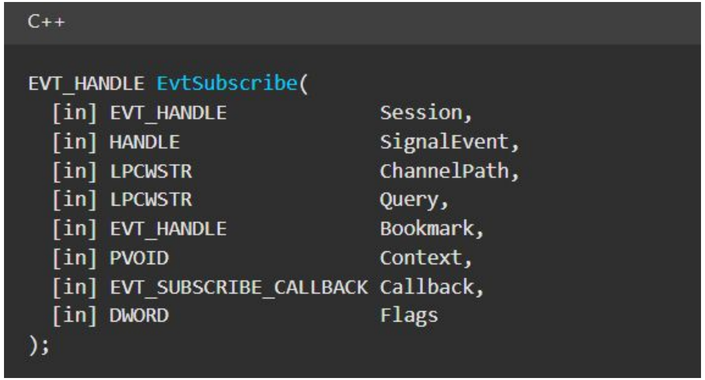
4. Allow action to be taken by user:
   - e.g. Kill process

1. Collect raw events

- Tired: Use Sysmon
- Wired: Write our own agent

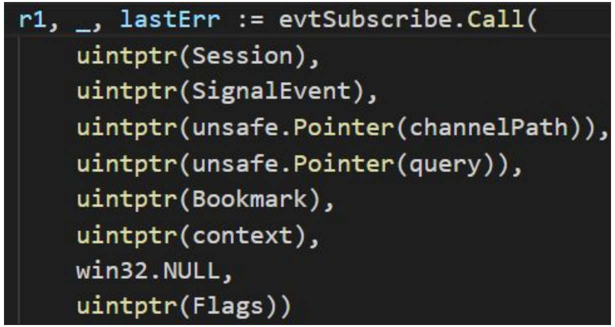
- Oops, already did that (sorta not really)
  - Sealighter research tracer
  - Uses ETW under the hood
  - E.g. get ETW Kernel Process Creation events

1. Collect raw events



C++

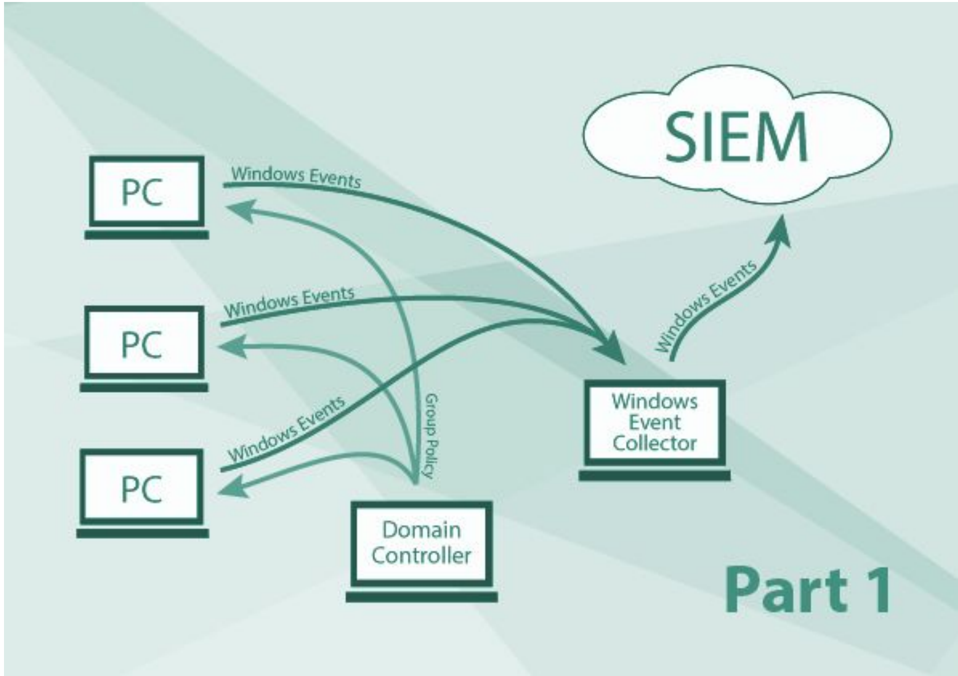
```cpp
EVT_HANDLE EvtSubscribe(
  [in] EVT_HANDLE             Session,
  [in] HANDLE                 SignalEvent,
  [in] LPCWSTR                ChannelPath,
  [in] LPCWSTR                Query,
  [in] EVT_HANDLE             Bookmark,
  [in] PVOID                  Context,
  [in] EVT_SUBSCRIBE_CALLBACK Callback,
  [in] DWORD                  Flags
);
```



```go
r1, _, lastErr := evtSubscribe.Call(
    uintptr(Session),
    uintptr(SignalEvent),
    uintptr(unsafe.Pointer(channelPath)),
    uintptr(unsafe.Pointer(query)),
    uintptr(Bookmark),
    uintptr(context),
    win32.NULL,
    uintptr(Flags))
```

- Sysmon and Sealighter publish events to a Windows Event Log
- Reading Event log off disk not ideal
  - Caching issues
- Better: Wevtapi.dll -> EvtSubscribe()
  - https://docs.microsoft.com/en-us/windows/win32/api/winevt/nf-winevt-evtsubscribe
  - EvtSubscribeToFutureEvents
- Existing Go Library from 0xrawsec:
  - https://github.com/0xrawsec/golang-win32
  - Events Converted to String Maps (i.e. Dictionaries)

