

KROLL

Q1 2022

Threat Landscape:

Threat Actors Target Email
for Access and Extortion



Q1 2022 Threat Landscape: Threat Actors Target Email for Access and Extortion

Authors



Laurie Iacono



Keith Wojcieszek



George Glass

In Q1 2022, Kroll observed a 54% increase in phishing attacks being used for initial access in comparison with Q4 2021. Email compromise and ransomware were the two most common threat incident types, highlighting the integral part played by end users in the intrusion lifecycle.

Kroll continues to observe widely-publicized vulnerabilities such as ProxyShell and Log4J being used as pivot points for attackers to access and compromise systems through approaches such as business email compromise (BEC) and cryptominers. In Q1 2022, Kroll observed these vulnerabilities being leveraged by multiple different ransomware groups for initial access into systems. In the same quarter, Kroll also observed an increase in attacks related to Emotet and IcedID malware.

While the proportion of ransomware incidents slipped by 20% from the last quarter, cybercriminals capitalized on other methods to extort victims, such as the large-scale data theft by groups like Lapsus\$, and a unique twist on BEC that led to significant extortion demands.

Q1 2022 Threat Timeline

- Jan 14** ● **REvil Arrests in Russia:** The Russian Federal Security Service (FSB) announces the **shutdown of the REvil ransomware gang**, with the arrests of dozens of individuals associated with ransomware distribution and the seizure of cryptocurrency wallets, computers, cars and more than 426 million rubles (\$600,000 USD).
- Feb 14** ● **The War in Ukraine:** The United States Cybersecurity & Infrastructure Security Agency (CISA) advises all organizations to adopt a “**Shields Up**” approach in anticipation of cyberattacks related to tensions between Russia and Ukraine. On February 24, multiple military strikes in Ukraine escalates tensions into war. Cyber incidents observed in Q1 include distributed denial of service (DDoS) and malware variants with data-wiping capabilities (such as WhisperGate, Cyclops Blink, Hermetic Wiper and CaddyWiper). Organizations are encouraged to take proactive steps towards hardening their networks against potential cyberattacks.
- Feb 25** ● **Raid Forums Takedown:** An admin on the Raid Forums Telegram channel announces the **seizure of Raid Forums**, one of the longest-running English language clearnet cybercriminals forums. Raid Forums was notable for its large stable of threat actors, which included everything from free hacking tools to stolen databases with millions of records.
- Feb 28** ● **Conti Leaks:** A Twitter account with the handle @ContiLeaks dumps a **large dataset** connected to the infamous ransomware gang, including 60,000 chat messages, source codes and internal documents. A subsequent review of the materials provided what is believed to be the most in-depth insight into the inner workings of a ransomware gang to date.
- Mar 22** ● **Lapsus\$ Extortion Spree:** Microsoft publishes initial access methods for Lapsus\$ (aka **DEV-0537**), which attempted to extort multiple large security and technology firms in Q1. The group, which frequently publicizes victims on their Telegram channel, targets companies via credentials stolen through password stealer malware like Redline, credentials purchased on underground markets, insider solicitation and SIM swapping.

