Non-stop Ports Scanning

The Temporal Advantage

Temporal Meetup Paris - October 19, 2023

👤 Whoami

Guillaume GRANJUS

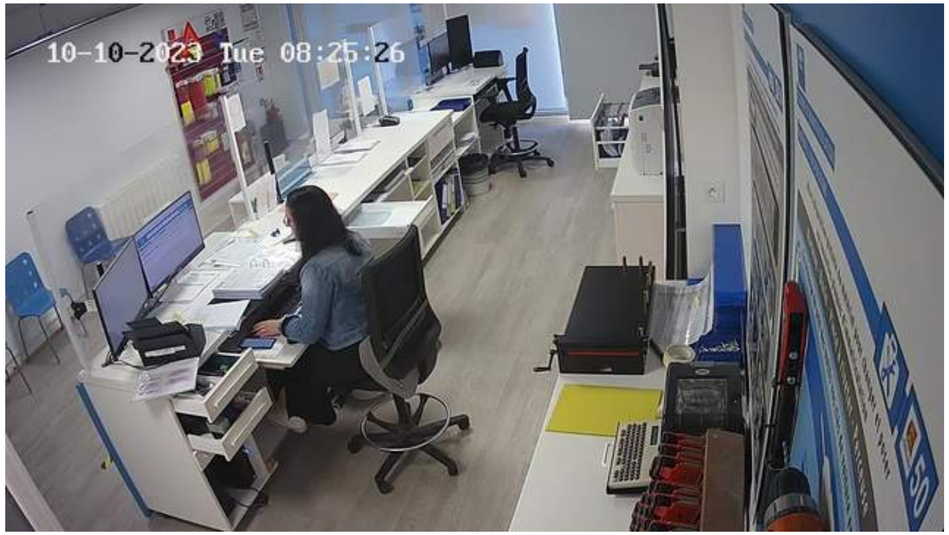
Squad Leader at Intrinsec, a cybersecurity company

(Product & Engineering Manager)