1. Collect raw events - Entire Domain

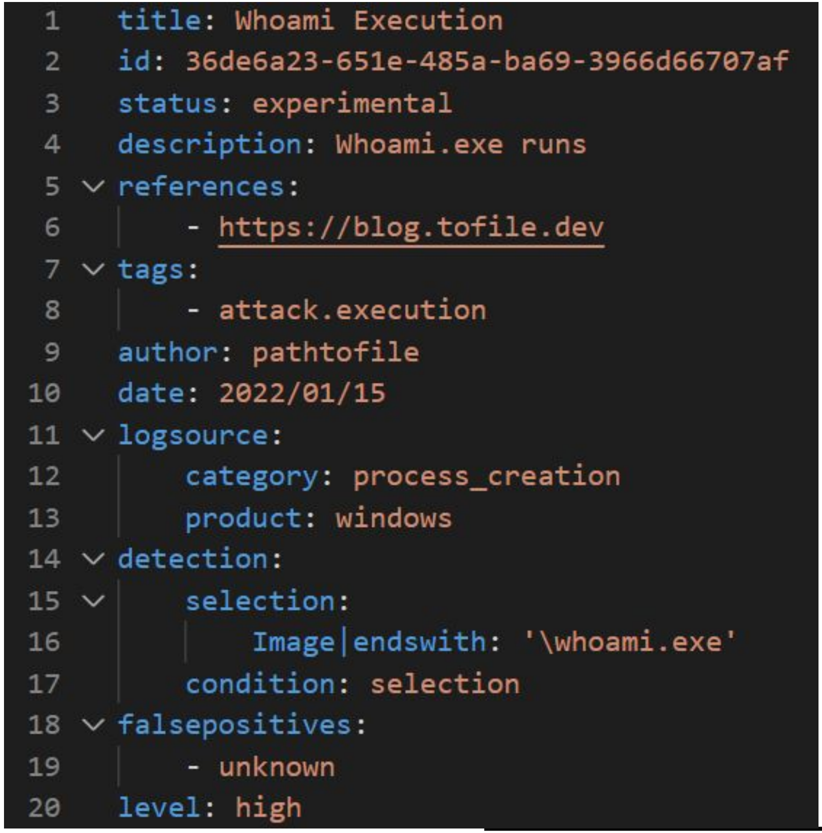


- Could call EvtOpenSession() on every PC or...

- Can use Windows Event Forwarding (WEF)
- Built into Windows
- Events end up in a single Event Log Channel on 1 PC

- SIEMCRAFT on WEF PC == Entire domain

2. Generate Detections



```yaml
title: Whoami Execution
id: 36de6a23-651e-485a-ba69-3966d66707af
status: experimental
description: Whoami.exe runs
references:
    - https://blog.tofile.dev
tags:
    - attack.execution
author: pathtofile
date: 2022/01/15
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith: '\whoami.exe'
    condition: selection
falsepositives:
    - unknown
level: high
```

- Raw events too noisy
    - What am I, a SOC?
- Use industry Standard Detection Schema - SIGMA
    - https://github.com/SigmaHQ/sigma
    - YAML 'Rule' detailing what a detection looks like
        - Unique ID
        - Name
        - Event severity
        - Process CommandLines, Filenames, etc
    - System-agnostic
        - No specific to specific EDR or SIEM
    - Repo has 100s of premade SIGMA Rules
- Go Library: sigma-go
    - https://github.com/bradleyjkemp/sigma-go
    - Takes in a String Map, returns True / False
- Some integration issues:
    - Issues in parsing certain rule types
    - Needed to run the right events against the right rules
        - e.g. Process Events against only Process Rules

