MINING AND METALS ISAC

MM-ISAC

We all should be feeling a little bit blue

Lessons learned from the CrowdStrike Outage

TLP: CLEAR

Rob Labbé

CISO-in-Residence
CEO

Agenda

- What Happened?
- Adversary Actions
- Lessons Learned
- EDR/XDR Best Practices
- Questions

What Happened

An Incident Review

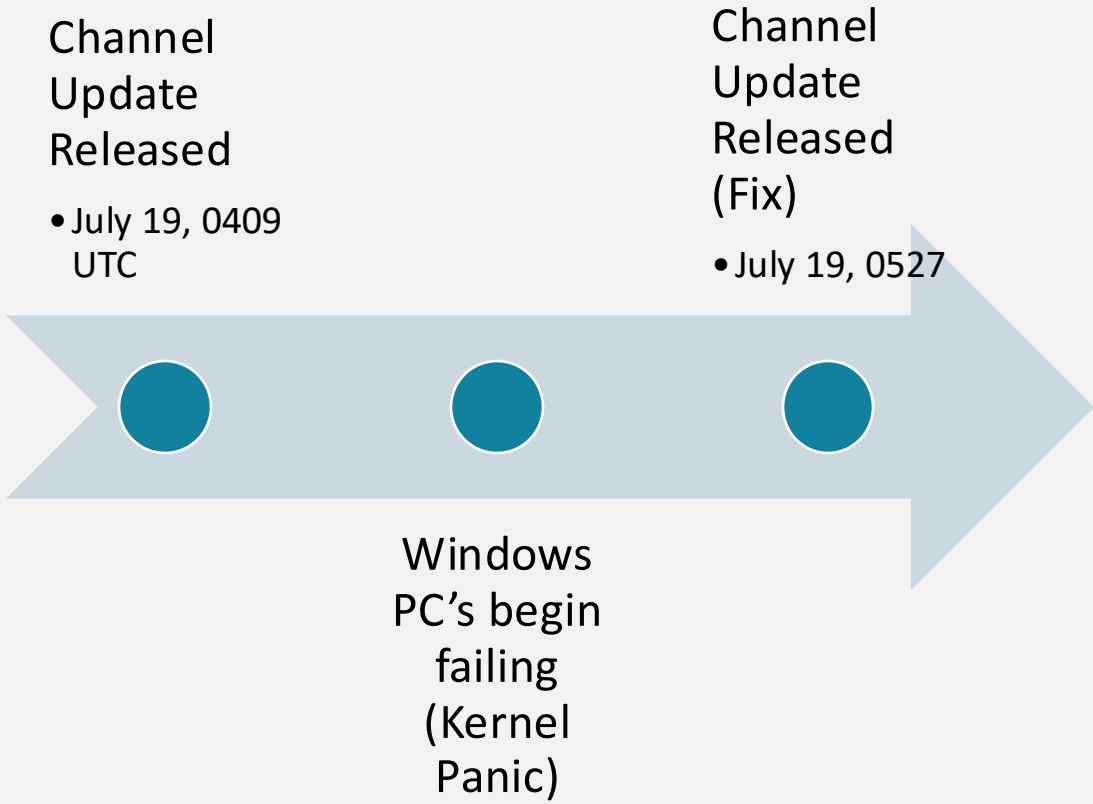
What Happened?

EDR/XDR solutions on Windows must run in the kernel to detect kernel level activity.

Kernel code is difficult to write and error checking and crash protection options are limited.