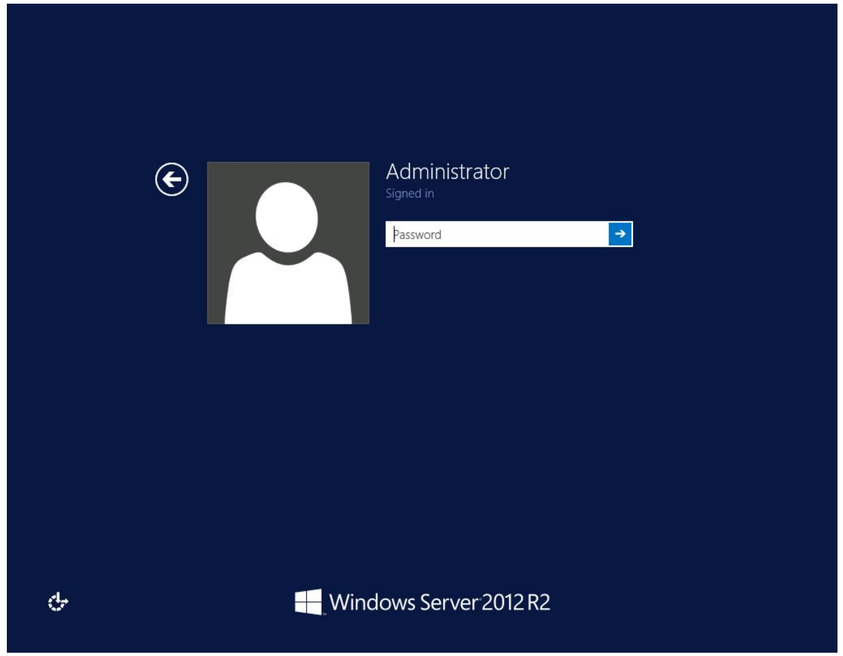
🕵️ Cyber Threat Intelligence

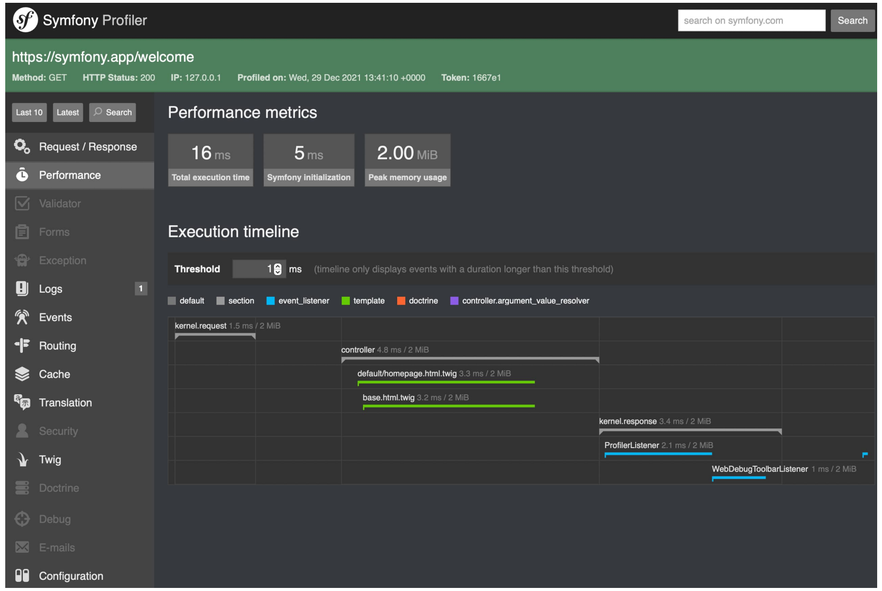
- Dataleak Detection
- Brand Protection
- Risk Anticipation
- **External Attack Surface Management**

