



Student Security Operations Center: Tools, Workflows, and Real-World Response

Aiden West, Emanuel Reynoso, Ibrahima Balde, Nehemia Araia

CYSE 368

4/23/2026



Introduction - Tools and Workflow

The background is a solid pink color. In the top right corner, there is a decorative graphic consisting of several overlapping geometric shapes: a dark pink square, a medium pink square, and a light pink square, all partially cut off by the edge of the frame.

Crowdstrike

What is CrowdStrike?

- Cloud based cybersecurity platform
- Gives SOC analysts visibility into threats
- Uses AI analytics to detect known attack patterns

What is EDR?

- Technology that monitors endpoints (laptops, phones, cameras, etc)
- Detects suspicious or malicious activity in real time
- Allows SOC Analysts to investigate and respond to threats immediately



Current Status

5 / 100

Temperature

76

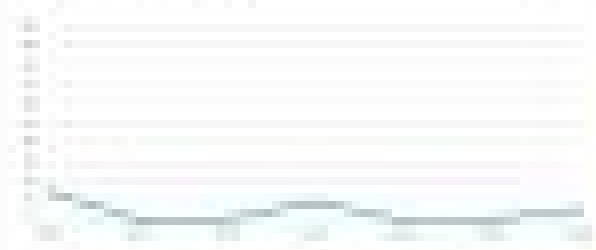
Humidity

45%
40%
35%

Pressure

1013 hPa

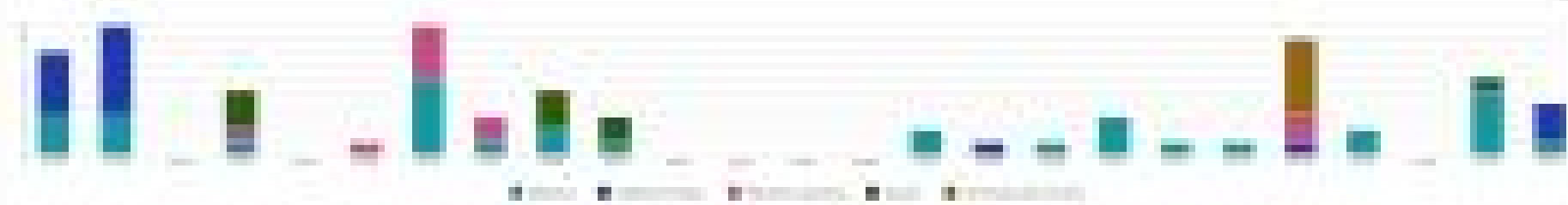
Temperature History



Temperature Details

Location	Temperature (°C)	Humidity (%)	Pressure (hPa)
Room 1	22	45	1013
Room 2	20	40	1013
Room 3	18	35	1013

