Cyber defense

Prepared By:
Kazim Ali Obad

Supervisor:

Anmar Mohammed
MOHAMMED .B. HASSAN

Contents

1. Prevention vs. Detection:

A popular debate within the InfoSec community revolves around a fundamental question: **Which is more critical prevention or detection?**

This is one of those discussions that comes up constantly in security teams. You walk into a SOC, you sit down with management, and somebody always asks: okay, are we a detection shop or a prevention shop? And the honest answer, as we are going to explore today, is that you cannot afford to be just one of them.

1.1 The Case for Prevention

Think about it this way. If you have a SOC analyst sitting there and a thousand alerts come in every single day phishing emails, suspicious logins, weird traffic what happens? The analyst gets overwhelmed. The team burns out. Important alerts get buried under noise. That is alert fatigue, and it is a real problem.

Now imagine you have strong **prevention measures** in place a properly configured Secure Email Gateway, solid firewall rules, network segmentation. Half of those thousand alerts never happen in the first place. Now your team is looking at 500 alerts, or maybe 150. Suddenly, they can actually focus. They can do real investigation work instead of just triaging noise all day.

That is the fundamental argument for prevention: it directly enhances the quality of your detection. If you prevent the common, low level stuff, your analysts get to focus on the threats that actually matter.

1.2 The Case for Detection

Now some people push back and say: look, breaches are inevitable. No matter how strong your prevention is, something is going to get through. And they are right. So if you have only invested in prevention and nothing slips past you great. But the moment something does slip through, and you have no detection capability? You are completely blind.

Detection gives you visibility. It tells you what is happening inside your environment. It lets you catch the attacker who already got in and is moving laterally through your network before they reach your crown jewels.

1.3 The Right Answer: Both, But in the Right Order

Prevention and detection are complementary one completes the other. You need detection to catch what prevention misses. But strong prevention makes your detection dramatically more effective.

2. Where Does the SOC Actually Spend Its Time?

Research has quantified this in a way that makes the argument very clear. Here is the breakdown of how SOC teams typically distribute their working hours:

SOC Activity	Time Spent
Investigation	46.9%
Response	26.6%
Prevention	26.5%

Nearly 47% of a SOC analyst's time goes into investigating threats after they have already happened. That is reactive work. That is expensive work. That is the kind of work that could often be avoided if the threat had been stopped earlier in the kill chain.

if you have a detection, what does that lead to? It leads to an investigation. And what does an investigation lead to? It leads to a response. So detection, investigation, and response are all chained together. That is roughly 73% of your SOC's time.

But if prevention had caught it in the first place? None of that chain happens. You save 75% of your SOC's time on that particular threat. That is why investing in prevention is not just a security decision it is a business decision.

3. A Practical CyberDefense Approach

There is no one size fits all answer in cybersecurity. What works perfectly for a bank will not necessarily work for a manufacturing company. What works for a thousand person enterprise will not work for a small business with three IT staff.

A good security approach must be:

- **Practical** applicable across different types of organizations
- **Easy to implement** you cannot require a ten person expert team to deploy
- **Cost effective** security budgets are real, and they are limited
- **Impactful** it should meaningfully improve your security posture
- **Disruptive to attackers** it should address root causes, not just symptoms

So the question becomes: where do you start? If you are building a security program from scratch, or you are trying to improve an existing one, **what is the single highest impact area you can address?**

The answer is almost always: **the email system.**

4. Why Email?

Email is the most widely used attack vector in existence today. This is not an opinion it is backed by research from multiple industry sources:

- 91% of targeted attacks involve spear phishing emails (TrendMicro)
- 95% of all state sponsored espionage attacks relied on phishing in some way (Verizon Data Breach Report)
- Phishing is still the number one attack vector in use today (IBM XForce, 2020)
- Email is the most commonly used attack vector for both opportunistic and targeted attacks (Gartner)

Why is email so attractive to attackers? There are eight key reasons:

1. **Ease of use:** everybody knows how to use email. No technical skill required on the attacker's side.
2. **Popularity:** every single organization has email. It is a universal attack surface.
3. **It targets the weakest link:** most end users lack basic security awareness. Even security professionals fall for phishing sometimes.
4. **Rewarding:** an attacker can send two thousand emails at once. If only one person clicks, the attack succeeds.