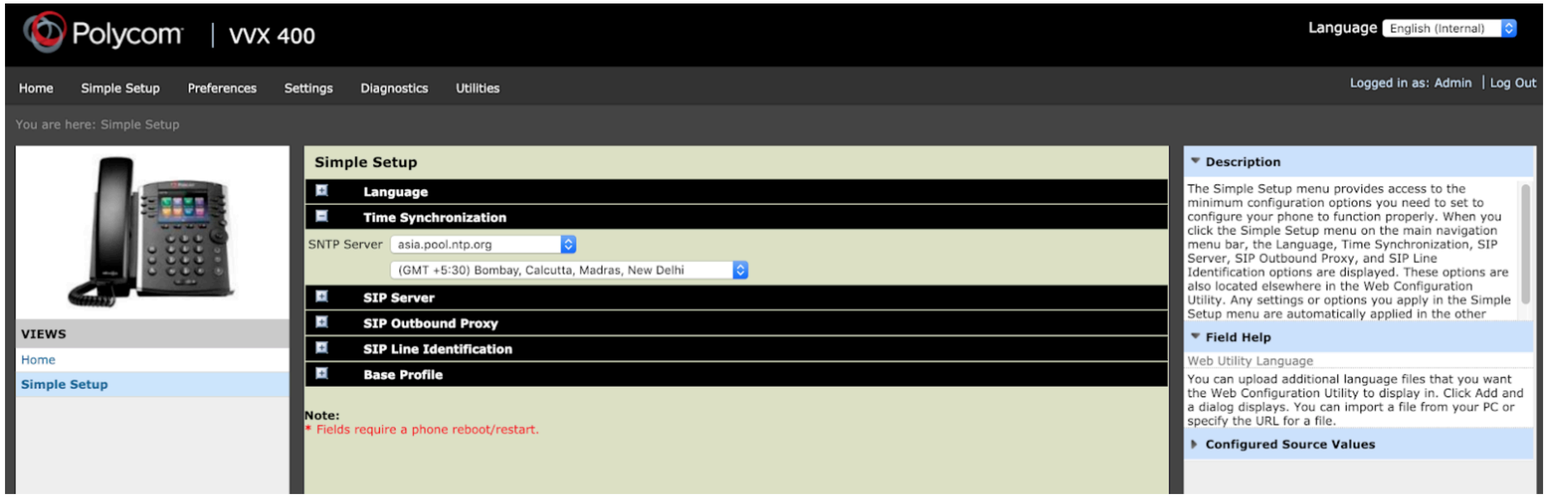
Examples


10-10-2023 Tue 08:25:26


phpMyAdmin
Welcome to phpMyAdmin
Language
English
Log in
Server:
Username:
Password:
Log in

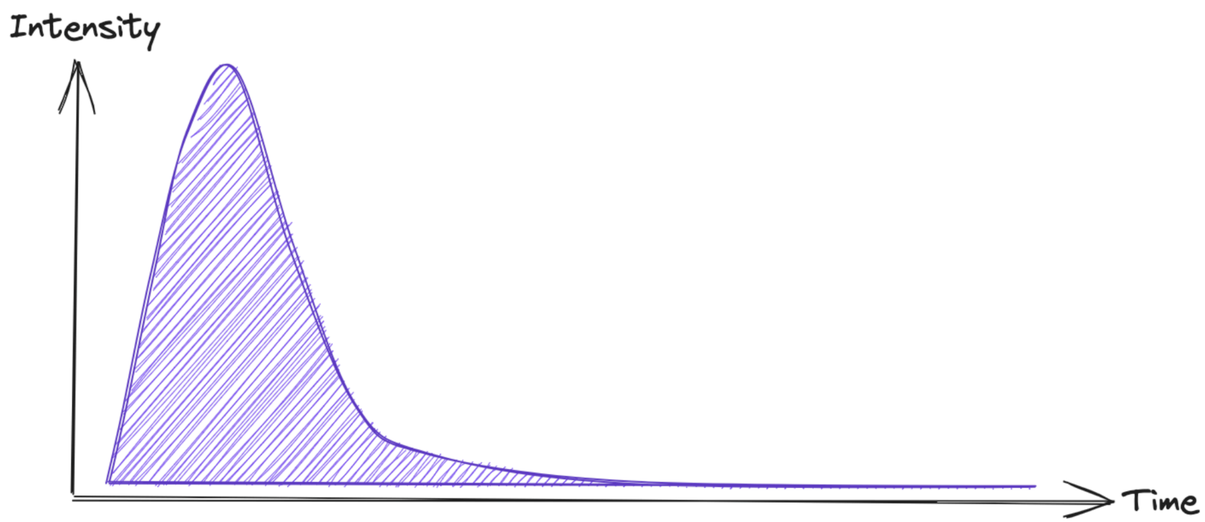

Administrator
Signed in
Password
Windows Server 2012 R2


Symfony Profiler
search on symfony.com
Search
https://symfony.app/welcome
Method: GET HTTP Status: 200 IP: 127.0.0.1 Profiled on: Wed, 29 Dec 2021 13:41:10 +0000 Token: 1667e1
Performance metrics
16 ms
Total execution time
5 ms
Symfony initialization
2.00 MiB
Peak memory usage
Execution timeline
Request / Response
Performance
Validator
Forms
Exception
Logs
Events
Routing
Cache
Translation
Security
Twig
Doctrine
Debug
E-mails
Configuration