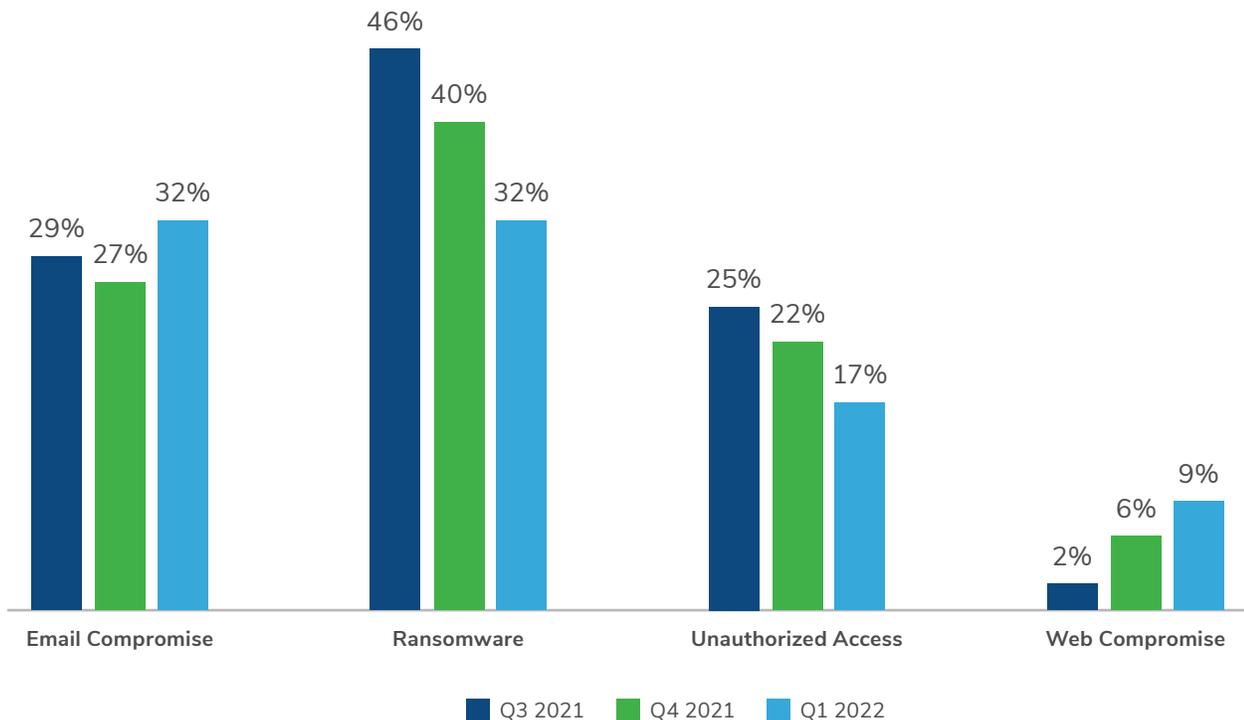
Threat Incidents: Email Compromise Rises, Ransomware Ebbs

While email compromise showed an increase of 19% from Q4, ransomware incidents trended down. Overall, ransomware activity in the first quarter of 2022 was down nearly 30% from Q3 2021.

As discussed in [previous Kroll reports](#), substantial international law enforcement operations at the end of 2021 disrupted many high-profile ransomware groups, such as REvil, while others, like BlackMatter, voluntarily announced an end to their operations due to pressure from the authorities. In the first month of 2022, additional REvil affiliates were arrested by Russian authorities. While these coordinated disruptions may have led to a temporary downturn in ransomware activity, Kroll observed an uptick in such incidents in March 2022, indicating the regrouping and rebranding of ransomware gangs as new variants like QuantumLocker and Dark Angel increased activity.

Web compromise continues to experience a gradual rise as significant vulnerabilities like Log4J and SpringShell make it easier for cybercriminals to exploit web applications.

