BRITTNEY ARGIRAKIS

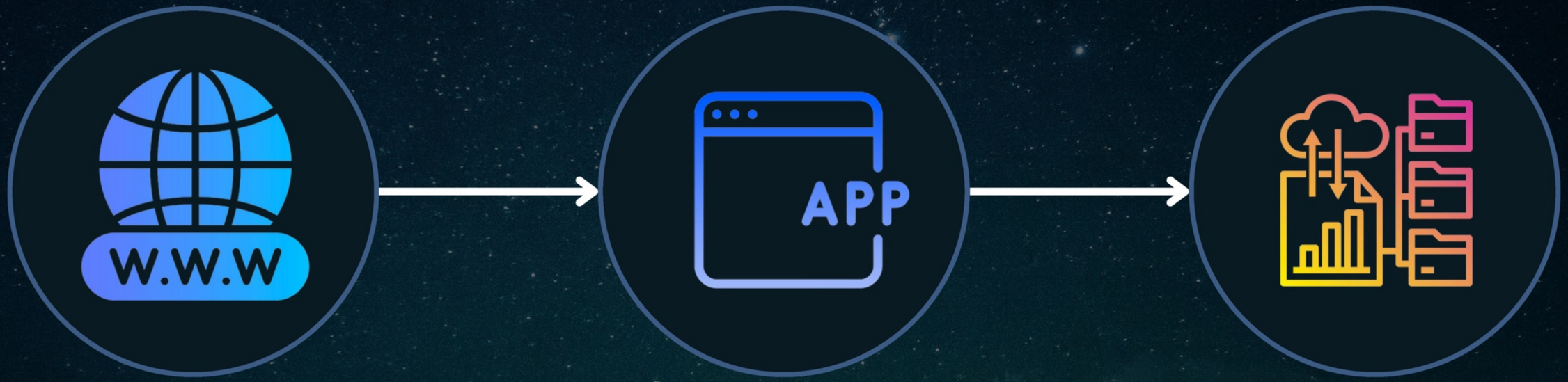
LUMINAUT

CHAPIN BRYCE

CASTING LIGHT ON SHADOW CLOUD DEPLOYMENTS

BACKGROUND

BACKGROUND



INTERNET

WEBAPP

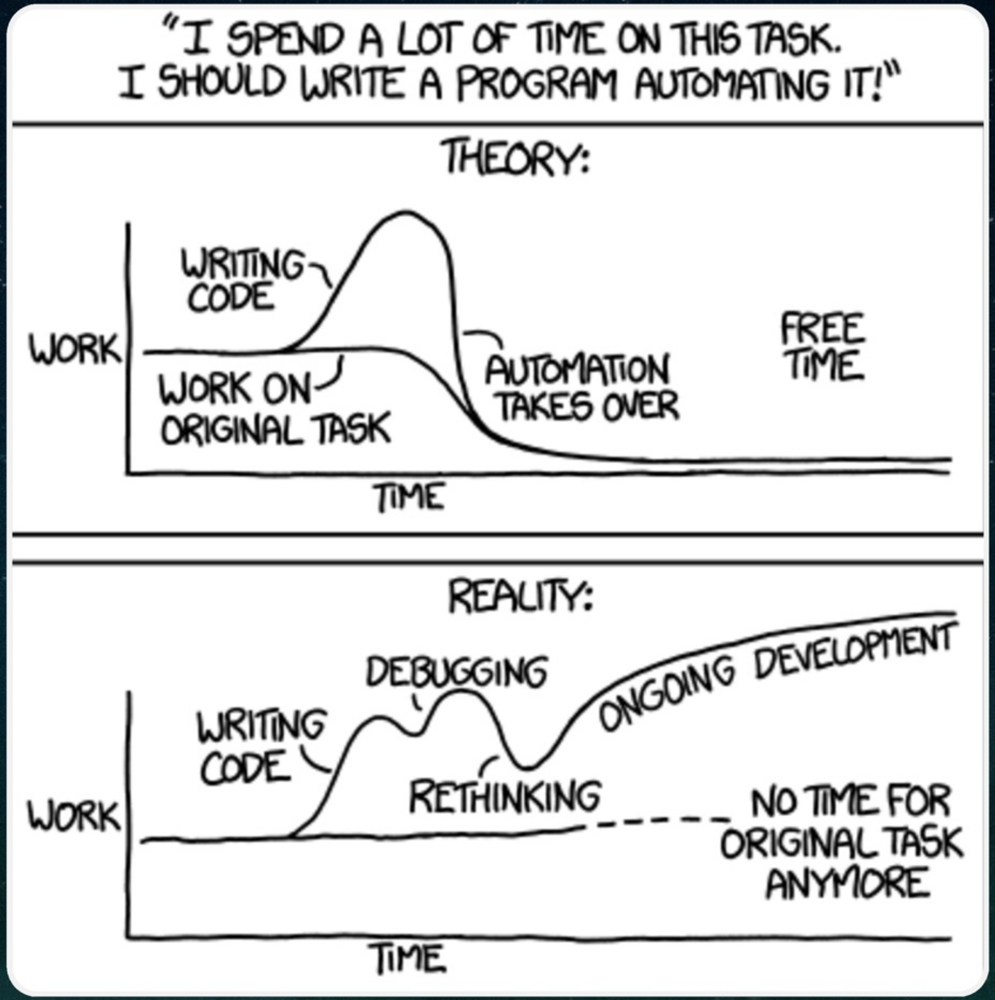
YOUR RESOURCES

BACKGROUND

BACKGROUND

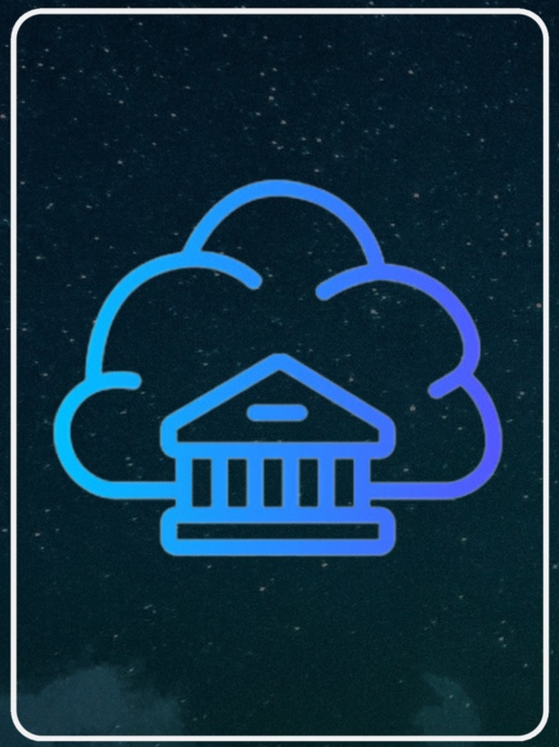
123.45.67.89

BACKGROUND