Kernel drivers must go through a certification process with Microsoft – This is a slow process so CrowdStrike updates the kernel drivers through content that is interpreted by the kernel

The channel update that caused the update was intended to detect new attack patterns affecting named pipes

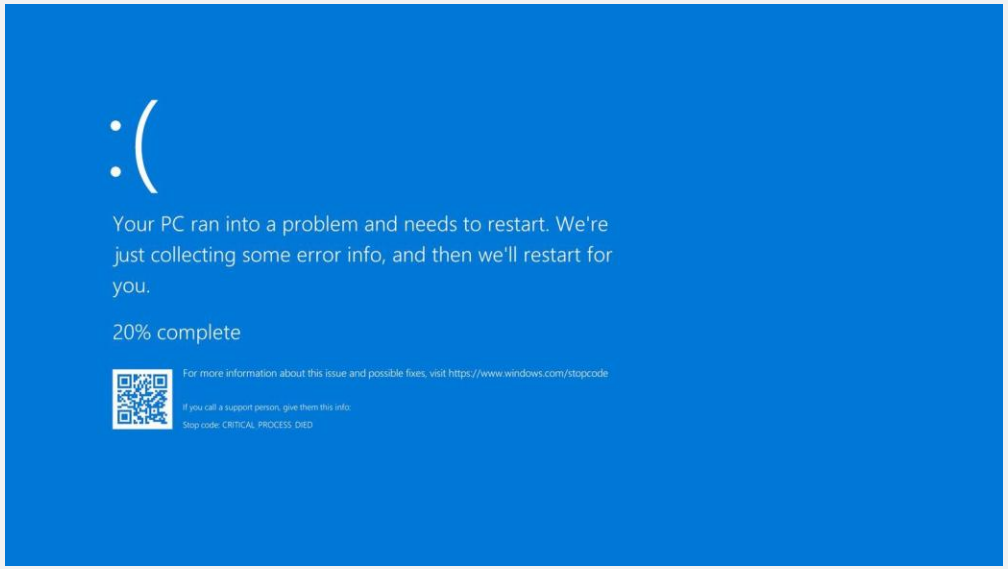


Why Such a Big Impact?

Update Types:

1. Engine Updates
   - Periodic updates to the application itself, similar to Windows and other updates
   - Corporate users typically deploy on a lag for testing, with a staged rollout.
2. Content Updates (Channel Updates)
   - Update detections based on the vendor's latest intelligence – similar to AV signature updates
   - Occur frequently – up to several times a day
   - May not respect the engine update schedule

With this being a channel update, Falcon agents picked up the update, crashed and could not reboot.



We Actually Got Lucky

This could have been way worse.

- Update timing meant many client computers in North America and Europe (laptops, etc.) were off during the at-risk period.
- The same mechanism that caused the issue could be used to ensure that computers that came online later were not impacted.

Time Zone	Start	End
UTC	0409	0527
Eastern US/CA	0009	0127
Pacific US/CA	2109 (July 18)	2227
Perth	1209	1327
London	0509	0627
Tokyo	1309	1427

Adversary Actions

Don’t let a good incident go to waste

Opportunistic Attacks

Shortlist:

- General scams- legal scams, CrowdStrike/Microsoft-themed phishing, typosquatting domains
- Fake Updates and Hotfixes
- Misinformation – add to confusion/ malicious links
- Ransomware, RATs and Wiper delivery

It only took minutes!

7:15 UTC – Google Cloud reports crash due to Crowdstrike Update
Source status.cloud.google.com/incidents

