451 Research

Business Impact Brief

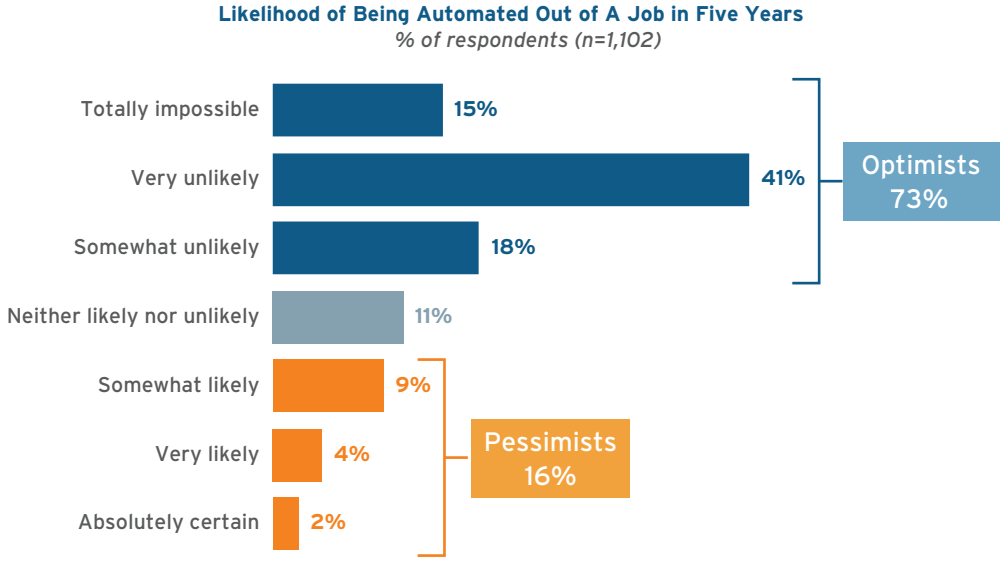
# Network Traffic Analytics Can Augment Security Operations Expertise

## The 451 Take

Network traffic analytics (NTA) based on machine learning has become proficient at recognizing active threats at each phase of an attack lifecycle, to the point that security operations staff increasingly utilize NTA insights when designing and implementing effective countermeasures. As enterprise networks become more complex and enterprise security is less able to control mobile endpoints, SOC teams leverage NTA in making better detection, response and prevention decisions to secure the business. The fear of machine learning architectures overriding security experts is dissipating, replaced with the vision that NTA provides essential guidance for security personnel who need to quickly identify compromised devices and workloads, the actions the cyberattacker is performing and how the threat spreads through the business. When it comes to network security, machine learning is augmenting the role of human security experts, as illustrated by the figure below.

### IT Job Security: The Machines Are Not Taking Over

Source: 451 Research, Digital Pulse: Workloads and Key Projects, 2018



# Business Impact Brief

## Business Impact

The normal course of action for a security investigation into a breached device or workload is to turn to the network to determine the current state of the attack, how the attack spread to reach the breached device or workload, and what other devices may be compromised, in order to decide on a corrective course of action and then evaluate the effectiveness of the security response. Security teams are also using attacker behavior detection in network traffic to initiate investigations in order to reduce process latency inherent in log data analysis or reacting to an external agency to report the breach. The positive business impacts of detecting security events, preventing damage and recovering from them include:

- Evidence of advanced threats are inevitably mingled in the network alongside authorized traffic, challenging security teams to design remediation steps that do not adversely affect legitimate business traffic. NTA reduces the risks of business disruption by enhancing security's ability to detect and respond to threats at each phase of the attack lifecycle, from botnet execution to command and control, reconnaissance, lateral movement and exfiltration phases.
- Security teams are besieged by alerts of devices, applications and user accounts misbehaving, with the result that valuable resources are expended investigating redundant alerts. Our qualitative research shows that using machine learning as a tool for security operations can reduce security workloads by a factor of roughly 25-30 by consolidating events.
- Understanding how threats propagate through the network enables security operations to improve both the mean time to detection and the mean time to remediation. The visibility afforded by NTA approaches measurably enhances security operations performance.
- Security personnel are responsible for detecting an attack and then coordinating with IT and networking organizations to remediate the issue. Having NTA automate monitoring of traffic patterns during the attack and after incident responses enables security to independently assess the effectiveness of remediation decisions, confidently close job tickets and continuously learn how to make the business more resilient to the next threat.
- Business revenue and reputation suffer from breach disclosures, but research also shows that performance can be sapped by threats stealing compute cycles. In particular, cryptocurrency mining consumes extensive computing power to rebuild manifests. NTA helps protect enterprise application performance by detecting illicit crypto-mining and enables security personnel to remove unauthorized blockchain botnet computations from networked resources.
- A security strategy that embraces NTA enables security services without impeding the progress of IT transformation efforts such as shifting to cloud-hosted servers, mobile user apps or Internet of Things devices without embedded security capabilities. Utilizing NTA as a tool allows security staff to protect the business by detecting threats and coordinating responses without overly burdening IT or its users.

## Looking Ahead

The promise of network traffic analytics is that it is the one security technology that can give security personnel end-to-end insight into all phases of cyberattacks, and can later confirm the effectiveness of remediation actions. Security personnel are executing a security strategy of using attacker behavior detections from NTA to augment log data analysis by feeding the SOC with information of active threats and feedback on remediation progress. The strategy of arming security personnel with the detection and intelligence capabilities of NTA to make better security decisions is gaining traction with enterprise security teams.

VECTRA®

*Click here to listen to the webcast* featuring Sean O'Connor, CISO at Worcester Polytechnic Institute, and Eric Ogren, Senior Security Analyst at 451 Research, to learn how AI is augmenting the security analyst workload and improving incident investigation when cyberattacks occur.