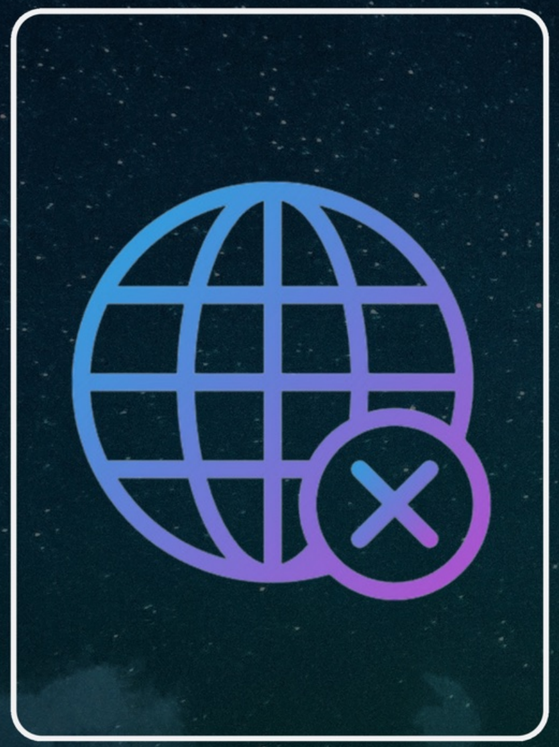
https://xkcd.com/1319/

IN THE WILD



ORGANIZATIONS WITHOUT CLOUD DISCOVERY AND GOVERNANCE ESTABLISHED

IN THE WILD



USERS CREATING THEIR OWN “OFF-THE-GRID” AWS, AZURE, GCP ACCOUNT OR INFRASTRUCTURE

WHY?

WHY?

“This is just a proof of concept”

WHY?

“This is just a proof of concept”

PoC’s turned production

WHY?