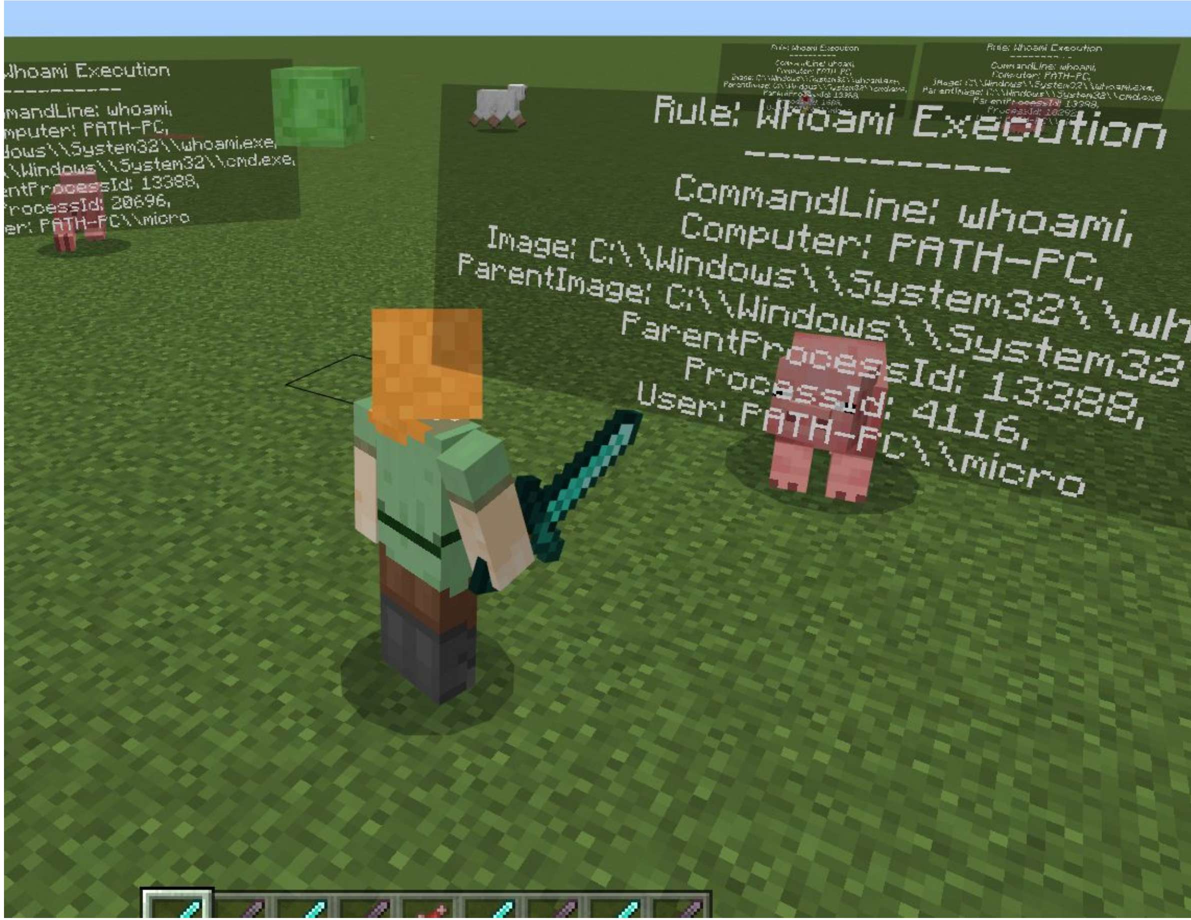
3. Send detections to User

- Now for the User Experience
- Visualise detections in a way never seen before
  - Break the mold of plain textual data
- Remember our stretch goal - Multi-user
  - multi-*player???*

SIEMCRAFT

Security Information and Event Management (SIEM)

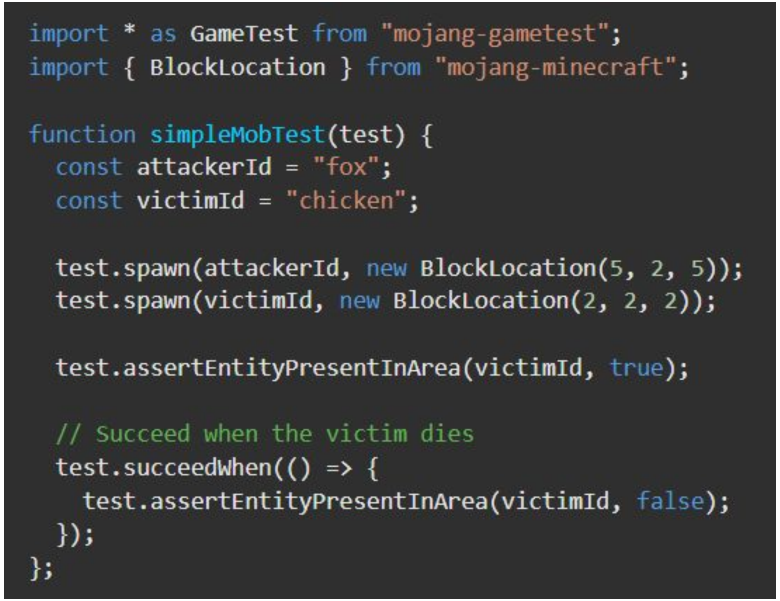
in Minecraft



```
Rule: Whoami Execution
-----------
CommandLine: whoami,
Computer: PATH-PC,
Image: C:\\Windows\\System32\\wh
ParentImage: C:\\Windows\\System32
ParentProcessId: 13388,
ProcessId: 4116,
User: PATH-PC\\micro
```

```
hoami Execution
----------
mandLine: whoami,
mputer: PATH-PC,
dows\\System32\\whoami.exe,
\\Windows\\System32\\cmd.exe,
ntProcessId: 13388,
rocessId: 20696,
er: PATH-PC\\micro
```

