NS EDGE

The problem

Medium to large organizations have multiple sources of cyber data: endpoint agents, network monitoring, perimeter defenses, vulnerability scanners, etc.

These cyber data sources are uncorrelated, inconsistently formatted, and lack the enterprise-wide context to allow any meaningful estimation of risk. Instead, they're dumped into a central tool (Splunk, Elastic Stack, Snowflake, etc.)

DROWNING IN LOGS

Splunk indexes and joins data well, but scaling is **extraordinarily expensive**. Elastic scales somewhat better, but joins and contextualizes poorly. **Neither can handle the volume of network flow information.**

Without network contextualization, understanding residual risk is impossible. Each alert, report, or log file exists as a single point of data about an individual asset, providing no way to prioritize threats to the Enterprise as a whole.

The SolarWinds Orion product is used to manage the networks of many major companies/agencies. Hackers breached the SolarWinds' build systems, gained access to the webhooks triggered by the build process, and inserted compiled malware into Orion. SolarWinds failed to see the unusual network activity

SolarWinds

NO NETWORK CONTEXT

Secondary Victims

Once Orion delivered malware in a signed update to the victim companies, the malware used a complex DNS and HTTP Command and Control (C2) system to communicate with the attackers. Attackers masked the communication by naming their remote C2 servers with the hostnames of legitimate company assets. Without a map of how network traffic **should** look, the attack remained hidden for **many months.**