“Don’t worry, It’s just test data”

WHY?

“Yeah, It’s a clone of Prod -- but it’s in our Dev account”

WHY?

“Yeah, It’s a clone of Prod -- but it’s in our Dev account”

- Exposed wider than intended
- Today’s forgotten instances turn into tomorrow’s initial access points

WHY?

“I wasn’t supposed to create a new cloud account?”

WHY?

“I didn’t know it needed a security review”

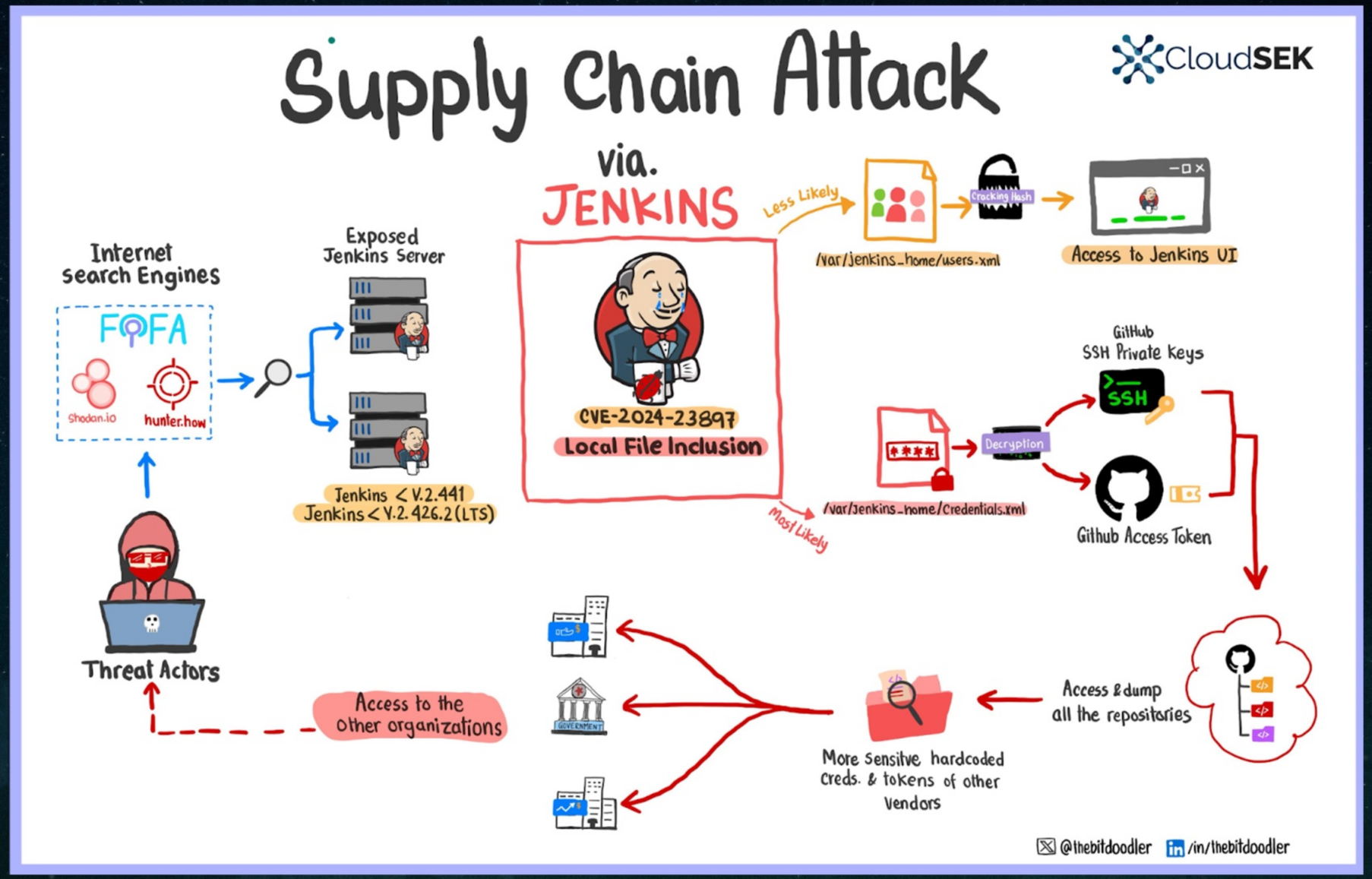
WHY?