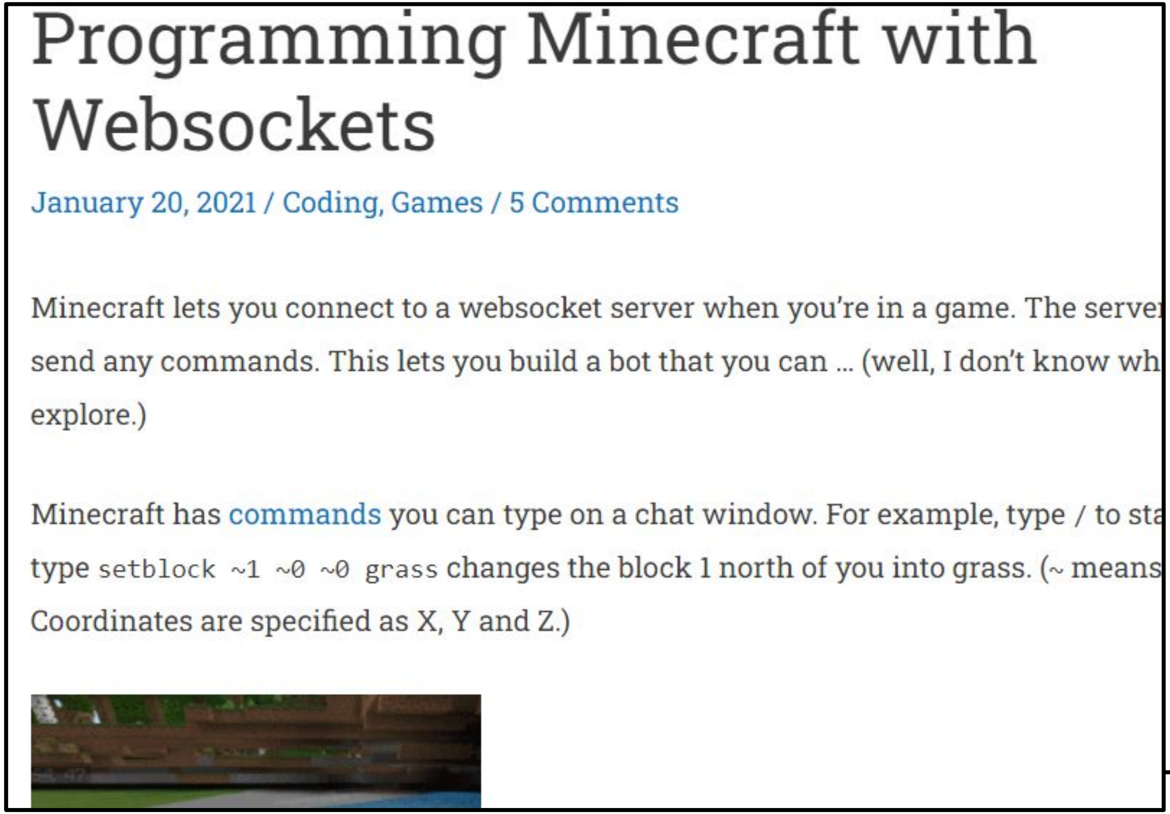
3. Send detections to MineCraft



```
import * as GameTest from "mojang-gametest";
import { BlockLocation } from "mojang-minecraft";

function simpleMobTest(test) {
  const attackerId = "fox";
  const victimId = "chicken";

  test.spawn(attackerId, new BlockLocation(5, 2, 5));
  test.spawn(victimId, new BlockLocation(2, 2, 2));

  test.assertEntityPresentInArea(victimId, true);

  // Succeed when the victim dies
  test.succeedWhen(() => {
    test.assertEntityPresentInArea(victimId, false);
  });
};
```

- MineCraft Bedrock
  - C++, Modern version of Minecraft
  - Java is gross
- No Mods, but “addons”
  - Lots of JSON to define new Animals and things
  - Super restricted Javascript ‘Game Test’ engine
    - I’m not cool enough for typescript
  - No ability to do things outside minecraft
- Could instead run custom server
  - Arbitrary code from server
  - But wouldn’t be able to handle other Addons
- Anything else?

Websockets!



