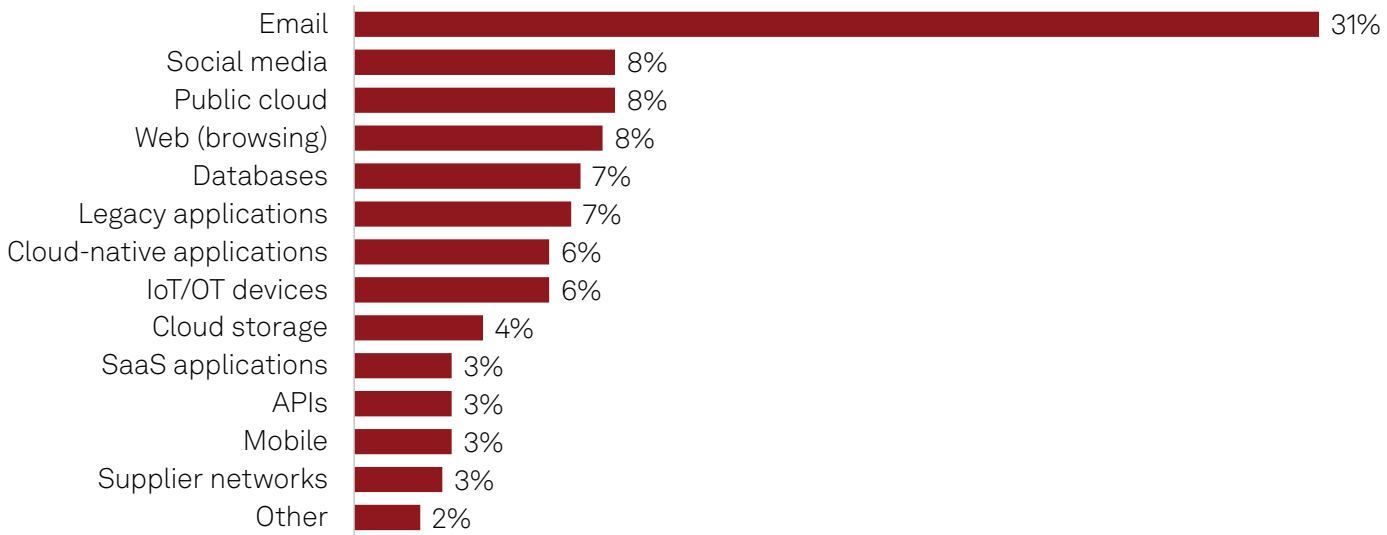
S&P Global
Market Intelligence
451 Research
Business Impact Brief

Attack analytics: Improving security effectiveness through direct integration in threat detection, investigation and response

The Take

Malware and malicious content such as credential phishing messages remain among the most successful tactics for cyberattacks — so much so that the vectors for these attacks are among the top security concerns for organizations of all sizes. Respondents to 451 Research's Voice of the Enterprise: Information Security, Organizational Behavior 2023 survey cite email as a source of security threats at nearly four times the rate of any other environment (see figure below), not least because it is used to deliver malicious content into organizations to compromise high-value data and IT assets.

Malicious content entering the organization is a top concern, as evidenced by the priority given to email threats – a primary means for delivering attacks



Q. When it comes to data security, which one of the following do you think poses the greatest security threat to your organization?
Base: All respondents, abbreviated fielding (n=290).
Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Behavior 2023.

Survey respondents notably emphasize approaches that defend against malicious content. Preventing malware from loading or executing is the top-ranked capability for endpoint security in our Voice of the Enterprise: Information Security, Endpoint Security 2023 study. Prevention of malicious intrusions is a primary objective of network security infrastructure.

What may be less evident is the potential for gaps within and between these silos of defense. If security approaches don't have the ability to coordinate detection across network, endpoint, content and human activity, attackers could discover and leverage gaps in security posture. Comprehensive threat detection, investigation and response systems that help close these gaps and detect threats in malicious content directly can improve not only defense but also the ability to act upon detection.

S&P Global
Market Intelligence

451 Research
Business Impact Brief

When threat detection, investigation and response systems that anchor the security operations center (SOC) directly incorporate the analysis of malicious content, they can have even greater impact. Analysis and detection can be more rapid, accurate and detailed, supporting more effective response — a critical factor when minutes count.

Business impact

Security teams are overwhelmed with data. Attack analytics integrated directly into detection, investigation and response systems can cut through noise and accelerate effectiveness. Without tools to refine input, identify and act on the highest-priority threats quickly, organizations can become overwhelmed by the sheer volume of security data. This volume has grown steadily, with alarming consequences. In 2023, for the first time in our survey research, the majority of respondents said they cannot address more than 50% of security alerts in a typical day. It is, therefore, imperative that organizations apply the most effective tools to identify the most significant threats in a vast volume of data. Attack analytics integrated directly into detection, investigation and response systems can be a key enabler for calling out the highest-priority issues.

With attack detection, time is of the essence. Malicious content can go to work as soon as it enters an organization. Ransomware is a prime example of an attack type that can wreak havoc within minutes. By the time traditional systems that correlate findings reach the SOC, significant damage may already have been done. Integration of malicious content analysis directly into detection, investigation and response systems in the SOC can significantly reduce time to detect and respond, helping to mitigate serious damage or prevent it altogether.

Attack analytics deployed directly in threat detection, investigation and response systems can improve correlation and close visibility gaps between silos. Various security technology silos offer their own approaches to analyzing and detecting malicious content such as malware or credential phishing attacks. However, correlating evidence across these silos introduces the potential for latency in identifying high-priority threats. A critical aspect of this correlation is delivering the context of an event to analysts and response systems; this context is necessary to triage and prioritize the nature and urgency of response. Attack analytics integrated directly into threat detection, investigation and response systems at the heart of security operations can provide faster detection at the "tip of the spear," driving more immediate response while additional evidence is gathered and correlated to provide richer context from telemetry sources.

Looking ahead

The acceleration of high-impact threat analysis and detection will continue to drive the evolution of detection and response technology. Because this functionality is at the heart of security operations, attack analytics will become increasingly integrated into security platforms.

As technology such as AI increasingly influences the direction of SecOps tech to help relieve overburdened staff and apply the benefits of compute at scale to threat detection, it will need access to centralized evidence to perform most effectively. But this is far from the only application of AI that SOC analysts can expect. Adversaries, too, recognize its potential and will use AI to accelerate the development of attacks such as custom malware and more credible phishing campaigns. These are among the factors that will drive attack analytics closer to the center of security operations and into the data-centric platforms on which this discipline depends.