“I didn’t know it needed a security review”

Ad hoc resources, which may not leverage usual deployment processes

RANSOMXX & INTELBROKER

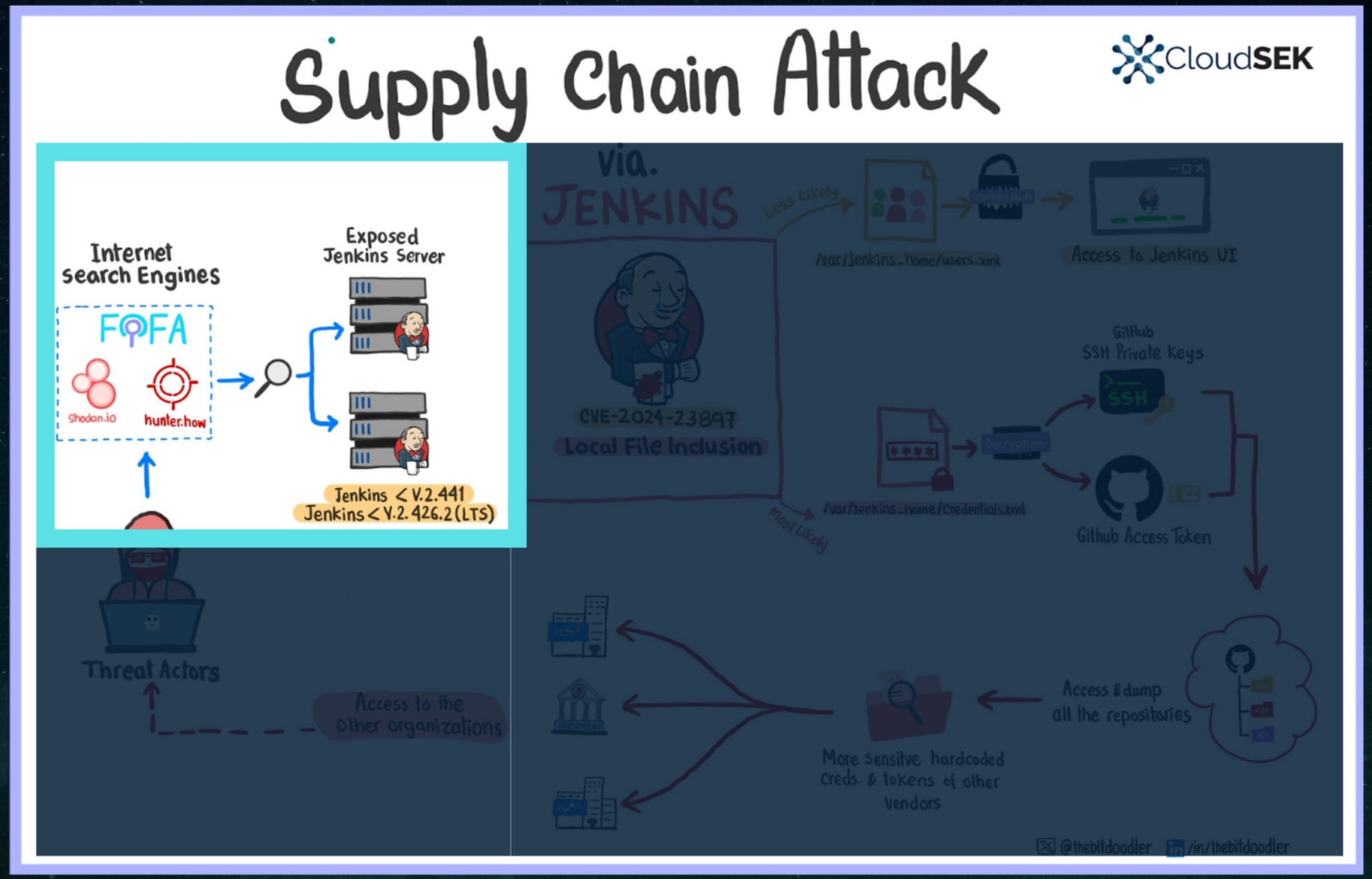
Your paragraph text



source: https://www.cloudsek.com/blog/major-payment-disruption-ransomware-strikes-indian-banking-infrastructure