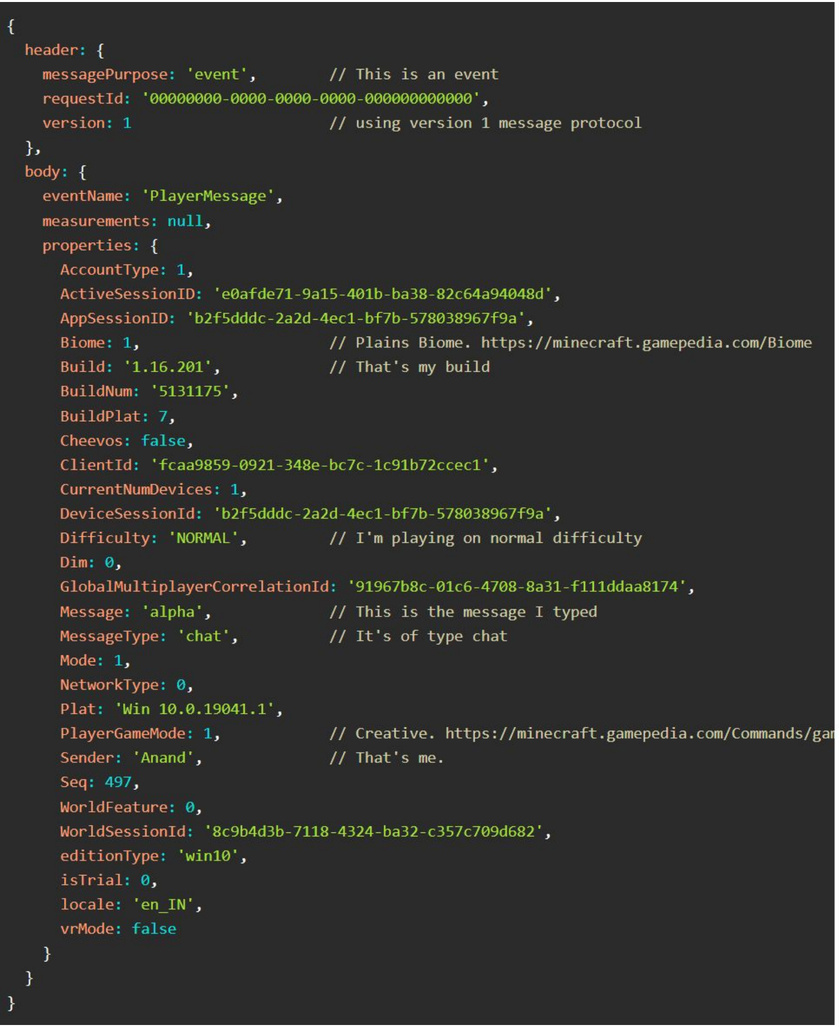
Programming Minecraft with Websockets

January 20, 2021 / Coding, Games / 5 Comments

Minecraft lets you connect to a websocket server when you're in a game. The serve
send any commands. This lets you build a bot that you can … (well, I don't know wh
explore.)

Minecraft has commands you can type on a chat window. For example, type / to sta
type `setblock ~1 ~0 ~0 grass` changes the block 1 north of you into grass. (~ means
Coordinates are specified as X, Y and Z.)

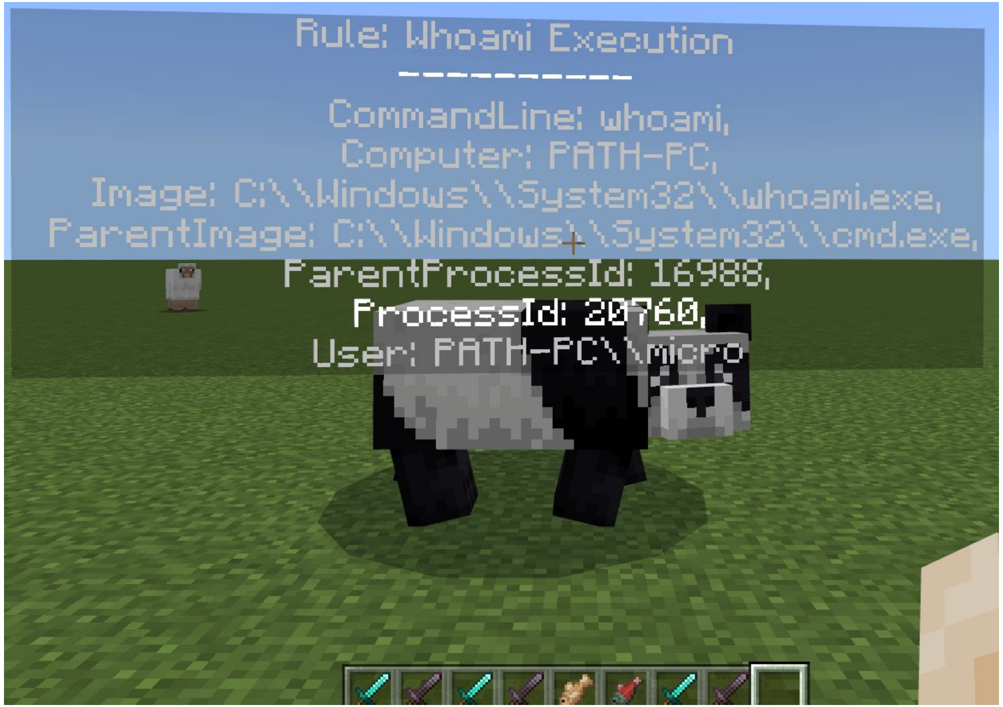
WebSockets!



```
{
  header: {
    messagePurpose: 'event',        // This is an event
    requestId: '00000000-0000-0000-0000-000000000000',
    version: 1                      // using version 1 message protocol
  },
  body: {
    eventName: 'PlayerMessage',
    measurements: null,
    properties: {
      AccountType: 1,
      ActiveSessionID: 'e0afde71-9a15-401b-ba38-82c64a94048d',
      AppSessionID: 'b2f5dddc-2a2d-4ec1-bf7b-578038967f9a',
      Biome: 1,                     // Plains Biome. https://minecraft.gamepedia.com/Biome
      Build: '1.16.201',            // That's my build
      BuildNum: '5131175',
      BuildPlat: 7,
      Cheevos: false,
      ClientId: 'fcaa9859-0921-348e-bc7c-1c91b72ccec1',
      CurrentNumDevices: 1,
      DeviceSessionId: 'b2f5dddc-2a2d-4ec1-bf7b-578038967f9a',
      Difficulty: 'NORMAL',         // I'm playing on normal difficulty
      Dim: 0,
      GlobalMultiplayerCorrelationId: '91967b8c-01c6-4708-8a31-f111ddaa8174',
      Message: 'alpha',             // This is the message I typed
      MessageType: 'chat',          // It's of type chat
      Mode: 1,
      NetworkType: 0,
      Plat: 'Win 10.0.19041.1',
      PlayerGameMode: 1,            // Creative. https://minecraft.gamepedia.com/Commands/gam
      Sender: 'Anand',              // That's me.
      Seq: 497,
      WorldFeature: 0,
      WorldSessionId: '8c9b4d3b-7118-4324-ba32-c357c709d682',
      editionType: 'win10',
      isTrial: 0,
      locale: 'en_IN',
      vrMode: false
    }
  }
}
```