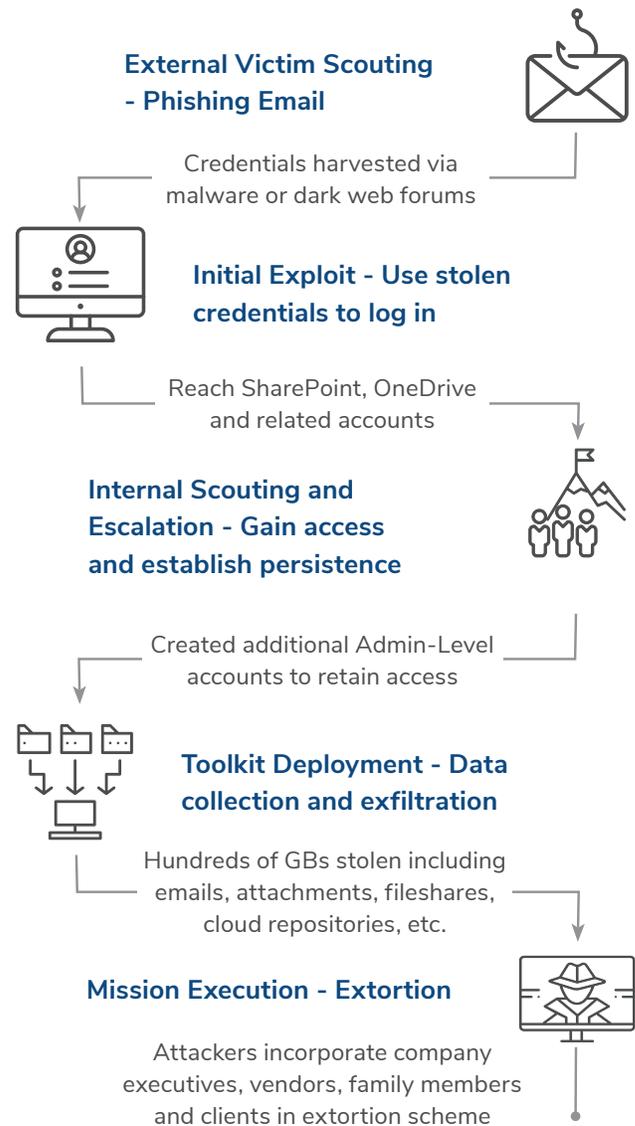
Most Popular Threat Incident Types - Past Three Quarters



Case Study: Email Compromise Leads to Extortion

Since mid-2021, Kroll has observed an ongoing trend of email compromises followed by attempts to financially extort individuals or organizations. In Q1, one such case started with a phishing email targeting IT departments. Once an end user clicked on the link to enter their log-in credentials, global admin credentials were harvested. Threat actors later used those credentials to gain access into the system and take over multiple email accounts belonging to IT staff and C-level employees. Due to their persistence on the network, the actors were also able to download data such as attachments and links to internal OneDrive and SharePoint instances.

Once the actors had left a ransom note on the system demanding a payment to end the attack, they began using multiple different methods to contact the compromised account holders, such as text message and email. In some cases, the actors took over social media accounts associated with the employees as a means to further pressure victims into meeting their ransom demands.

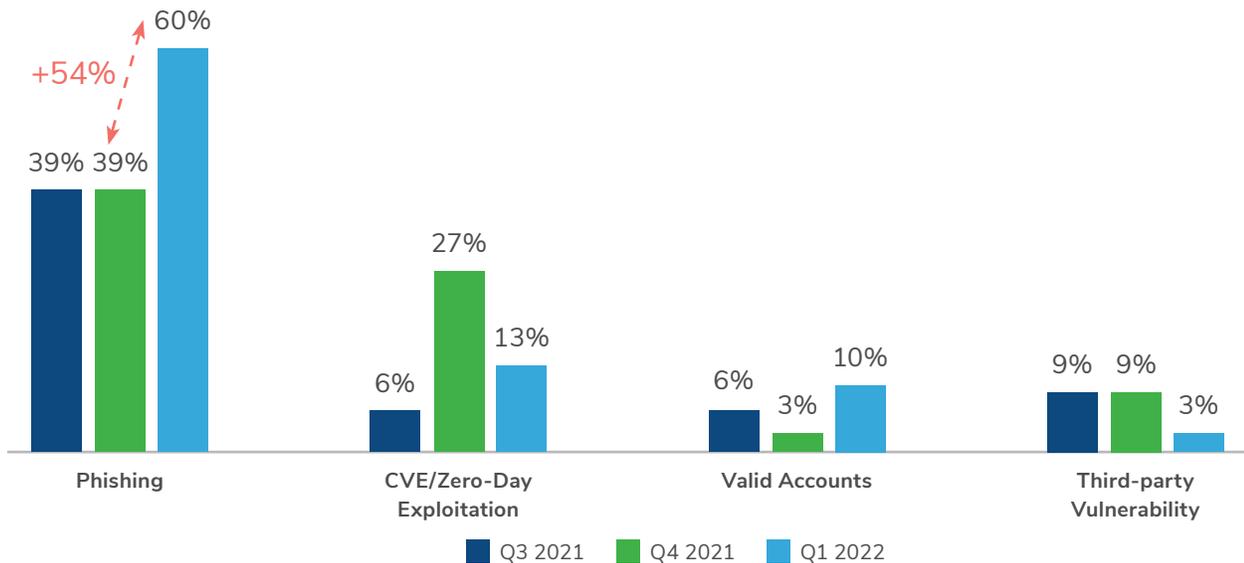


“ While these methods mirror the pressure tactics used by ransomware gangs, they are less sophisticated and easier to launch ”