5. **Hard to block completely:** attackers can rotate domains constantly. Block one domain, they register a new one instantly.
6. **Cheap:** sending thousands of emails costs almost nothing, whether through bots or disposable servers.
7. **Organizations have weak email security:** because any mistake in securing email can break it for the whole business, and nobody wants to be the security person who took down email. So teams are cautious, and gaps remain.
8. **Highly reusable:** once an attacker compromises a user account, they can use that trusted identity to phish other users internally including privileged ones like admins and executives.

A 2010 Symantec study found that **approximately 85% of all emails were spam.** If your organization receives 1,000 emails a day, that is 850 emails that are noise. If your SOC is triaging those manually, that is an enormous waste of skilled human resources. But if a properly configured Secure Email Gateway blocks those 850 before they even reach your users, your team can focus entirely on the 150 that made it through and do it much more effectively.

5. Email Attack Vectors

To defend against email attacks, we need to understand how they work. Regardless of the specific technique an attacker uses, they must rely on one of three root techniques:

- **Email Spoofing:** faking who the email is from
- **Malicious Attachments:** embedding malware or payloads in files
- **Embedded URLs:** tricking users into clicking malicious links

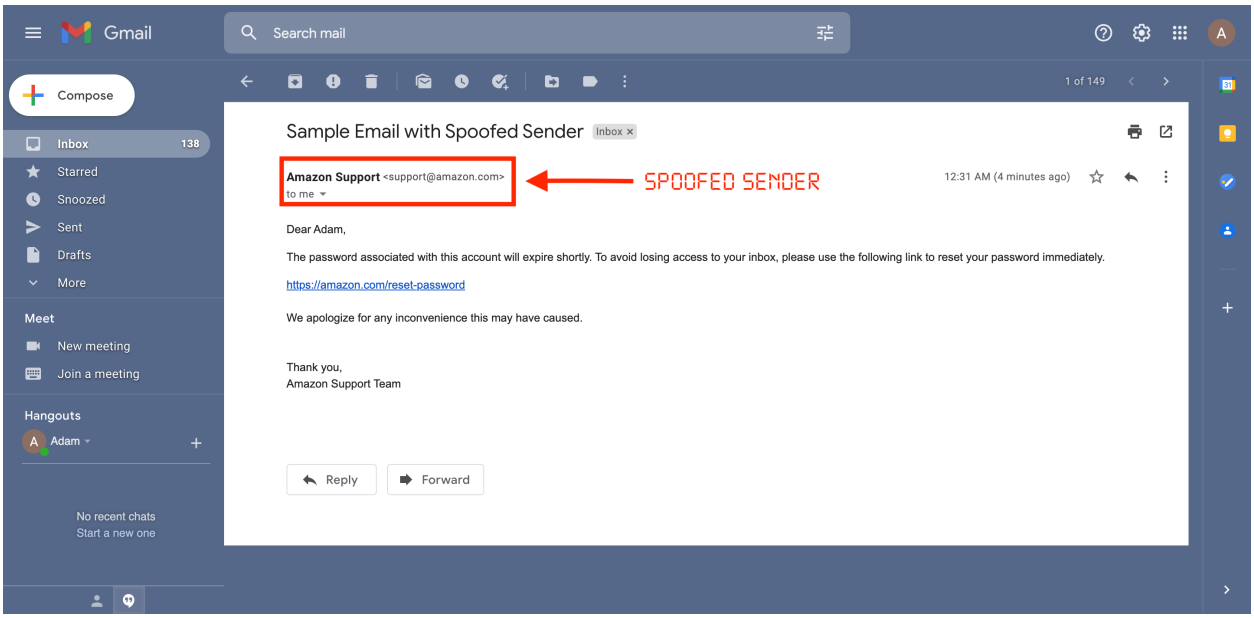
FireEye research found that **86% of email attacks are malwareless** meaning they do not rely on executable malware at all. They are pure impersonation, phishing, and social engineering. That makes spoofing the dominant technique.