Polycom | VVX 400
Language English (Internal)
Home
Simple Setup
Preferences
Settings
Diagnostics
Utilities
Logged in as: Admin | Log Out
You are here: Simple Setup
VIEWS
Home
Simple Setup
Simple Setup
Language
Time Synchronization
SNTP Server asia.pool.ntp.org
(GMT +5:30) Bombay, Calcutta, Madras, New Delhi
SIP Server
SIP Outbound Proxy
SIP Line Identification
Base Profile
Note:
* Fields require a phone reboot/restart.
Description
The Simple Setup menu provides access to the minimum configuration options you need to set to configure your phone to function properly. When you click the Simple Setup menu on the main navigation menu bar, the Language, Time Synchronization, SIP Server, SIP Outbound Proxy, and SIP Line Identification options are displayed. These options are also located elsewhere in the Web Configuration Utility. Any settings or options you apply in the Simple Setup menu are automatically applied in the other
Field Help
Web Utility Language
You can upload additional language files that you want the Web Configuration Utility to display in. Click Add and a dialog displays. You can import a file from your PC or specify the URL for a file.
Configured Source Values

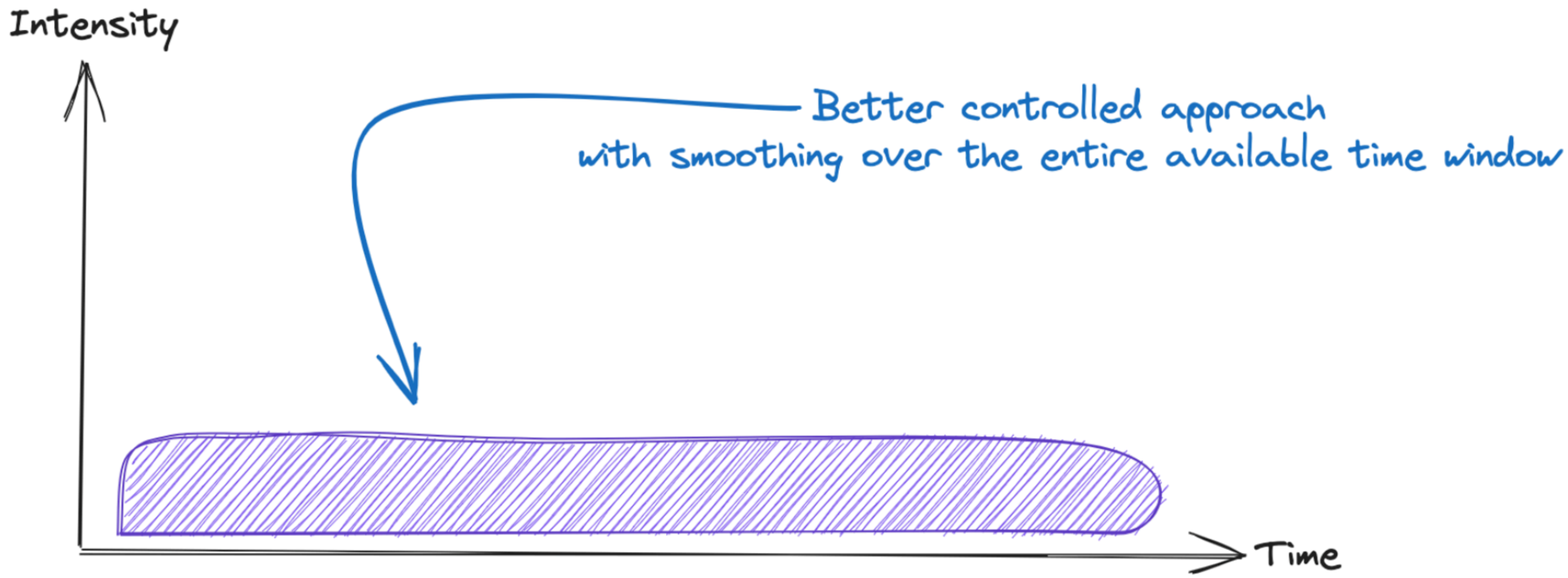
🥃 Port Scan: The Old Fashioned Way

- A scan API composed of 400 workers.
- Each customer perimeter scan is launched at “night” to avoid working hours.
- Each customer perimeter scan must last no more than 2 hours on average to be able to do it for all our customers.
- 🔥 Orchestration, planning and scan intensity issues.
- 🤷‍♂️ Our initial solution was reaching its limits



🚀 The Desired Solution

- No longer a daily perimeter scan at a fixed time, but a continuous scan of IPs all day long
- Isolated scan environments between customers



👽 The Temporal Way

- A namespace per customer.
- A schedule per IP to scan with a random offset in seconds between 00:00:00 and 23:59:59.
- A PortScan Workflow with TCPScan & UDPScan Activities.
- Number of workers related to number of IPs to scan per customer and the scan time window.