— Jaycee Roth, Associate Managing Director,
Cyber Risk, Kroll

Rise in Phishing Lures for Initial Access: Emotet and IcedID

Most Popular Initial Access Methods - Past Three Quarters



In Q1, incidences of phishing for initial access soared by 54%. The increase in incidents of phishing for initial access may be driven by a rise in malspam campaigns by Emotet and IcedID. Emotet developers continued to experiment, as demonstrated by the rise of spam campaigns and the ongoing use of detection aversion techniques. Conti operators have also started using Emotet instead of TrickBot.

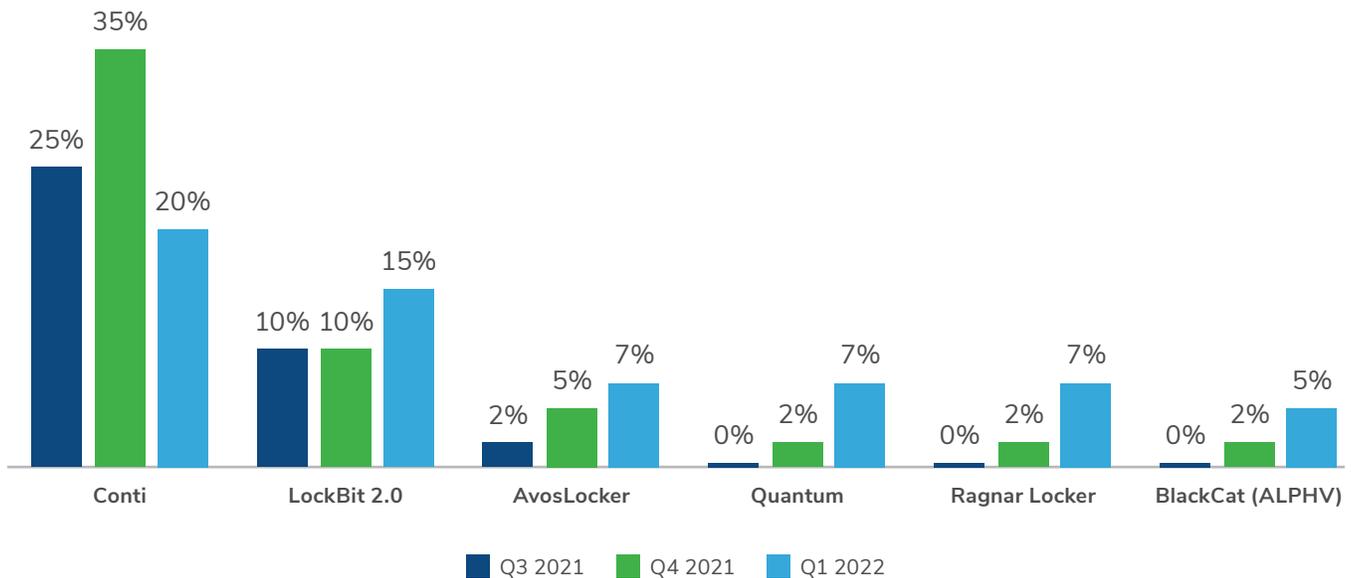
The use of BEC campaigns was highlighted in a case investigated by Kroll in which a reply chain attack between a third party and their victim led to an employee downloading an attached .zip file containing a malicious Excel document with macros which then launched PowerShell. This then contacted the Emotet download server and accessed an .ocx file. In this instance, the installation of Emotet was halted due to [Endpoint Detection and Response \(EDR\) technology detecting](#) a connection to a malicious Command and Control (C2) server, but the email was still shared internally, resulting in multiple infections.