Temperature Analysis



Project Overview

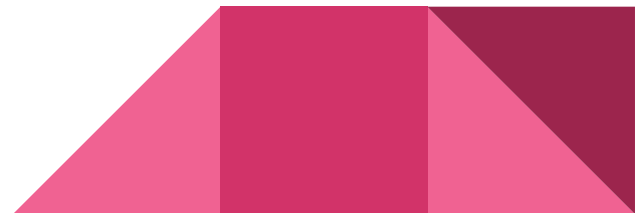
Task ID	Task Name	Start Date	End Date	Progress (%)	Assignee	Status	Dependencies
1	Task 1	2023-01-01	2023-01-15	100	John	Completed	
2	Task 2	2023-01-15	2023-02-01	100	Jane	Completed	1
3	Task 3	2023-02-01	2023-02-15	100	John	Completed	2
4	Task 4	2023-02-15	2023-03-01	100	Jane	Completed	3
5	Task 5	2023-03-01	2023-03-15	100	John	Completed	4
6	Task 6	2023-03-15	2023-04-01	100	Jane	Completed	5
7	Task 7	2023-04-01	2023-04-15	100	John	Completed	6
8	Task 8	2023-04-15	2023-05-01	100	Jane	Completed	7
9	Task 9	2023-05-01	2023-05-15	100	John	Completed	8
10	Task 10	2023-05-15	2023-06-01	100	Jane	Completed	9
11	Task 11	2023-06-01	2023-06-15	100	John	Completed	10
12	Task 12	2023-06-15	2023-07-01	100	Jane	Completed	11
13	Task 13	2023-07-01	2023-07-15	100	John	Completed	12
14	Task 14	2023-07-15	2023-08-01	100	Jane	Completed	13
15	Task 15	2023-08-01	2023-08-15	100	John	Completed	14
16	Task 16	2023-08-15	2023-09-01	100	Jane	Completed	15
17	Task 17	2023-09-01	2023-09-15	100	John	Completed	16
18	Task 18	2023-09-15	2023-10-01	100	Jane	Completed	17
19	Task 19	2023-10-01	2023-10-15	100	John	Completed	18
20	Task 20	2023-10-15	2023-11-01	100	Jane	Completed	19
21	Task 21	2023-11-01	2023-11-15	100	John	Completed	20
22	Task 22	2023-11-15	2023-12-01	100	Jane	Completed	21
23	Task 23	2023-12-01	2023-12-15	100	John	Completed	22
24	Task 24	2023-12-15	2024-01-01	100	Jane	Completed	23
25	Task 25	2024-01-01	2024-01-15	100	John	Completed	24
26	Task 26	2024-01-15	2024-02-01	100	Jane	Completed	25
27	Task 27	2024-02-01	2024-02-15	100	John	Completed	26
28	Task 28	2024-02-15	2024-03-01	100	Jane	Completed	27
29	Task 29	2024-03-01	2024-03-15	100	John	Completed	28
30	Task 30	2024-03-15	2024-04-01	100	Jane	Completed	29
31	Task 31	2024-04-01	2024-04-15	100	John	Completed	30
32	Task 32	2024-04-15	2024-05-01	100	Jane	Completed	31
33	Task 33	2024-05-01	2024-05-15	100	John	Completed	32
34	Task 34	2024-05-15	2024-06-01	100	Jane	Completed	33
35	Task 35	2024-06-01	2024-06-15	100	John	Completed	34
36	Task 36	2024-06-15	2024-07-01	100	Jane	Completed	35
37	Task 37	2024-07-01	2024-07-15	100	John	Completed	36
38	Task 38	2024-07-15	2024-08-01	100	Jane	Completed	37
39	Task 39	2024-08-01	2024-08-15	100	John	Completed	38
40	Task 40	2024-08-15	2024-09-01	100	Jane	Completed	39
41	Task 41	2024-09-01	2024-09-15	100	John	Completed	40
42	Task 42	2024-09-15	2024-10-01	100	Jane	Completed	41
43	Task 43	2024-10-01	2024-10-15	100	John	Completed	42
44	Task 44	2024-10-15	2024-11-01	100	Jane	Completed	43
45	Task 45	2024-11-01	2024-11-15	100	John	Completed	44
46	Task 46	2024-11-15	2024-12-01	100	Jane	Completed	45
47	Task 47	2024-12-01	2024-12-15	100	John	Completed	46
48	Task 48	2024-12-15	2025-01-01	100	Jane	Completed	47
49	Task 49	2025-01-01	2025-01-15	100	John	Completed	48
50	Task 50	2025-01-15	2025-02-01	100	Jane	Completed	49
51	Task 51	2025-02-01	2025-02-15	100	John	Completed	50
52	Task 52	2025-02-15	2025-03-01	100	Jane	Completed	51
53	Task 53	2025-03-01	2025-03-15	100	John	Completed	52
54	Task 54	2025-03-15	2025-04-01	100	Jane	Completed	53
55	Task 55	2025-04-01	2025-04-15	100	John	Completed	54
56	Task 56	2025-04-15	2025-05-01	100	Jane	Completed	55
57	Task 57	2025-05-01	2025-05-15	100	John	Completed	56
58	Task 58	2025-05-15	2025-06-01	100	Jane	Completed	57
59	Task 59	2025-06-01	2025-06-15	100	John	Completed	58
60	Task 60	2025-06-15	2025-07-01	100	Jane	Completed	59
61	Task 61	2025-07-01	2025-07-15	100	John	Completed	60
62	Task 62	2025-07-15	2025-08-01	100	Jane	Completed	61
63	Task 63	2025-08-01	2025-08-15	100	John	Completed	62
64	Task 64	2025-08-15	2025-09-01	100	Jane	Completed	63
65	Task 65	2025-09-01	2025-09-15	100	John	Completed	64
66	Task 66	2025-09-15	2025-10-01	100	Jane	Completed	65
67	Task 67	2025-10-01	2025-10-15	100	John	Completed	66
68	Task 68	2025-10-15	2025-11-01	100	Jane	Completed	67
69	Task 69	2025-11-01	2025-11-15	100	John	Completed	68
70	Task 70	2025-11-15	2025-12-01	100	Jane	Completed	69
71	Task 71	2025-12-01	2025-12-15	100	John	Completed	70
72	Task 72	2025-12-15	2026-01-01	100	Jane	Completed	71
73	Task 73	2026-01-01	2026-01-15	100	John	Completed	72
74	Task 74	2026-01-15	2026-02-01	100	Jane	Completed	73
75	Task 75	2026-02-01	2026-02-15	100	John	Completed	74
76	Task 76	2026-02-15	2026-03-01	100	Jane	Completed	75
77	Task 77	2026-03-01	2026-03-15	100	John	Completed	76
78	Task 78	2026-03-15	2026-04-01	100	Jane	Completed	77
79	Task 79	2026-04-01	2026-04-15	100	John	Completed	78
80	Task 80	2026-04-15	2026-05-01	100	Jane	Completed	79
81	Task 81	2026-05-01	2026-05-15	100	John	Completed	80
82	Task 82	2026-05-15	2026-06-01	100	Jane	Completed	81
83	Task 83	2026-06-01	2026-06-15	100	John	Completed	82
84	Task 84	2026-06-15	2026-07-01	100	Jane	Completed	83
85	Task 85	2026-07-01	2026-07-15	100	John	Completed	84
86	Task 86	2026-07-15	2026-08-01	100	Jane	Completed	85
87	Task 87	2026-08-01	2026-08-15	100	John	Completed	86
88	Task 88	2026-08-15	2026-09-01	100	Jane	Completed	87
89	Task 89	2026-09-01	2026-09-15	100	John	Completed	88
90	Task 90	2026-09-15	2026-10-01	100	Jane	Completed	89
91	Task 91	2026-10-01	2026-10-15	100	John	Completed	90
92	Task 92	2026-10-15	2026-11-01	100	Jane	Completed	91
93	Task 93	2026-11-01	2026-11-15	100	John	Completed	92
94	Task 94	2026-11-15	2026-12-01	100	Jane	Completed	93
95	Task 95	2026-12-01	2026-12-15	100	John	Completed	94
96	Task 96	2026-12-15	2027-01-01	100	Jane	Completed	95
97	Task 97	2027-01-01	2027-01-15	100	John	Completed	96
98	Task 98	2027-01-15	2027-02-01	100	Jane	Completed	97
99	Task 99	2027-02-01	2027-02-15	100	John	Completed	98
100	Task 100	2027-02-15	2027-03-01	100	Jane	Completed	99

