IBM Security

Detect and Stop Advanced Threats
Solution Overview

CLEARLY VISUALIZE – INTELLIGENTLY UNCOVER – SEAMLESSLY STOP

Kim Rejman
IBM Security

22.8.2019

IBM

Norsk Hydro cyber attack – What happened?

Root cause was ransomware LockerGoga

Hit against Microsoft Active Directory

Used legitimate means to spread the ransomware

No indication of use or exploitation of vulnerabilities

Disabled all network interfaces, disconnected devices from the network, hit several PCs and servers simultaneously and asked Admin privileges.

Started to encrypt everything on the machines

Norsk Hydro cyber attack – Few things to notice

Anyone can be a target – crimes of opportunity

Protect your data

Create a strategy that considers how to respond to a cyber attack – essential for resiliency

Create threat models that assumes threat comes from an internal source – e.g. user behavior analytics

Network segmentation

Approach to effectively & efficiently detect & stop threats

Clearly Visualize

Detect threats in less time with more accuracy with **integrated systems** and **sound strategy**

Intelligently Uncover

Investigate suspicious activity by **transforming data into intelligence** using AI, machine learning and advanced rules engines

Seamlessly Stop

Block threats and reduce their impact with the **orchestration of people, processes and systems automation**

Clearly Visualize

Move from **fuzzy to clear** vision

Big-picture views and single command console of your environment's overall health and risk posture

Event chaining that enables spotting threats quickly

Data- and threat-agnostic solutions that can connect with your existing systems

Use applications that deliver out-of-the-box integrations to extend solution capabilities

Experienced analysts and threat intelligence experts following a robust strategy to quickly sift through the noise to spot threats

Intelligently Uncover

Move from **data to intelligence and insights**

Artificial Intelligence (AI) to enhance incident investigation, unstructured data analysis and threat correlation

Ensure your (SIEM) system takes advantage of threat intelligence data

Advanced analytics and machine-learning algorithms to quickly identify high-risk activities and prioritize the riskiest users

Intelligence sharing across analysts and stakeholders

Collaborative threat repository, analyses and investigations

Seamlessly Stop

Move from **simply seeing to seamlessly stopping**

Near real-time containment of insider threats by automatically suspending high-risk users' accounts with **dynamic identity and access policies**

Integration with enterprise systems from alerting to automatically initiating remediation and response, including threat blocking measures for your endpoints

Proactive strategy and playbooks for stopping threats across people, processes and technology

Detect and stop threats smarter and faster

Clearly Visualize

Reduce time to detect potential offenses and suspicious behavior

Receive precise analysis of the threat landscape to reduce false positives

See a comprehensive picture of risky activities to proactively address potential threats

Intelligently Uncover

Radically increase the speed of analysis and insight generation

Ingest internal and external data, structured or unstructured, with AI to identify likely threats

Add to the capabilities of security analysts to address skills gaps

Seamlessly Stop

Decrease the time to respond to and impact of advanced threats with integrated and automated systems

Lessen the effect on user productivity, brand value and customer trust as you protect against interruptions

Shorten the dwell time of cybercriminals' activity on your systems

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM