NIST: Respond and Recover

NIST: Respond

- NIST Definition: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Creating incident response plans and playbooks to quickly respond to a cybersecurity event.
- Defining roles and duty assignments during a cybersecurity event
- This is go time! Triage, Containment, Eradication, and Mitigation of lost/exfiltrated/encrypted/stolen data.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

To Catch a Criminal

- At this stage we know we have been compromised and a bad actor is on our network or affecting our systems in some way.
- What do we do now?
- RESPOND! But we have a few things to consider in our response before we act.

Questions to consider

- Who or what is this bad actor?
- What are their goals and objectives?
- What systems do we know they've infected?
- What information do we want or need about them?
- Do we show our hand now letting them know they've been spotted and kicking them off our network or take actions to observe their behavior?
- How quickly can we get operations running or does this affect up-time or our clients?

SOAR

- Security orchestration, automation, and response (SOAR) refers to a set of services and tools that automate cyberattack prevention and response. This automation is accomplished by unifying your integrations, defining how tasks should be run, and developing an incident response plan that suits your organization’s needs. With the help of SOAR technology, security operation center (SOC) teams that were previously inundated with repetitive and time-consuming tasks are now able to resolve incidents more efficiently, in turn reducing costs, filling coverage gaps, and boosting productivity.

https://www.microsoft.com/en-us/security/business/security-101/what-is-soar

Endpoint Detection and Response (EDR)

- Coined by Anton Chuvakin, EDR is defined as a solution that “records and stores endpoint-system-level behaviors, uses various data analytics techniques to detect suspicious system behavior, provides contextual information, blocks malicious activity, and provides remediation suggestions to restore affected systems.”

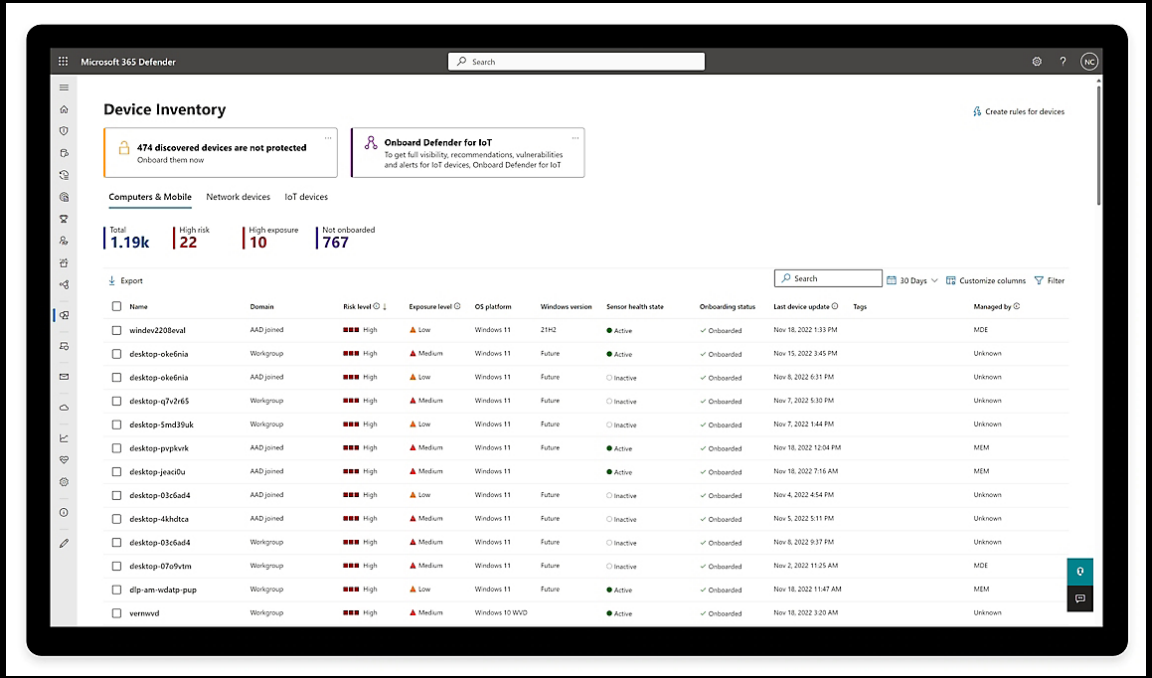
https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

Endpoint Detection and Response (EDR)

- Continuous monitoring of all endpoint devices for indicators of compromise or signs of malicious actives.
- EDR tools utilize pattern recgoniiton, known attack patterns, and anomalous behavior recognition to identify when a cyberattack is underway and apply proper remediations autonomously.
- EDR tools aid in investigation, isolation, and automated response to detected threats on endpoint devices. This helps mitigate the spread and potential damage from an ongoing cyberattack.

Endpoint Detection and Response (EDR)

- Microsoft Defender is an example of a widely used EDR system. Every modern copy of Windows comes with it preinstalled and Microsoft provides enterprise level management



https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint

Extended Detection and Response (XDR)

- XDR is an approach that integrates and analyzes data from multiple security layers, such as endpoints, networks, and cloud environments.
- Given this overview and integrations of our systems we can act on trends and threats affecting a wide range of our assets at once.
- Today machine learning and big data analytics is being utilized to respond to threats that would classically be missed by any one tool or system.

Security and AI

- Today the trend in IT and cybersecurity is we are integrating AI into our workflows. This does not mean AI is replacing us, but that we are starting to and likely will continue to work more closely with AI systems.
- Do I need to study and become proficient in AI development?
  - In a word no. You and most people do not need to learn the ins and outs of AI and Machine Learning systems, but be open to learning how to use these systems as tool are released and adopted into our workflows. Being adaptable and willing and able to learn new systems is what's important.

NIST: Recover

- NIST Definition: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
- Get the machine turning again! Mitigate downtime and restore service.
- Recovering from backups, system restorations, Incident analysis, and postmortems/lessons learned

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Restore Operations

- Down-time is money lost and in the corporate world that’s bad. One of our primary objectives then is to get service and operations restored as quickly and safely as possible.
- [It is estimated Amazon would lose] $203,577 every minute [of down-time] in today's [2021] numbers, or a $2,646,501 price tag for the 13 minute episode of downtime.

https://www.upguard.com/blog/the-cost-of-downtime-at-the-worlds-biggest-online-retailer

Recovering Endpoints

- What is the best way to ensure a system is no longer infected or compromised in any way?
- How can we maintain up-time during response and recovery?

Postmortems

- “Blameless” Culture: Having a Just [“Blameless”] Culture means that you’re making effort to balance safety and accountability. It means that by investigating mistakes in a way that focuses on the situational aspects of a failure’s mechanism and the decision-making process of individuals proximate to the failure, an organization can come out safer than it would normally be if it had simply punished the actors involved as a remediation.

https://www.etsy.com/codeascraft/blameless-postmortems/

Post Event Activities

- From here you team should have actionable items as a result of your well run postmortem meetings and detailed reports So, now we begin taking action on those items: upgrading and updating systems, revising our policies and procedures, moving back into Identify and Protect phases of the NIST Cybersecurity Framework.