In another attack investigated by Kroll, the victim received a phishing email in their personal email account, accessed on a corporate device. The legitimacy of the email was convincing due to a third-party compromise in January in which a list of users' emails were leaked. The victim clicked on malicious links embedded in the email, resulting in multiple redirects to a malicious .html file hosted on OneDrive.

Sometimes actors use a vulnerability to gain access, followed by a second-stage attack, such as email phishing, to spread malware. In another case investigated by Kroll, actors leveraged the ProxyShell vulnerability to access the network and once inside, they sent a widespread phishing campaign throughout the client organization. The phishing lures took the form of email thread hijacking attacks where the actors replied to a legacy thread with a .zip file that appeared to be an invoice and a unique passcode for extracting the files. Users that clicked on the link and entered the passcode opened the files which then downloaded IcedID onto their systems. Nearly two weeks later, QuantumLocker ransomware was deployed.

Ransomware Actors Take Advantage of Vulnerabilities

Most Popular Ransomware Variants - Past Three Quarters



Although ransomware activity saw a downturn in comparison with previous quarters, it still accounted for 32% of Kroll cases. Incidences of Conti attacks dropped by nearly 43% from Q4 2021 to Q1 2022, while the frequency of other variants, such as LockBit 2.0, AvosLocker, QuantumLocker and Ragnar Locker, grew.

In Q1, Kroll observed ransomware gangs using vulnerabilities such as ProxyShell and Log4j for initial access into networks. One of the ransomware variants on the rise, AvosLocker, has previously been observed both by Kroll and other entities as using ProxyShell for initial access.

In Q1, Kroll observed an AvosLocker incident that began with an attacker gaining access to a client’s VMWare Horizon instance via the [Log4j vulnerability](#). It is notable that initial access was made in December, just a few days after the mass publication of the vulnerability. Actors maintained persistence in the system via tools such as AnyDesk, NGROK and Cobalt Strike before deploying AvosLocker with PDQDeploy via a domain admin account nearly two months later. Dark Angel ransomware was also observed using Log4j for an initial foothold before ransomware deployment.