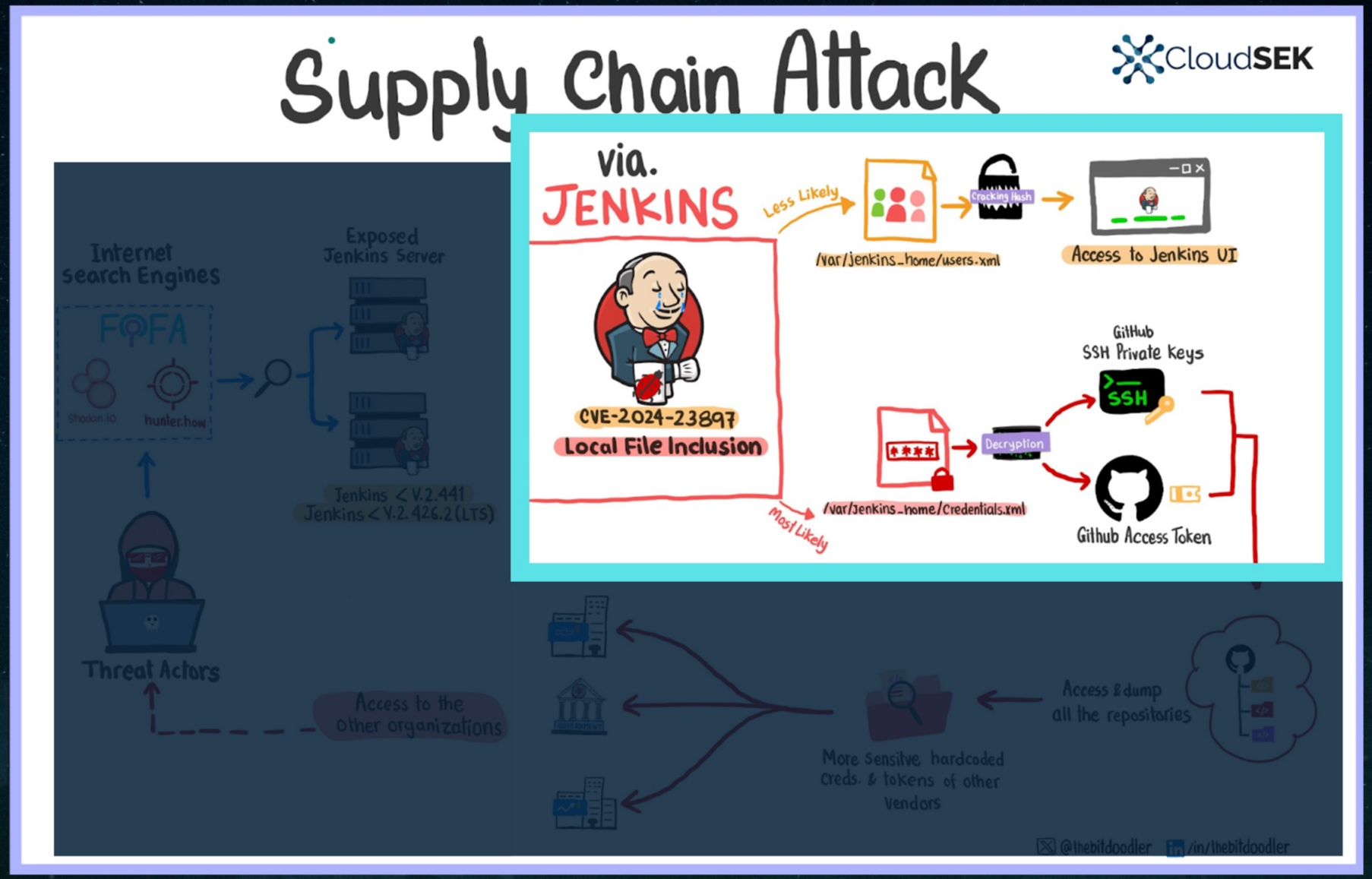
RANSOMXX & INTELBROKER

Your paragraph text



source: https://www.cloudsek.com/blog/major-payment-disruption-ransomware-strikes-indian-banking-infrastructure