Workflow

```go
func PortScan(ctx workflow.Context, input PortScanInput) ([]Result, error) {
	logger := workflow.GetLogger(ctx)

	opts := workflow.ActivityOptions{
		StartToCloseTimeout: 5 * time.Minute,
		HeartbeatTimeout: time.Minute,
		RetryPolicy: &temporal.RetryPolicy{
			MaximumAttempts: 1,
		},
	}
	ctx := workflow.WithActivityOptions(ctx, opts)

	results := make([]Result, 0)
	var finishedScans int

	workflow.GoNamed(ctx, "TCP_Scan", func(gctx workflow.Context) {
		var tcpResults []Result
		err := workflow.ExecuteActivity(gctx, activities.TCPScan, input.Host).Get(gctx, &tcpResults)
		[...]
		results = append(results, tcpResults...)
		finishedScans += 1
	})

	workflow.GoNamed(ctx, "UDP_Scan", func(gctx workflow.Context) {
		var udpResults []Result
		err := workflow.ExecuteActivity(gctx, activities.UDPScan, input.Host).Get(gctx, &udpResults)
		[...]
		results = append(results, udpResults...)
		finishedScans += 1
	})

	workflow.Await(func() bool {
		return finishedScans == 2
	})

	[...]

	return results, nil
}
```

Activity

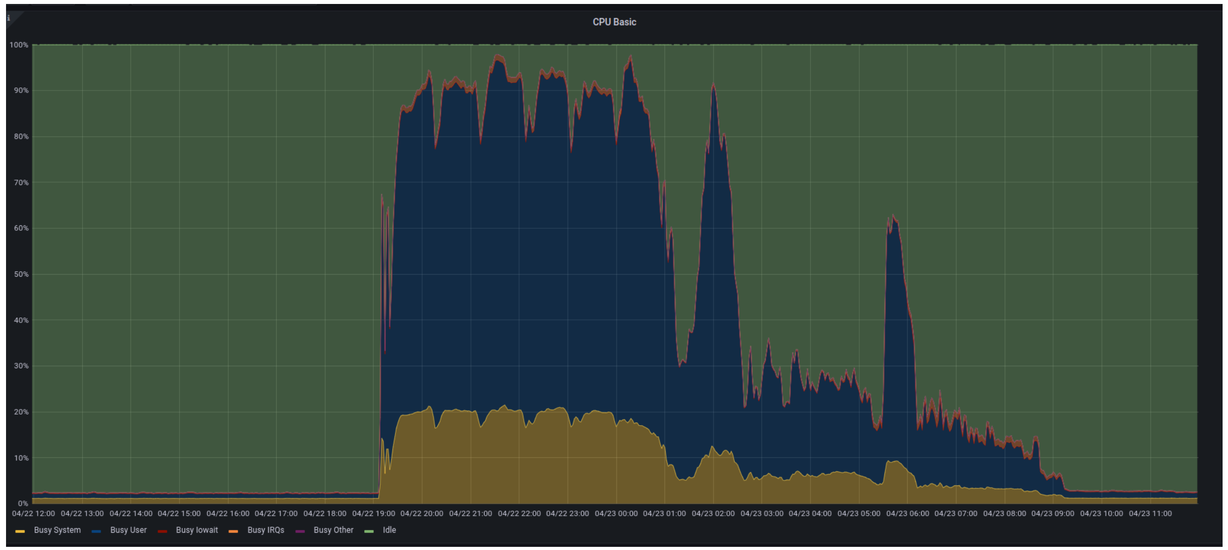
```go
func TCPScan(ctx context.Context, host string) ([]scan.Result, error) {
        logger := activity.GetLogger(ctx)

        opts := []nmap.Option{
                nmap.WithContext(ctx),
                nmap.WithTargets(host),
                [ ... ]
                nmap.WithSYNScan(),
        }

        scanner, err := nmap.NewScanner(opts ... )
        [ ... ]

        progress := make(chan float32)
        go func() {
                for p := range progress {
                        logger.Info("scan in progress", "target", host, "progress", p)
                        activity.RecordHeartbeat(ctx)
                }
        }()

        result, warnings, err := scanner.RunWithProgress(progress)
        [ ... ]
        return result, nil
}
```