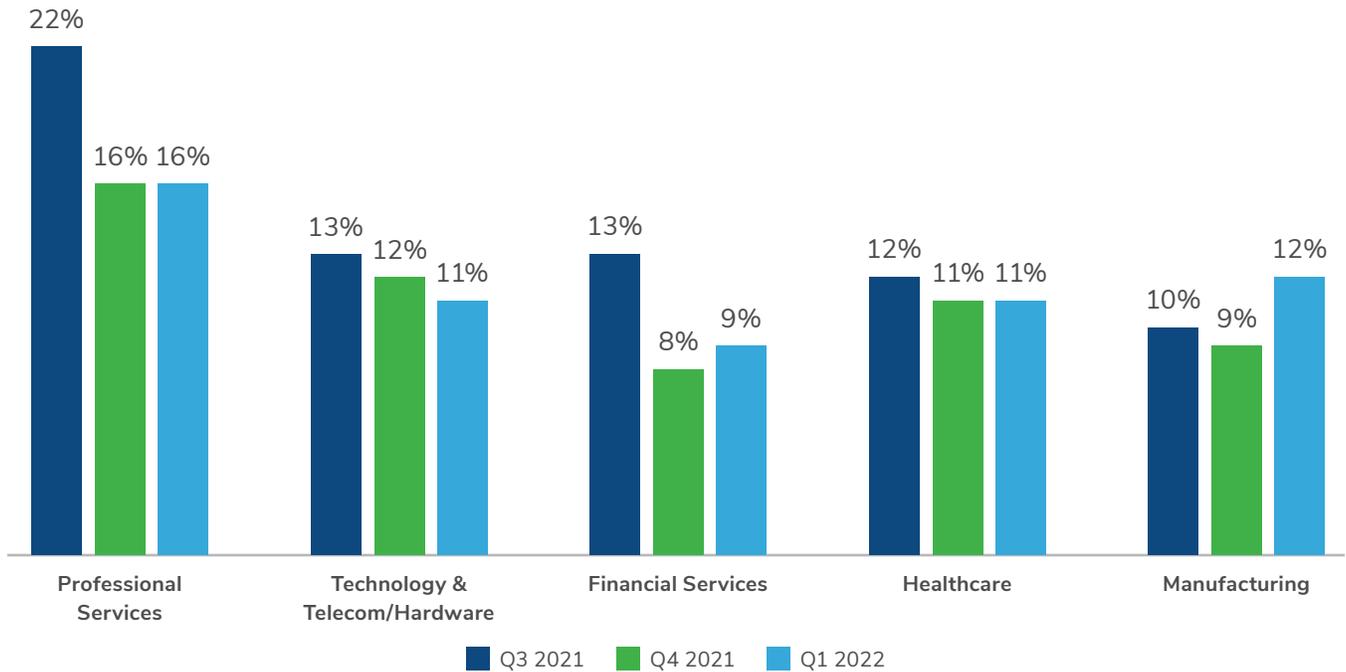


“ Attackers are continually scouring the internet looking for organizations that are unpatched for widely publicized vulnerabilities such as Microsoft Exchange servers and Java’s Log4j Remote Code Execution flaw ”

— Ron Rader, Senior Vice President, Cyber Risk, Kroll

Sector Analysis

Most Targeted Sectors - Past Three Quarters



Consistent with the previous two quarters, professional services was the most targeted sector across Kroll incident response cases. In Q1, Kroll observed a 33% increase in incidents impacting the manufacturing sector, with 68% of incidents being ransomware. Of those attacks, Conti was the most frequently observed ransomware variant impacting the sector. Kroll observed that targeting against manufacturing trended upward as the quarter drew to a close, with the bulk of incidents targeting that sector occurring in March.

Email Security Best Practices

To improve email hygiene, our experts recommend users to:



Archive emails every three to-six months if allowable for your business needs

This way, if a bad actor ever did infiltrate your email platform, they would only have access to the last three to six months of emails rather than years' worth of data.



Use secure methods for sharing information and credentials

When sending a document that may contain sensitive information, ensure that it is encrypted or password protected. If protecting with a password, make sure that the password is sent securely.



Manage privilege access and disable legacy protocols as needed

Admin accounts should not be used for anything outside of admin tasks and should not have an inbox tied to them. Legacy protocols such as IMAP/POP3 that cannot enforce multi-factor authentication (MFA) should be disabled.



Enable MFA

That being said, not all types of MFA are created equal. The best MFA would be to use a push code, ideally through something like Microsoft Authenticator. This makes it much harder to accidentally accept a push notification and allow a bad actor into your account, and also prevents issues such as SIM swapping.



Provide security training to identify and report suspicious activity

Invest in a robust security culture so employees know how to spot suspicious behaviors or social engineering attempts, and are empowered to raise concerns should mistakes be made (like clicking on a suspicious link).

From Established Methods to New Approaches

Activity observed in Q1 2022 highlights that the threat landscape remains complex, despite a decrease in ransomware incidents and the disruption and exposure of a number of key threat groups. 2022 is proving to be the year of attacker diversity, with actors exploiting new methods, such as email compromise, leading to extortion. This, and the ongoing events relating to the Russian war on Ukraine, mean that it is highly likely that conditions will remain challenging throughout 2022.

As with the previous quarter, the watchwords for organizations continues to be vigilance, detection and response. Security and risk leaders need actionable threat intel not only to prioritize key threats and vulnerabilities, but also to retain the ability to **quickly detect and confidently respond** to attacks.

