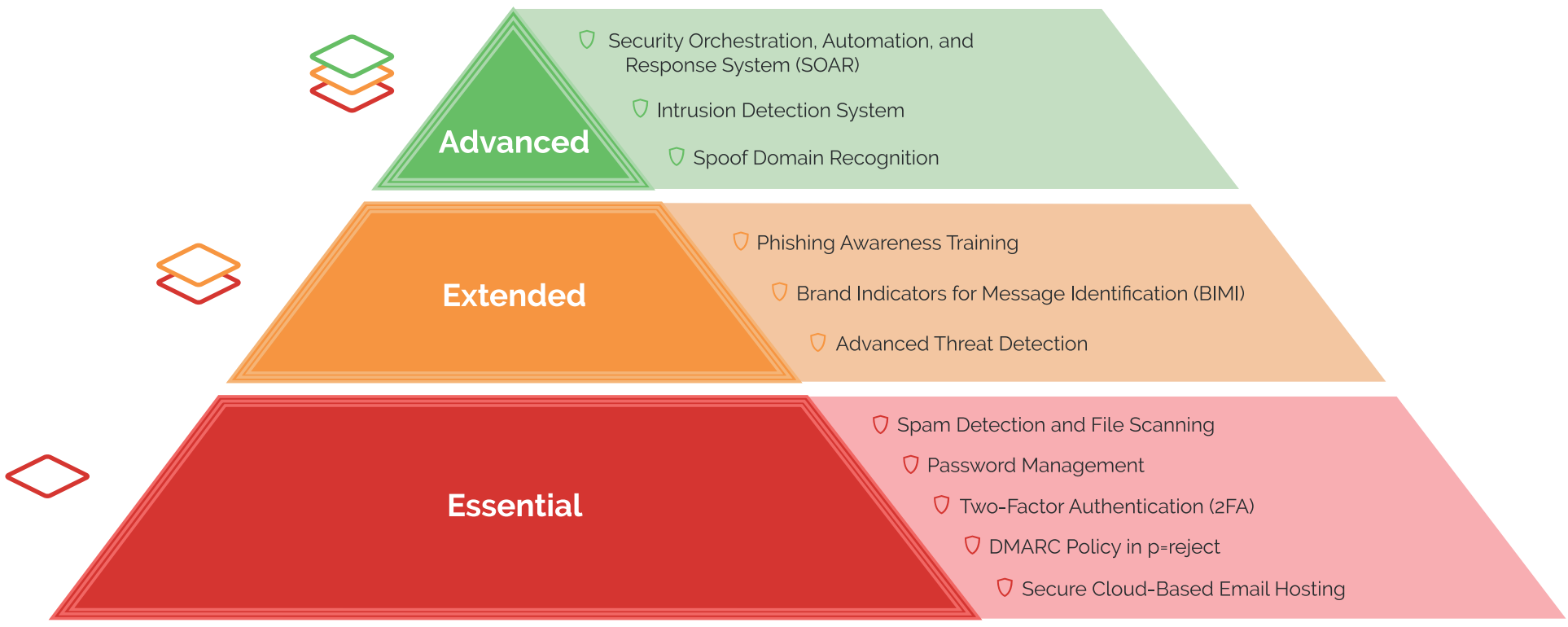
RED SIFT

The Hierarchy of Business Email Security Needs



Essential	
Secure Cloud-Based Email Hosting	Cloud-Based Email Hosting provides businesses with the tools needed to send, receive, and store messages. Vendors will provide security and maintenance too, for example, most modern solutions support 2FA and DMARC authentication along with good spam and virus filtering out of the box. Two of the most popular vendors are Microsoft O365 and Google Workspace.
DMARC Policy in p=reject	DMARC is a vital form of outbound protection which all businesses need to have in place. It's a globally standardized protocol which, when configured correctly in p=reject, protects your domain against exact impersonation. This means no one can use your domain to send fraudulent emails, reducing phishing and socially engineered attacks throughout your supply chain. DMARC also protects inbound mail, providing the mail system used by your organization supports it. By implementing it you not only protect your brand and business, but also your customers, employees, and anyone who interacts with you.
Two-Factor Authentication (2FA)	Two-Factor Authentication (2FA) is the practice of setting up an added layer of security to your logins. It is essential for your email security posture as it protects from account takeover, especially when passwords are reused and then leaked
Password Management	A Password Manager securely stores the passwords for your various accounts across the internet. While it's best practice not to reuse passwords, the logistics of managing these can be challenging. Until there's a more intuitive solution, a Password Manager can be a useful way to ensure your passwords are secure and accessible, but this isn't a substitute for 2FA.
Spam Detection and File Scanning	Spam Detection and File Scanning technology scans inbound emails for threats. There are a variety of products to choose from, but these are provided by most modern email providers such as Google and Microsoft, as well as more traditional SEG vendors too.

Extended	
Advanced Threat Detection	Advanced Threat Detection in email is a more intuitive approach to email security. Whereas an SEG or spam detector acts as a firewall, threat detection software detects problems within an email based on its content and sender, often using Artificial Intelligence to assess the email's DNA and notifying the recipient. It's essentially like having an expert in every email, letting you know whether the email is safe to interact with or not.
Brand Indicators for Message Identification (BIMI)	BIMI is a new protocol that allows registered logos to be displayed in the avatar slot of any DMARC authenticated emails a business sends. It's not a security protocol in itself, but it indicates DMARC has been correctly configured. Plus, its positive impact shown on recipient interaction suggests it pays for itself.
Phishing Awareness Training	Phishing Awareness Training educates employees to recognize the signs of phishing attacks, and how to report them. This can help to improve employee response to phishing attacks throughout your organization. However, this shouldn't be the groundwork of your security posture, as it can quickly become outdated and therefore expensive, due to additional costs and employee time.

Advanced	
Spoof Domain Recognition	Spoof Domain Recognition is a step up in email security. It actively scans the internet for cousin and lookalike domains and allows you to remove them, preventing reputational damage to your business. There's a fast-growing need for this as businesses look for ways to secure their domain perimeter against spoofing.
Intrusion Detection System	An Intrustion Detection System monitors threats, malicious activities, and violations of policy within your network. It's an additonal layer of domain perimieter protection which is key for larger enterprises.
Security Orchestration, Automation, and Response System (SOAR)	A SOAR system is an assortment of security software tools which collect threat data from different sources. Using both human and machine learning, the system then analyzes the data and automates appropriate responses to threats. This is valuable for organizations looking to automate and standardise repeated workflows at scale.