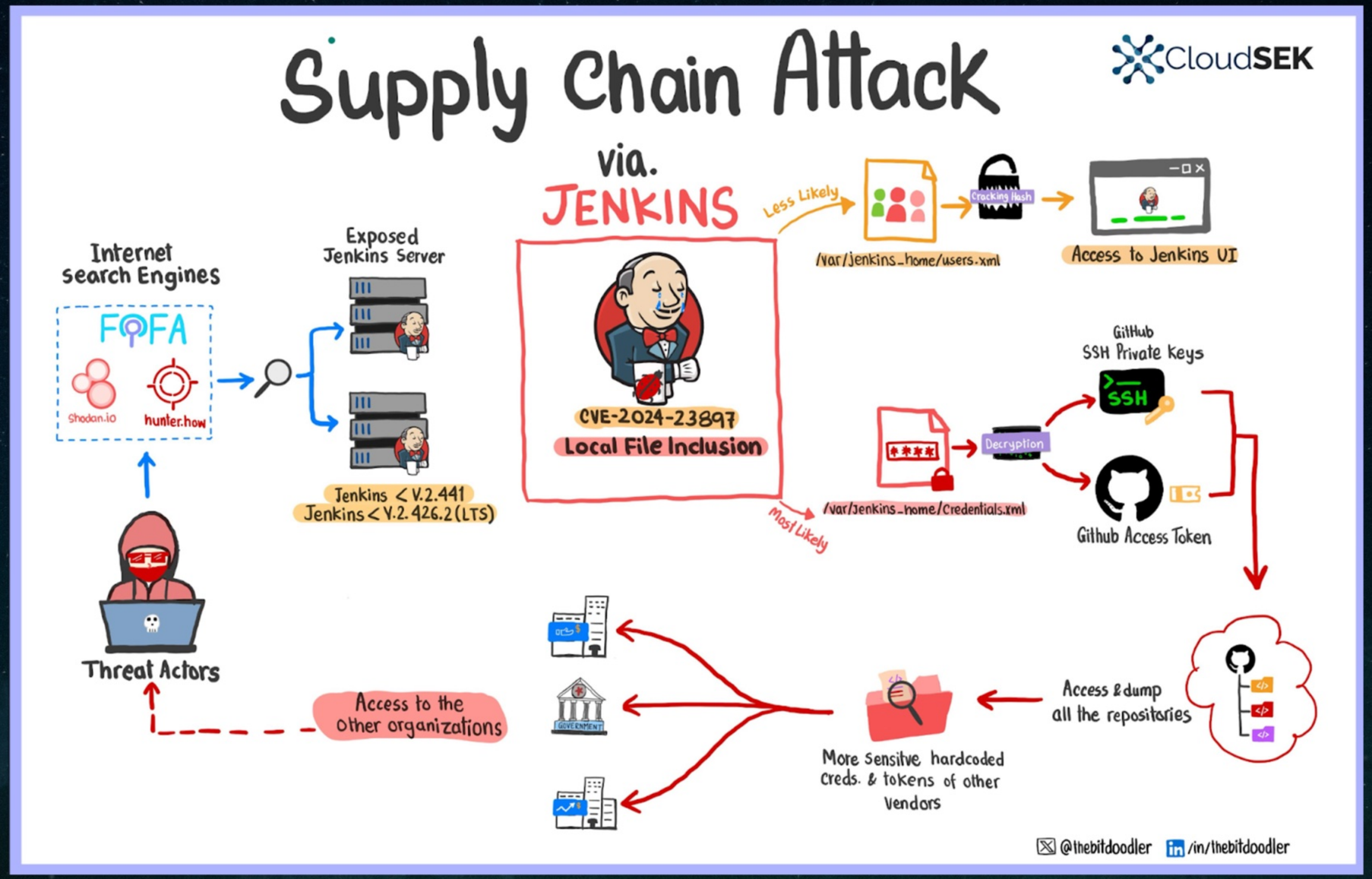
RANSOMXX & INTELBROKER



source: https://www.cloudsek.com/blog/major-payment-disruption-ransomware-strikes-indian-banking-infrastructure

RANSOMXX & INTELBROKER

Your paragraph text



source: https://www.cloudsek.com/blog/major-payment-disruption-ransomware-strikes-indian-banking-infrastructure

CRYPTOJACKING

source: https://www.coinguides.org

RELATED TOOLS

PROWLER

- AWS security best practices assessments, audits, incident response
- Continuous monitoring with SaaS

PERIMETERATOR

- Continuous auditing of internet facing AWS services
- Leverages nmap scans
- Returns raw results for processing

CLOUDSPLOIT

- CSPM
- Primarily used in pentesting
- Scans for insecure configurations, exposed services, or improper permissions

