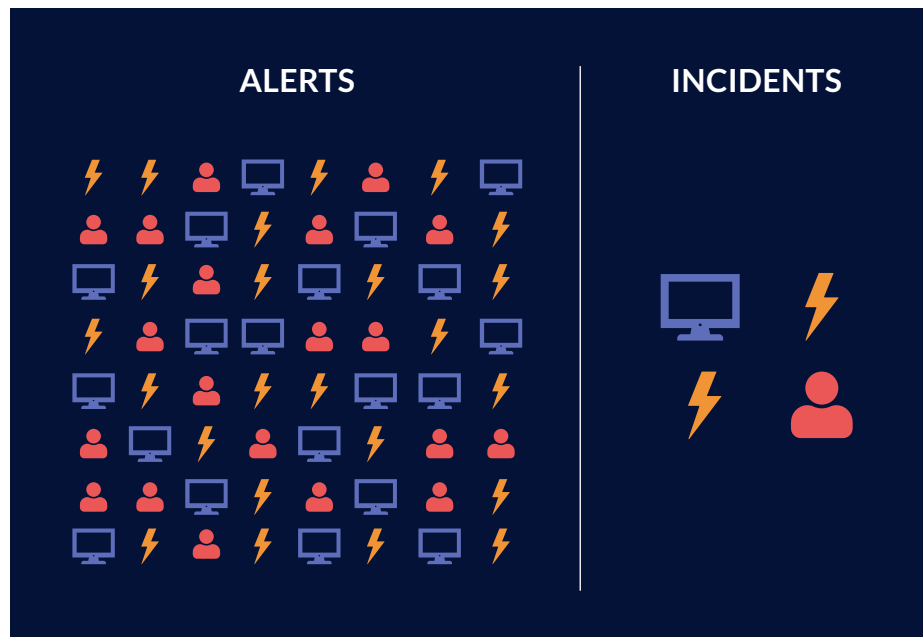


# Breakthroughs for Defenders

Incidents – Shrinking the problem space by orders of magnitude in many dimensions

## Stellar Cyber's Incidents avoid alert fatigue



- ✓ Automatically groups related alerts into incidents that show the progression of an attack – reducing the investigation effort from the number of alerts to the number of incidents, orders of magnitude reduction.
- ✓ Automatically combines related alerts into incidents with high fidelity – reducing the noise from the false positive of individual alerts – an order of magnitude improvement in accuracy.
- ✓ Automatically prioritizes incidents to clearly identify the most serious attacks – shows analysts exactly where and how to respond.
- ✓ Leverages telemetry from existing security tools as well as its own sensors – preserves existing security investment and provides 360-degree visibility by filling in the gaps.
- ✓ Feeds the AI engine with normalized and enriched quality data to initiate instant and effective responses – AI works better when it has the right data to work from.

# STELLAR CYBER LEVERAGES STATE-OF-THE-ART ML TO PRODUCE ALERTS, THEN TO HELP RANK AND GROUP ALERTS INTO INCIDENTS

By using incidents as the tool for analysis, security teams more quickly find and act on an attack.

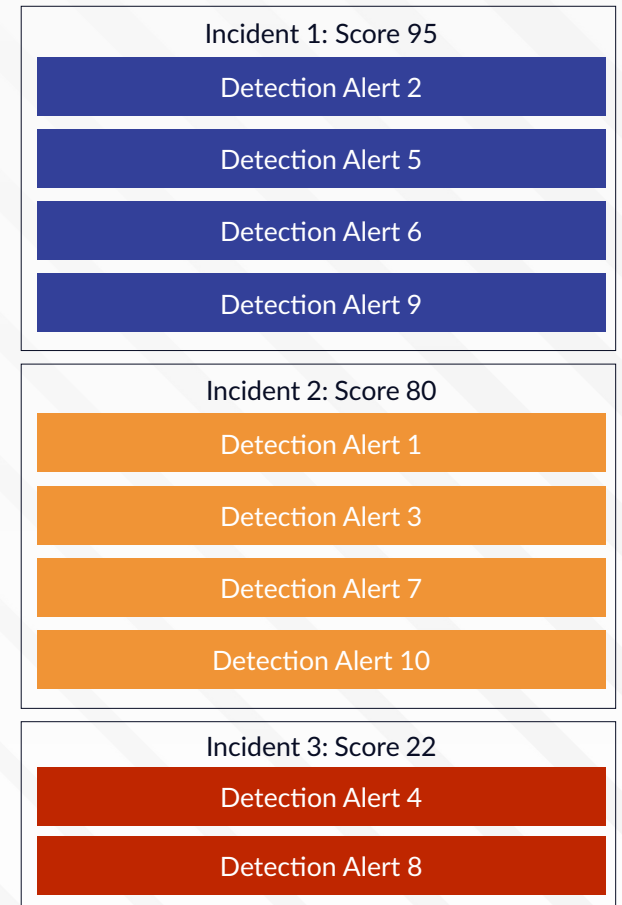
Alerts have limited context



Rank alerts by risk to look for context



Group alerts into incidents to see attacks fast



# STELLAR CYBER'S INCIDENTS REVEAL INTRUSIONS BY PRESENTING THE ATTACK AND WHAT ALERTS REPRESENT IT

The screenshot displays the Stellar Cyber 'Investigate' interface. On the left, a network diagram shows a central node '10.11.190.88' connected to several other nodes, including '10.11.191.138', 'test', '8ervteyfo08vshaocaaaw0tu...', '10.11.191.95', and 'wmic.exe'. Below this, a process tree shows the execution of '...Windows\System32\cmd.exe', which then branches into '...ndowe\System32\metah.exe', '...ndowe\System32\mstsc.exe', and '...hellv1.0\powershell.exe'. The 'powershell.exe' process is further linked to '195.243.214.107'. On the right, a list of 8 alerts is shown, including:

- 76 Score** Volume Shadow Copy Deletion via WMIC (7/1/21, 8:23 AM) - 20 minutes
- 93 Score** Internal SQL Dumpfile Execution (7/1/21, 8:03 AM) - 12 minutes
- 86 Score** Mimikatz Credential Dump (7/1/21, 7:51 AM) - 23 minutes
- 68 Score** PowerShell Remote Access

A circular callout on the right side of the interface compares 'Alerts' (represented by a 10x10 grid of dots) and 'Incidents' (represented by four large blue circles), illustrating the reduction in problem space.

✓ This problem space reduction leads to better, faster results – a breakthrough for defenders.