PagerDuty



Phishing and Incident Response

- Coordinating Alerts
 - Documenting Incidents
 - MTTA & MTTR Analytics
- 1: Email reported -> Alert generated
 - 2: Review email
 - 3: Check for similar reports
 - 4: Document and conclude



PD Interface



Main content area containing a large grey rectangular placeholder and a small orange button.

Right sidebar containing a profile picture, name, and bio information.

Left sidebar containing a list of items with various icons and text labels.

Right sidebar containing a 'Registered' section with a profile picture and text.

COOL Account: Next Immediate Action Required

Dear Member,

There have been concerns about the COOL program. To ensure you receive the best possible service, please call our customer service line at 1-800-833-8333. We will be happy to assist you with any questions or concerns you may have.

- Call us
- Visit us
- Write us

Thank you for your support.

Best regards,
COOL Customer Service

COOL
1-800-833-8333
www.cool.com



Your Account's Login Has Been Affected - Check Eligibility Now

1/1/2021



Hi [Name],

Microsoft's new digital licensing model means that all government (and other) users are responsible for their own licenses. This means you will be responsible for making sure you have the right licenses for your organization.

What does this mean for your organization?

There are several things you should do:

- Audit your licenses
- Inventory your devices
- Check device status
- Investigate options

Go to [Microsoft's new digital licensing model](#) page for more information.

For help with your digital licensing, go to [Microsoft's new digital licensing](#) page.