CLOUDMAPPER

- Generate AWS network map
- Find public hosts
- Looks for unused resources

THE GAP

QUICK TRIAGE

- Identify resources affected
- Resource owner
- Exposure timeframe
- Impacted service
- Vulnerabilities

THE GAP

NASCENT ENVIRONMENTS

- Lack of detection
- Missing alarms
- Limited context due to default configuration

LUMINAUT

INSIDE

1. Enumerate ENIs with public IPs
2. Gather context about related:
   a. Security groups
   b. EC2
   c. ELB
3. Query AWS CloudTrail & Config

OUTSIDE

1. Scan ports with nmap
2. WhatWeb HTTP service detection
3. Query Shodan for service & vulns

CONFIG

ENABLE OR DISABLE SCAN OPTIONS BASED ON INDIVDUAL USE-CASES

ALLOW LIST FOR KNOWN AND/OR APPROVED RESOURCES

REPORTING TO THE TERMINAL, HTML, JSON, AND CSV TIMELINE

DEMO

LUMINAUT

“DEMO”

```
$ luminaut -c configs/shodan.toml
```

```
18.223.4.11 | us-east-2
☁️AWS Elastic Network Interfaces
Resources:
eni-0c888102e7b76111a in vpc-08c43b16d92f5abe9 (us-east-2a)
Security Groups: grafana-web (sg-06d81b937dad1ff48)

🔒 AWS Security Groups
Resources:
grafana-web (sg-06d81b937dad1ff48)
  0.0.0.0/0 ingress 443 to 443 tcp (sgr-0cb39edad36edeb6f: web)

☁️AWS Elastic Load Balancers
Resources:
ecs-grafana-01 internet-facing (active) Created: 2025-01-07 12:56:46.829000+00:00
  Listeners: 443/HTTPS
```

⚙️AWS Config
Resources:
  2 resources discovered.

☁️AWS CloudTrail
Events:
2025-01-07 12:56:46+00:00 Resource created: Load balancer created by cbryce-dev. (AWS::ElasticLoadBalancingV2::LoadBalancer arn:aws:elasticloadbalancing:us-east-2:474813326059:loadbalancer/app/ecs-grafana-01/8c23025c4c6e9027)
2025-01-07 13:06:37+00:00 Security group rule changed: Ingress rule added by cbryce-dev. Allow: 32.221.0.0/16:443 over tcp. (AWS::EC2::SecurityGroup sg-06d81b937dad1ff48)
2025-01-07 13:14:28+00:00 Security group rule changed: Security group rules modified by cbryce-dev. Rule updated to: 0.0.0.0/0:443 over tcp. (AWS::EC2::SecurityGroup sg-06d81b937dad1ff48)
2025-01-07 13:14:48+00:00 Security group rule changed: Security group rules modified by cbryce-dev. Rule updated to: 32.221.0.0/16:443 over tcp. (AWS::EC2::SecurityGroup sg-06d81b937dad1ff48)
2025-01-07 13:30:55+00:00 Resource created: Network interface created by ElasticLoadBalancing. (AWS::EC2::NetworkInterface eni-0c888102e7b76111a)
2025-01-07 13:35:44+00:00 Security group rule changed: Security group rules modified by cbryce-dev. Rule updated to: 0.0.0.0/0:443 over tcp. (AWS::EC2::SecurityGroup sg-06d81b937dad1ff48)

🔍 nmap
Services:
tcp/443 Status: open Name: http Product: AWS Elastic Load Balancing

🌐 Shodan.io
Services:
tcp/80 Apache httpd (as of 2024-12-22 16:06:34.596104)
  HTTP Server: Apache/2.4.62 (Amazon Linux) OpenSSL/3.0.8 HTTP Title: 302 Found
  Vulnerability: CVE-2009-2299 (CVSS: 5.0)
  Vulnerability: CVE-2009-1390 (CVSS: 6.8)
  Vulnerability: CVE-2013-4365 (CVSS: 7.5)
  Vulnerability: CVE-2012-3526 (CVSS: 5.0)
  Vulnerability: CVE-2023-5678 (CVSS: 5.3)
  29 total vulnerabilities found. See JSON for full report.
tcp/443 Grafana (Open Source) (as of 2025-01-10 00:12:47.650876)
  HTTP Title: Grafana
Resources:
 Hostname: luminaut.org (as of 2025-01-10T00:12:47.650876)
 Hostname: amazonaws.com (as of 2025-01-10T00:12:47.650876)