- Created for “Minecraft Educational Edition”
- JSON Protocol
- Can receive and send events
- Receive events:
  - Player Message
  - Block Placed
  - Mob Killed
  - …
- Send Events:
  - Command Request

3. Send detections to MineCraft

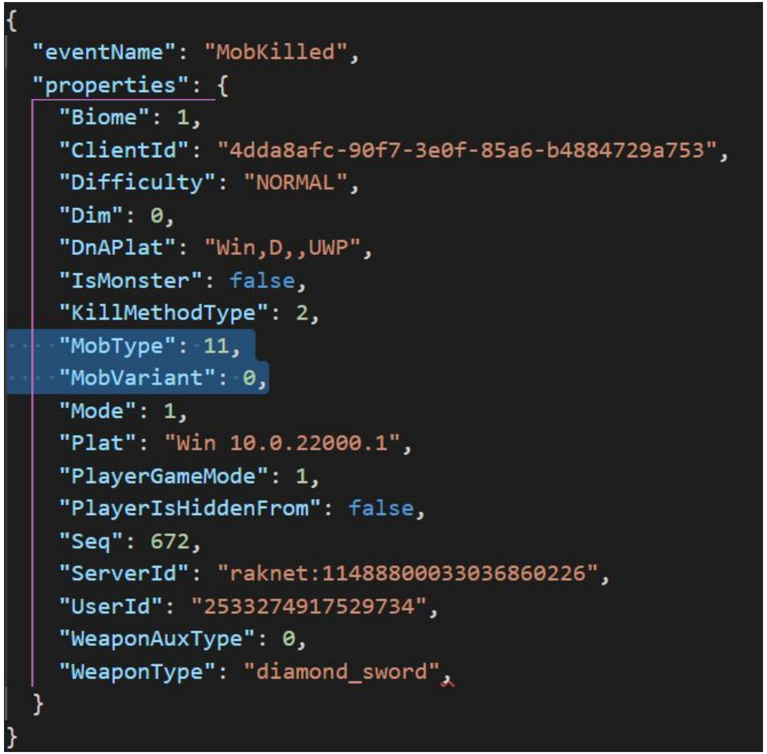


```
Rule: Whoami Execution
------------
CommandLine: whoami,
Computer: PATH-PC,
Image: C:\\Windows\\System32\\whoami.exe,
ParentImage: C:\\Windows\\System32\\cmd.exe,
ParentProcessId: 16988,
ProcessId: 20760,
User: PATH-PC\\micro
```

- Run SIEMCraft in a separate process
- Send command: Create Entity
  - `/summon cow`
  - Different animal for different event severities
    - Low: Chicken, cow
    - High: Spider, Panda, Bear
  - Set animal ‘name’ to be event details

- Needed some Addon magic
  - Make names always visible
  - Create non-polar bears
  - Make animals aggressive

4. Allow action to be taken by user



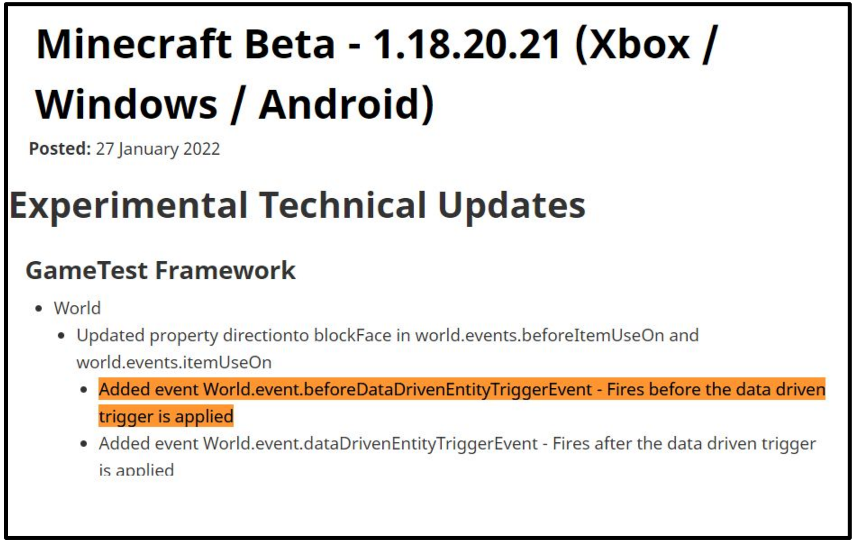
```
{
  "eventName": "MobKilled",
  "properties": {
    "Biome": 1,
    "ClientId": "4dda8afc-90f7-3e0f-85a6-b4884729a753",
    "Difficulty": "NORMAL",
    "Dim": 0,
    "DnAPlat": "Win,D,,UWP",
    "IsMonster": false,
    "KillMethodType": 2,
    "MobType": 11,
    "MobVariant": 0,
    "Mode": 1,
    "Plat": "Win 10.0.22000.1",
    "PlayerGameMode": 1,
    "PlayerIsHiddenFrom": false,
    "Seq": 672,
    "ServerId": "raknet:11488800033036860226",
    "UserId": "2533274917529734",
    "WeaponAuxType": 0,
    "WeaponType": "diamond_sword",
  }
}
```