19 Jul 2024	00:15 PDT	Impacted users may observe Serial port 1 showing the call trace, SYSTEM_THREAD_EXCEPTION_NOT_HANDLED Csagent.sys (part of the Crowdstrike Application package) 0xFFFFFFFFC0000005 0xFFFFF80E88CF033D 0xFFFF858A870FAC58 0xFFFF858A870FA4A0 Dumping stack trace: 0xFFFFF809E35317BF (pvpanic.sys+0x17BF) 0xFFFFF809E35316CB (pvpanic.sys+0x16CB) 0xFFFFF80335941B27 (ntoskrnl.exe+0x292B27) 0xFFFFF80335940AD9 (ntoskrnl.exe+0x291AD9) 0xFFFFF80335868CE7 (ntoskrnl.exe+0x1B9CE7) 0xFFFFF8033588447C (ntoskrnl.exe+0x1D547C) 0xFFFFF803358416BF (ntoskrnl.exe+0x1926BF) 0xFFFFF8033587335F (ntoskrnl.exe+0x1C435F) 0xFFFFF803356D77D0 (ntoskrnl.exe+0x0287D0) 0xFFFFF8033579D214 (ntoskrnl.exe+0x0EE214) 0xFFFFF8033587CF42 (ntoskrnl.exe+0x1CDF42) 0xFFFFF8033587893D (ntoskrnl.exe+0x1C993D) 0xFFFFF809E314033D (csagent.sys+0x0E033D) 0xFFFFF809E3115EEE (csagent.sys+0x0B5EEE) 0xFFFFF809E3117185 (csagent.sys+0x0B7185) 0xFFFFF809E334A037 (csagent.sys+0x2EA037) 0xFFFFF809E3346BB4 (csagent.sys+0x2E6BB4) 0xFFFFF809E30C68C1 (csagent.sys+0x0668C1) 0xFFFFF809E30C597E (csagent.sys+0x06597E) 0xFFFFF809E30C56EB (csagent.sys+0x0656EB) 0xFFFFF809E316883A (csagent.sys+0x10883A) 0xFFFFF809E30BDD3B (csagent.sys+0x05DD3B) 0xFFFFF809E30BDB57 (csagent.sys+0x05DB57) 0xFFFFF809E315D4D1 (csagent.sys+0x0FD4D1) 0xFFFFF803357B4A85 (ntoskrnl.exe+0x105A85) 0xFFFFF803358719FC (ntoskrnl.exe+0x1C29FC) Workaround: We recommend the affected users to work with the application package provider.

Name: CROWDSTRIKEUPDATE[.]COM
Created: 2024-07-19 07:51:10 UTC

TLP CLEAR

RemCos RAT

CROWDSTRIKE | BLOG

Featured

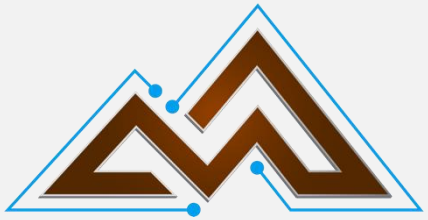
Details

On July 19, 2024, a ZIP archive named `crowdstrike-hotfix.zip` (SHA256 hash: `c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2`) was uploaded to an online malware-scanning service by a Mexico-based submitter.

The ZIP file's accompanying Spanish-language instructions appear to pose as a utility for automating recovery for the content update issue. The instructions prompt the user to run `Setup.exe` (SHA256 hash: `5ae3838d77c2102766538f783d0a4b4205e7d2cdba4e0ad2ab332dc8ab32fea9`) to start the patch installation.

TLP CLEAR

Moving Forward



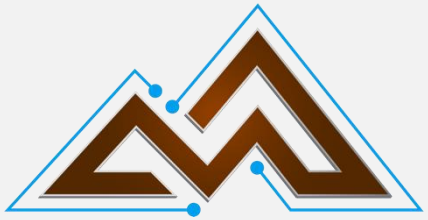
What can we expect?

TLP
CLEAR

Lessons Learned

Resilience Matters

Two Types of Response



Not a security incident, IT Problem

- Unclear ownership – IT is down, but it is a security tool that caused it
- Freelancing and unclear chain of command
- Blame and lack of accountability

This is a Security Incident

- ✓Immediate implementation of incident response plan
- ✓Selection of a playbook that is close – often Ransomware
- ✓Clear, effective chain of command involving security and IT
- ✓Lack of blame and finger-pointing

Incident?

There is much debate within companies and online if this should count as a security incident or not

MM-ISAC definition of a cyber security incident:

"A cyber event that materially impacts, or has the potential to impact materially, the ability of the company to execute on its mission in a safe, sustainable way."