Best,

Microsoft Support

1/1/2021

Global Market Overview

The global market is characterized by a high level of volatility and uncertainty, driven by a combination of factors including geopolitical tensions, economic challenges, and technological advancements. The market is segmented into various regions, each with its own unique characteristics and growth prospects.

- North America
- Latin America
- Europe
- Asia Pacific
- Middle East & Africa
- Oceania
- Key Market Drivers and Challenges
- Market Outlook
- Investment Opportunities
- Risk Factors

Key Market Drivers and Challenges

The market is driven by several key factors, including technological innovation, demographic changes, and economic growth. However, it also faces significant challenges, such as geopolitical tensions, economic uncertainty, and environmental concerns.

Key Challenges: High volatility, geopolitical tensions, economic uncertainty, and environmental concerns.

IBM Qradar



Why is it important?

- Halts malicious activity
- Prevents data breaches
- Enforces security

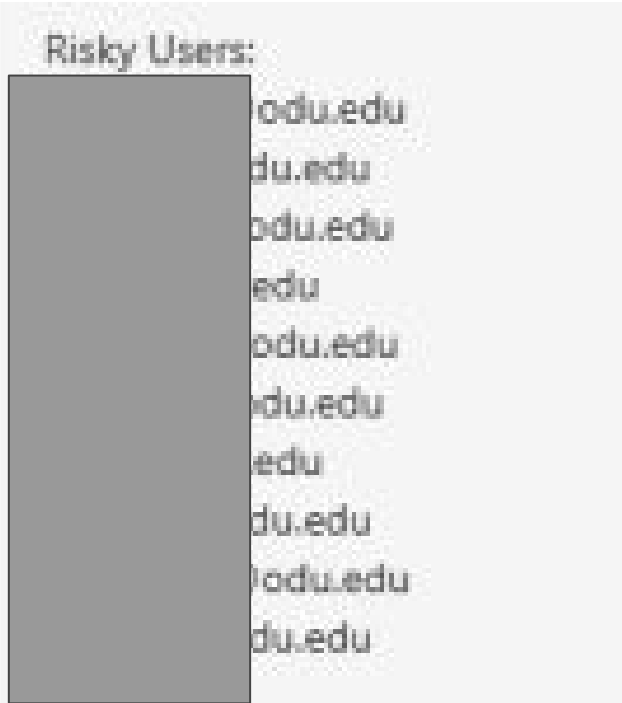


User Investigation Protocol

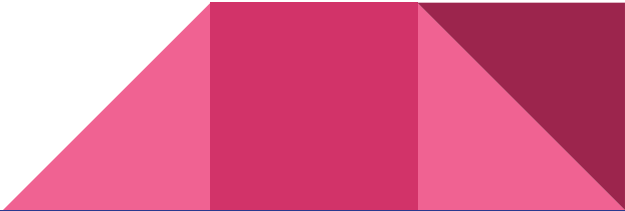
- List of Risky Users (Time, Day, and Username)
 - QRadar Log Analysis
- Analyse for false positives and compromised accounts



Example Scenario Pt.1



- List of Risky Users
- Go through each one in-depth
- Possibly reset password



Example Scenario Pt. 2

1) Use filter to look for risky user

Make sure we're looking at the time that's reported

2) Check IP addresses to see where the log-in was at

Example Scenario Pt. 3

10/17/2015 10:00 AM: [Redacted] [Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]

[Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]

[Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]
10/17/2015 10:00 AM: [Redacted] [Redacted]



Real SOC Workflow

Alert Triggered

- **PagerDuty** - Phishing email reports
- **QRadar** - Risky user flags
- **CrowdStrike** - Endpoint detection

Review

- **PagerDuty & QRadar** - Note key indicators
- **CrowdStrike** - Prioritize by severity

Investigate

- **PagerDuty** - Sender domain, URLs, Attachments, etc.
- **QRadar** - Geo location, login attempts, etc.
- **CrowdStrike** - Trace full process tree

Verdict

- **True positive** - Real threat
- **False positive** - Normal activity flagged by mistake

Wrap up

- Document findings
- Resolve and close ticket
- Notify team

Concluding Remarks



Thank you!

Any Questions?

Stay Connected with us on LinkedIn!

Nehemia Araia, Aiden West, Emanuel Reynoso,
Ibrahima Balde