- Animal killed by diamond sword?
  kill process (or parent process)

- Can’t do it from Minecraft Addon
  - Need to use external websocket

- Subscribe to “MobKilled” event?
  - Missing Mob Name 😿
  - Need name for process id
- No other useful killed/death/despawn events
  - But we do have ‘PlayerMesssage’...

4. Allow action to be taken by user



Minecraft Beta - 1.18.20.21 (Xbox / Windows / Android)

Posted: 27 January 2022

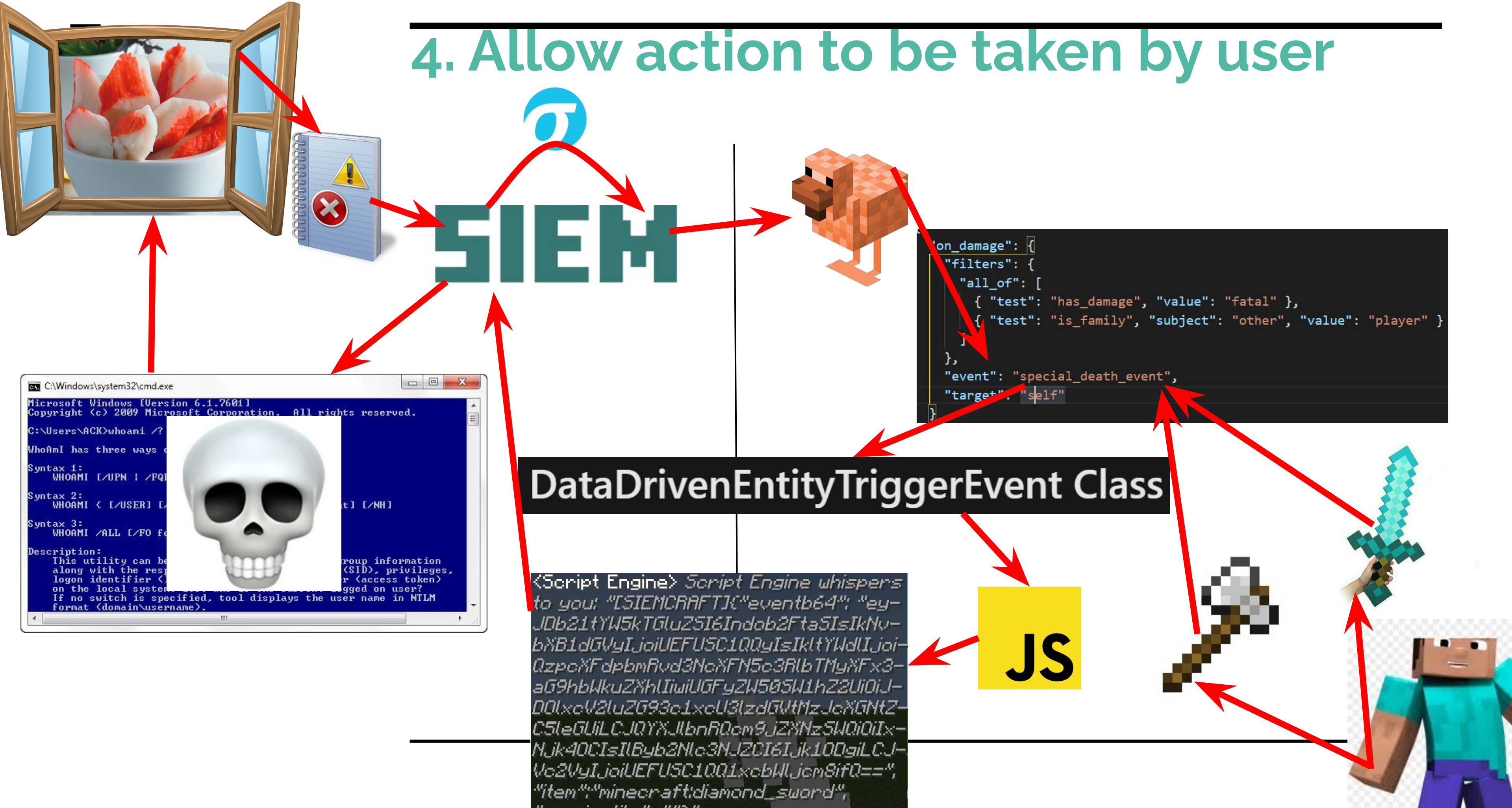
Experimental Technical Updates

GameTest Framework

- World
  - Updated property directionto blockFace in world.events.beforeItemUseOn and world.events.itemUseOn
    - Added event World.event.beforeDataDrivenEntityTriggerEvent - Fires before the data driven trigger is applied
    - Added event World.event.dataDrivenEntityTriggerEvent - Fires after the data driven trigger is applied

- New GameTest Feature - Event Triggers
  - E.g. “turn into pig-zombie”
  - Calls Javascript code when an ‘event’ occurs
- Javascript can run commands
  - Including '/say’
- /say from Javascript fires PlayerMessage websocket event
- No event fires on regular animal death
  - But Addons can create their own animals and events!