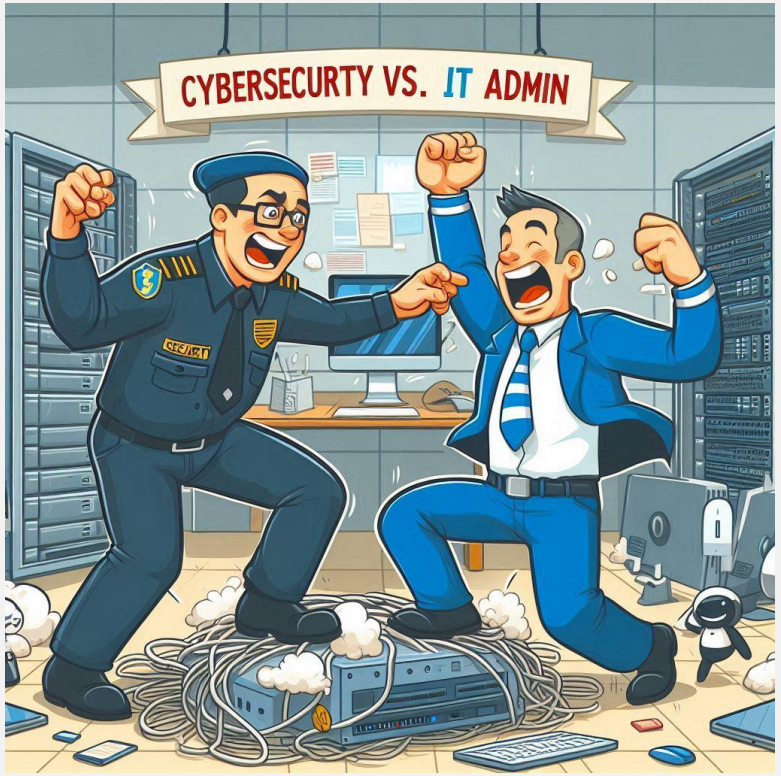
An incident can be:

a. Malicious

b. Inadvertent

c. Control or security technology failure

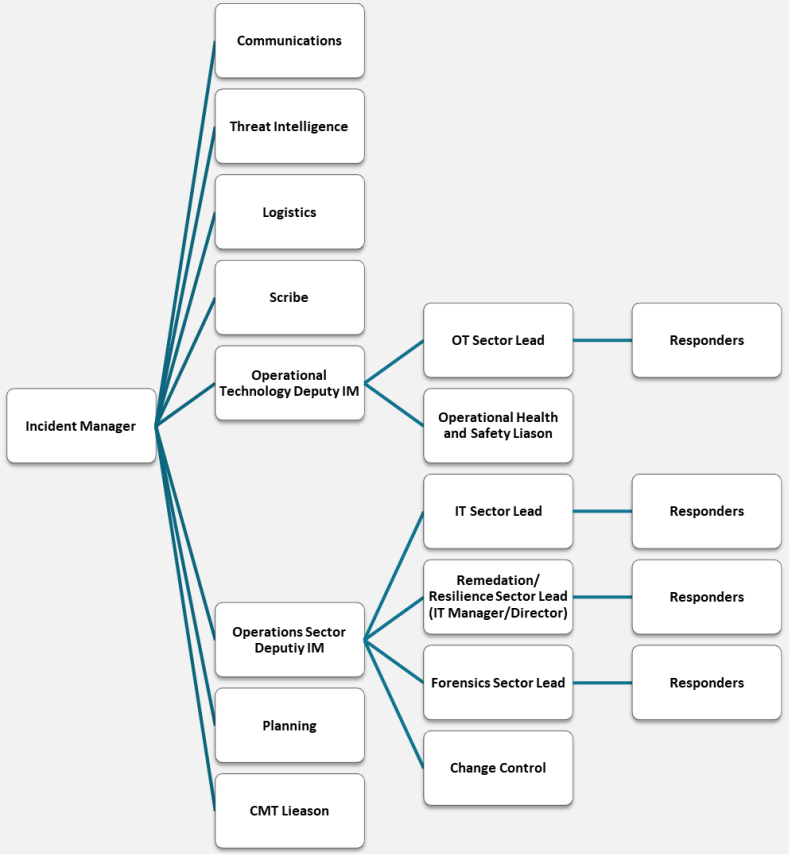
.