🕸Whatweb

```
Services:
- http://18.223.4.11:443
  HTTPServer: awselb/2.0
  Title: 400 The plain HTTP request was sent to HTTPS port

- https://18.223.4.11:443
  RedirectLocation: /login
  UncommonHeaders: x-content-type-options

- https://18.223.4.11/login
  Grafana: 11.4.0
  HTML5
  Title: Grafana
  UncommonHeaders: x-content-type-options
```

timestamp	ip	source	event_type	message	resource_id
2025-01-07T12:56:46+00:00	3.141.249.143	AWS CloudTrail	Resource created	Load balancer created by cbryce-dev.	arn:aws:elasticloadbalancing:us-eas 2:474813326059:loadbalancer/app/e s-grafana-01/8c23025c4c6e9027
2025-01-07T12:56:46+00:00	18.223.4.11	AWS CloudTrail	Resource created	Load balancer created by cbryce-dev.	arn:aws:elasticloadbalancing:us-eas 2:474813326059:loadbalancer/app/e s-grafana-01/8c23025c4c6e9027
2025-01-07T13:06:37+00:00	3.141.249.143	AWS CloudTrail	Security group rule changed	Ingress rule added by cbryce-dev. Allow: 32.221.0.0/16:443 over tcp.	sg-06d81b937dad1ff48
2025-01-07T13:06:37+00:00	18.223.4.11	AWS CloudTrail	Security group rule changed	Ingress rule added by cbryce-dev. Allow: 32.221.0.0/16:443 over tcp.	sg-06d81b937dad1ff48
2025-01-07T13:14:28+00:00	3.141.249.143	AWS CloudTrail	Security group rule changed	Security group rules modified by cbryce-dev. Rule updated to: 0.0.0.0/0:443 over tcp.	sg-06d81b937dad1ff48
2025-01-07T13:14:28+00:00	18.223.4.11	AWS CloudTrail	Security group rule changed	Security group rules modified by cbryce-dev. Rule updated to: 0.0.0.0/0:443 over tcp.	sg-06d81b937dad1ff48
2025-01-07T13:14:48+00:00	3.141.249.143	AWS CloudTrail	Security group rule changed	Security group rules modified by cbryce-dev. Rule updated to: 32.221.0.0/16:443 over tcp.	sg-06d81b937dad1ff48
2025-01-07T13:14:48+00:00	18.223.4.11	AWS CloudTrail	Security group rule changed	Security group rules modified by cbryce-dev. Rule updated to: 32.221.0.0/16:443 over tcp.	sg-06d81b937dad1ff48
2025-01-07T13:30:55+00:00	18.223.4.11	AWS CloudTrail	Resource created	Network interface created by ElasticLoadBalancing.	eni-0c888102e7b76111a
2025-01-07T13:31:09+00:00	3.141.249.143	AWS CloudTrail	Resource created	Network interface created by ElasticLoadBalancing.	eni-0efebcd18c7bb5ae3
2025-01-07T13:35:44+00:00	3.141.249.143	AWS CloudTrail	Security group rule changed	Security group rules modified by cbryce-dev. Rule updated to: 0.0.0.0/0:443 over tcp.	sg-06d81b937dad1ff48
2025-01-07T13:35:44+00:00	18.223.4.11	AWS CloudTrail	Security group rule changed	Security group rules modified by cbryce-dev. Rule updated to: 0.0.0.0/0:443 over tcp.	sg-06d81b937dad1ff48

```toml
[report]
console = true

json = true
json_file = "configs/test.json"

html = true
html_file = "configs/test.html"

timeline = true
timeline_file = "configs/test.timeline.csv"
```

```toml
[tool]
nmap.enabled = true
whatweb.enabled = false

[tool.shodan]
enabled = true
api_key = "your-api-key"

[tool.aws]
aws_regions = ["us-east-2"]

cloudtrail.start_time = 2025-01-07T00:00:00Z
cloudtrail.end_time = 2025-01-08T00:00:00Z

[[tool.aws.allowed_resources]]
type = "AWS::EC2::NetworkInterface"
id = "eni-04e4a7127387ec230"
```

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LuminautReadResourcePermissions",
      "Action": [
        "cloudtrail:LookupEvents",
        "config:GetResourceConfigHistory",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroupRules",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

QUESTIONS

https://luminaut.org

SLIDES

https://luminaut.org