4. Allow action to be taken by user



SIEM
C:\Windows\system32\cmd.exe
DataDrivenEntityTriggerEvent Class
JS

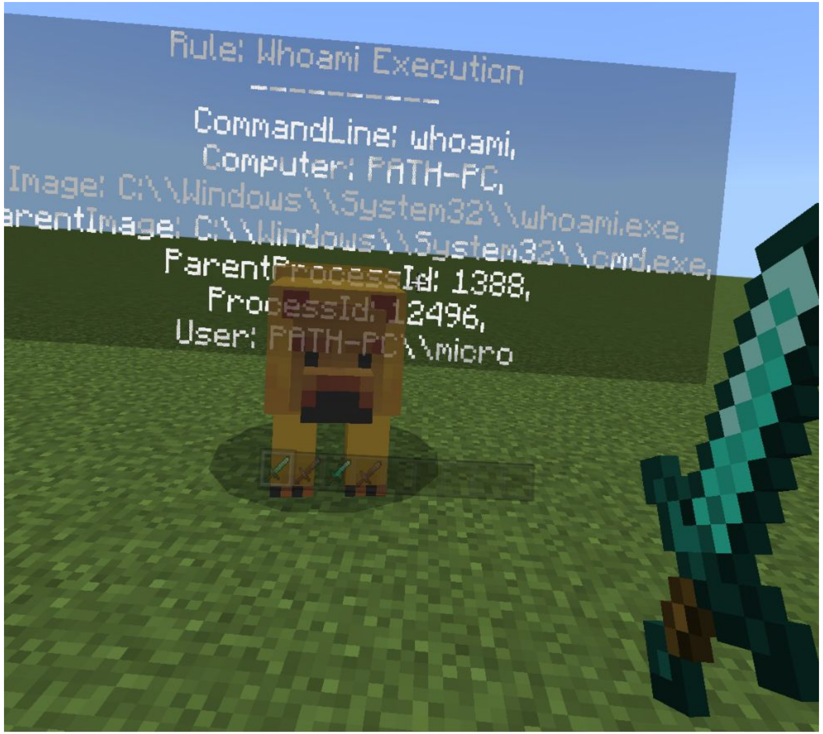
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\ACK>whoami /?

WhoAmI has three ways o

Syntax 1:
    WHOAMI [/UPN | /FQD

Syntax 2:
    WHOAMI { [/USER] [/                          t] [/NH]

Syntax 3:
    WHOAMI /ALL [/FO fo

Description:
    This utility can be                          roup information
    along with the resp                          (SID), privileges,
    logon identifier (L                          r (access token)
    on the local system                          ogged on user?
    If no switch is specified, tool displays the user name in NTLM
    format (domain\username).
```

```
"on_damage": {
  "filters": {
    "all_of": [
      { "test": "has_damage", "value": "fatal" },
      { "test": "is_family", "subject": "other", "value": "player" }
    ]
  },
  "event": "special_death_event",
  "target": "self"
}
```

```
<Script Engine> Script Engine whispers
to you: "[SIEMCRAFT]{"eventb64": "ey-
JDb21tYW5kTGluZSI6Indob2FtaSIsIkNv-
bXB1dGVyIjoiUEFUSC1QQyIsIkltYWdlIjoi-
QzpcXFdpbmRvd3NcXFN5c3RlbTMyXFx3-
aG9hbWkuZXhlIiwiUGFyZW50SW1hZ2UiOiJ-
DOlxcV2luZG93c1xcU3lzdGVtMzJcXGNtZ-
C5leGUiLCJQYXJlbnRQcm9jZXNzSWQiOiIx-
NJk4OCIsIlByb2Nlc3NJZCI6IJk1ODgiLCJ-
Vc2VyIjoiUEFUSC1QQ1xcbWljcm8ifQ==",
"item":"minecraft:diamond_sword",
```

Demo

Wrap Up



```
Rule: Whoami Execution
-----------
CommandLine: whoami,
Computer: PATH-PC,
Image: C:\\Windows\\System32\\whoami.exe,
arentImage: C:\\Windows\\System32\\cmd.exe,
ParentProcessId: 1388,
ProcessId: 12496,
User: PATH-PC\\micro
```

(Works in VR also!)

- Worth it?
  - Eh, sure
- Code, slides, etc.:
  - https://github.com/pathtofile/siemcraft
- Questions / life evaluations
  - https://blog.tofile.dev
  - Twitter: @pathtofile
  - Email: path@tofile[.]dev
- Thanks to:
  - RawSec for Go-Win32
  - SigmaHQ and Florian Roth for Sigma
  - Bradley Kemp for Sigma-Go
  - Minecraft API Devs and Writers
  - InfoSect for hosting CSides