The goal? Resilience.

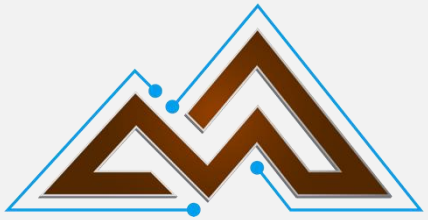
Effective Incident Response Plans

- Scale up to large global incidents and down to small incidents
- Provide for unity of command, clear communication and rapid decision-making
- Manageable span of control
- Clear roles and responsibilities
- But – only if people are trained and it is rehearsed



TLP CLEAR

Next Steps:



If you are a CrowdStrike customer, conduct a lessons learned/ retrospective:

- Blame free
- Conducted by a neutral party
- While memories are fresh

If you are not:

- Tabletop a similar failure (even if your vendor says it could not happen to them)
- Conduct the retrospective

Compare against the best performers:

- Clear incident response plan based on ICS (Incident Command System) principles
- Executed a previously rehearsed playbook for something close and made adjustments as they went
- Span of control was manageable
- Tactical Priorities were clear
- Mental health and burnout were managed
- Capacity remained for other incidents

EDR/XDR Best Practices

Operational/Critical Environments

What Not To Do

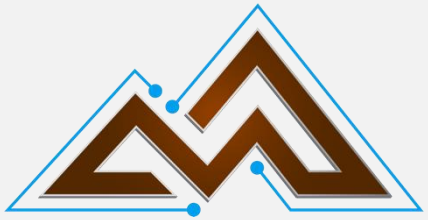
Don’t dump your current EDR solution

- Without a risk assessment
- Without a plan for replacement controls
- Based on emotion

If you do… Don’t

TLP CLEAR

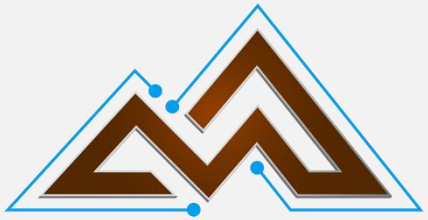
EDR/XDR Best Practices



One EDR for IT and operations

- Simpler environments are more secure
- Single view of all EDR clients
- Data does not fall through the cracks
- Simplify training and staff deployment