Additional Resources



Three Tactics to Bypass Multi-factor Authentication in Microsoft 365



10 Essential Cyber Security Controls for Increased Resilience (and Better Cyber Insurance Coverage)

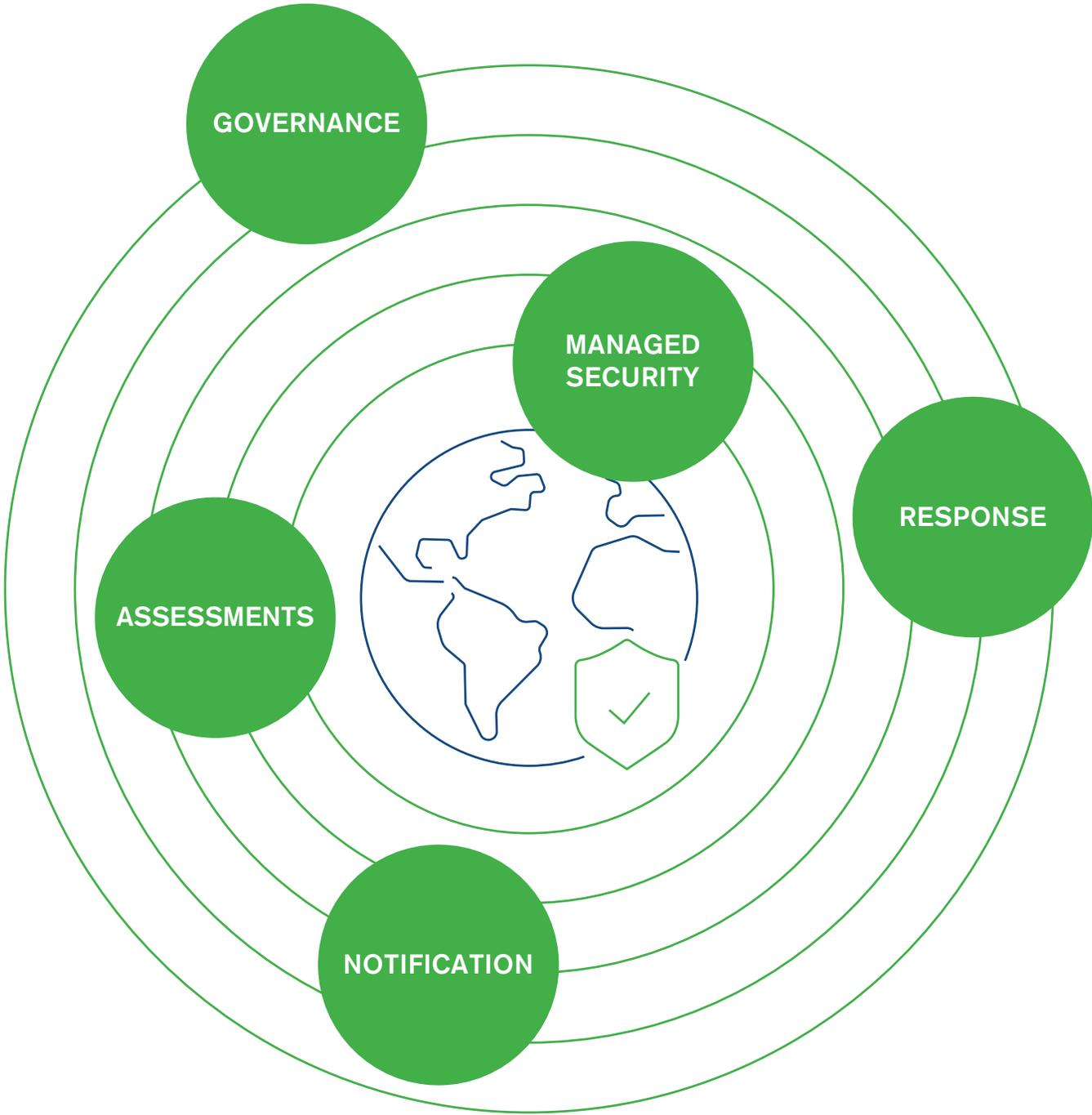


How Basic Cyber Hygiene Can Lead to More Effective Vulnerability Assessments



Kroll Responder Managed Detection and Response

Seamless Cyber Risk Solutions



See more at kroll.com/cyber



Browse the latest editions of Kroll's Quarterly Threat Landscape reports and subscribe for free at kroll.com/cyberblog

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With 5,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC), M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.