https://github.com/Ullaakut/nmap

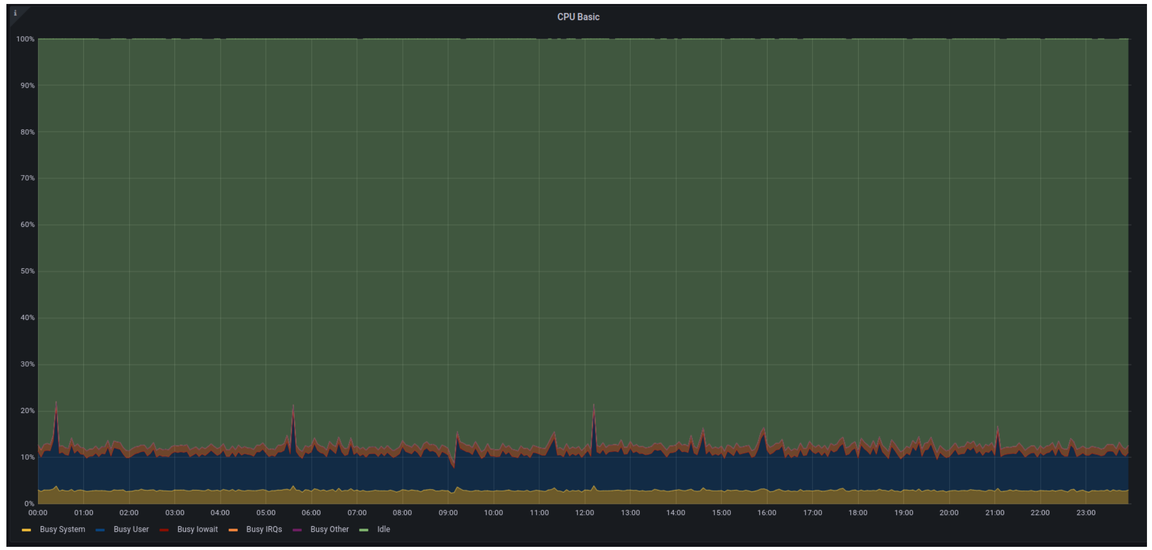
✨ Outcome

- Low and stable intensity for both customer and for us
- Predictability

CPU on a node containing our scan workers



Before



After

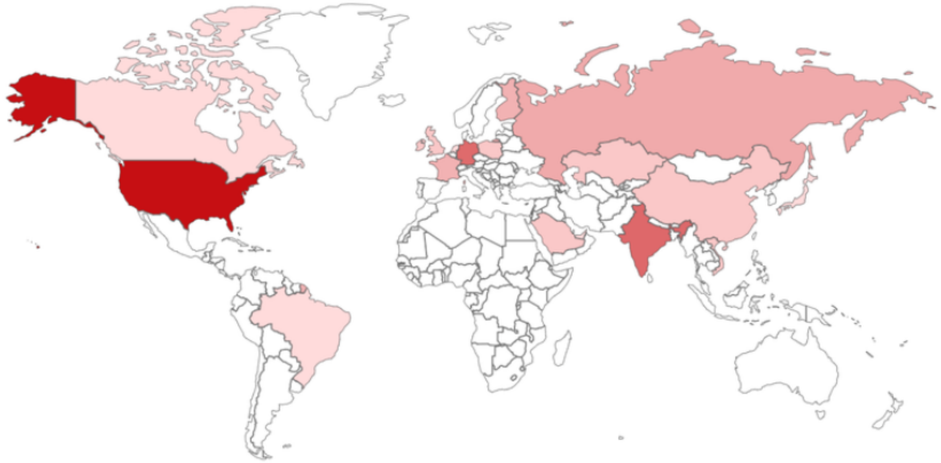
💚 Feedback On Temporal

- It matchs our need for orchestration and planning.
- 500k Workflows executed every day on a single node (12 CPU / 16 Go RAM), deployed with Docker Compose.
- Multiple languages Workflow helps onboarding.
- Documentation and tutorials are great.
- Time spent understanding how schedules work (trigger time when offset is set).
- The CLI and UI are so practical to manage the platform.

🚨 Exposed Temporal Web UIs

Shodan Report `http.favicon.hash:557327884`

// GENERAL



Countries

United States	114
India	24
Germany	23
Singapore	7
Russian Federation	5

Ports

8080	116
443	38
80	28
8082	3
7080	2

Organization

Amazon Technologies Inc.	33
Google LLC	33
Amazon Data Services NoVa	17
Amazon Data Services India	16
Microsoft Corporation	14

Vulnerabilities

No information available.

Total: 201

37 accessible without authentication

21 with visible workflows

🙈 Leaked Credentials

Input


```
{
  "webhook_id": "b4f58e3c-de3a-4fa3-96cc-02930ba445da",
  "event_id": "375ef8bf-1187-465f-aba6-2155cb7f1575",
  "application_id": "vkRMKErIgRHR",
  "client_id": "f15b8811-449f-4ff9-98bf-850714f355bd",
  "session_id": "737d2f86-4629-46c4-9ba3-8f721ab49606",
  "event_name": "liveness_check_success",
  "event_description": "",