EDR/XDR Best Practices



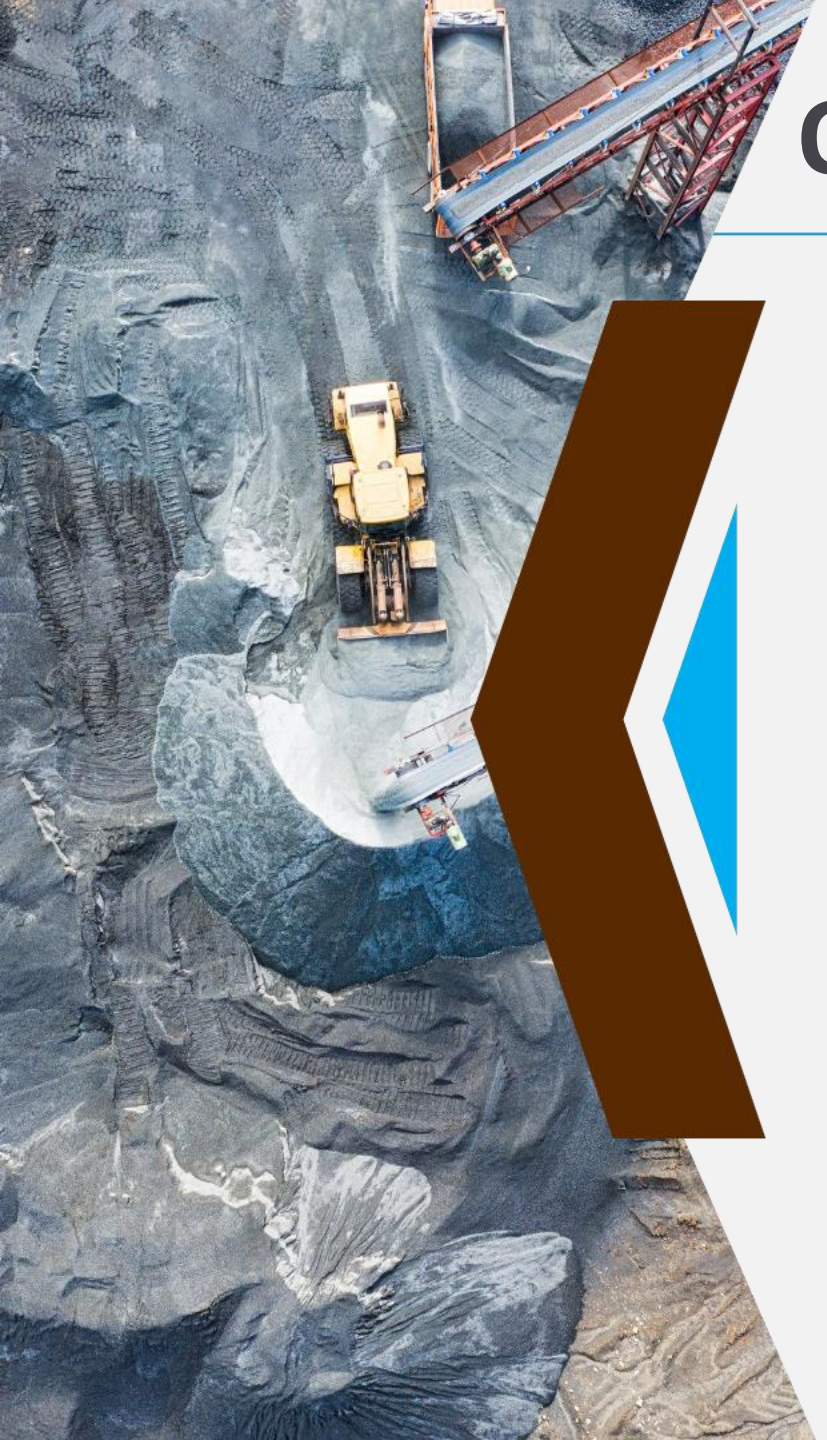
- IT Configuration
  - Workstations – Cloud-based controller
    - n-0.5 or 1 engine deployments
    - Phased content deployment (10%, 40%, 50%)
    - All detection engines running
    - Automatic containment rules
  - Servers – On-prem/proxy or cloud controller
    - n-1 engine deployments (full change control)
    - Phased content deployment (after workstations)
    - Blocking actions enabled
    - No automatic containment
- OT configuration or protected IT operations – On-prem or DMZ proxy controller
  - n-1.5 or 2 engine deployments (full change control)
  - Manual content updates with engine updates
  - Detection engines tuned down based on risk assessment
  - Alerting only – With the exception of highly mature environments

Summary

This one was bad, it could have been worse

Summary

- The issue's root cause was a bad content update from CrowdStrike that escaped testing
- Adversaries of all types were very quick to jump on this one and will apply the lessons to get quicker next time
- There will be a next time…
- This was an incident, those who treated it as such performed, on average, much better than those who did not.
- For those who struggled, there was often a mismatch between business and security objectives; alignment is critical to resilience.
- If you worked through the incident, do a lessons learned. If you did not, do a tabletop, update your incident response plans.



Questions

rlabbe@mmisac.org