  "webhook_url": "https://[redacted]v1/services/activityHook",
  "meta_data": {},
  "headers": {
    "x-api-key": "ijkl"
  },
  "created_at": "2023-10-16T10:03:28.414817832Z"
}
```


Input


```
{
  "source": {
    "name": "pg_src",
    "type": "POSTGRES",
    "postgresConfig": {
      "host": "[redacted].postgres.database.azure.com",
      "port": 5432,
      "user": "[redacted]",
      "password": "test123!",
      "database": "temp_src"
    }
  },
  "destination": {
    "name": "pg_dst",
    "type": "POSTGRES",
    "postgresConfig": {
[redacted]atabase.azure.com",
```


Input


```
{
  "payload": {
    "url": "https://[redacted]/automate/api/v1/customers/[redacted]",
    "method": "POST",
    "data": {
      "state": "failed",
      "status": "Workflow failed",
      "statusMessage": "Failed for action 'Get_curation_configuration_2'. Code Message - ' \n '",
      "workflowId": "Default-79278bd0-329a-4209-9ea7-c476dc0a6c84:!9b9e7353-1916-4f95-b175-fc6241064761",
      "runId": "08585042266778788944263959254CU165"
    }
  },
  "apiKey": "z64T^ZvUGzY^mvlO3jwP7",
  "eventSinkUrl": "https://[redacted]/automate/api/v1/customers/[redacted]
}
```


</> Input and Results

Input


```
{
  "email": "j.[redacted]@[redacted].de",
  "password": "123456789"
}
```

✅ Remediations

- Detect on your own with open source vulnerability scanner Nuclei and related template https://templates.nuclei.sh/public/unauth-temporal-web-ui.
- Contact Intrinsec to reduce your attack surface :-)
- Use Temporal Cloud :-)

💬 Questions