5.1 Email Spoofing

Email spoofing is the manipulation of email headers to fake what the recipient sees in the 'From' field. It works because the SMTP protocol the protocol that underlies all email was designed without authentication in mind. There is nothing in SMTP that prevents you from claiming to be anyone you want.

Here is a real example of how this plays out. Imagine your company has an HR department. An attacker compromises a lowlevel account let's say an HR assistant named Ahmed. Now, using Ahmed's account, the attacker sends an email to the CEO. The CEO sees it is from Ahmed in HR, someone he recognizes. He opens the attachment. Suddenly the attacker has access at the executive level. That is the power of spoofing combined with trust.

Another common example: you receive an email claiming to be from Amazon Support, telling you your password is expiring and you need to reset it immediately. You click the link, enter your credentials on what looks like Amazon's login page, and the attacker now has your password. The following screenshot is for an email I sent to a Gmail inbox using a free online spoofing service https://emkei.cz/. The email looked completely legitimate because the sender address was spoofed to show support@amazon.com.



Email spoofing is easy to execute because **SMTP lacks builtin authentication.** A quick Google search for 'Email Spoof Test' returns multiple free tools that let anyone send emails as anyone else. The solution is implementing proper authentication protocols primarily **DMARC, DKIM, and SPF** https://github.com/chenjj/espoofer/

6. SPF Sender Policy Framework

SPF (Sender Policy Framework) is an email authentication protocol that allows a domain owner to specify which mail servers are authorized to send email on their behalf. This information is published as a DNS TXT record.

When a receiving mail server gets an email, it checks the SPF record of the sender's domain. If the email came from a server that is listed as authorized, it passes. If it came from a server that is not listed, it fails and depending on the policy, may be rejected.

6.1 What Does an SPF Record Contain?

An SPF record contains two key things:

- A list of mail servers authorized to send email on behalf of the domain
- Instructions for what to do when an email arrives from an unauthorized server

6.2 How to Check an SPF Record

To look up the SPF record for any domain, use this command:

```
dig <domain> TXT | grep spf
```

For example:

```
dig earthlink.iq TXT | grep spf
```

This returns something like:

```
v=spf1 include:_spf.google.com -all
```

Let's break that down:

- v=spf1 declares this is an SPF record
- include:_spf.google.com Google's mail servers are authorized to send on behalf of this domain
- -all any server NOT listed should be rejected (hard fail)

```
┌──(kali㉿kali)-[~]
└─$ dig earthlink.iq TXT | grep spf
earthlink.iq.           5       IN      TXT     "v=spf1 mx include:_spf.getresponse.com include:serve
rs.mcsv.net a:stegw1.elcld.net a:exmta.elcld.com a:earthlink-iq.mail.protection.outlook.com include:s
pf.protection.outlook.com include:_spf.createsend.com a:mailgw1.earthlink.iq a:mailgw2.earthlink.iq a
:" "mailgw3.earthlink.iq -all"
```

6.3 SPF Mechanisms

Mechanism	Example	Meaning
ip4	v=spf1 ip4:192.168.1.1/24	Authorizes a specific IP range
a	v=spf1 a:example.com	Authorizes IPs from the A record
mx	v=spf1 mx:example.com	Authorizes IPs from the MX record
include	v=spf1 include:_spf.domain.com	Pulls in another domain's SPF record
all	v=spf1 all	Matches all IPs (catchall)

6.4 SPF Qualifiers

Qualifier	Name	Action
+	Pass	Accept the email
-	Fail	Reject the email
~	SoftFail	Mark as spam/junk
?	Neutral	Accept but no opinion

SPF records are evaluated from left to right, stopping as soon as a match is found. The 'all' mechanism always comes last and acts as the catchall rule.

6.5 SPF Result Codes

Result	Meaning
None	No SPF record exists for the domain
Pass	The sender's IP is authorized
Neutral	SPF makes no claim about the IP
SoftFail	IP is not authorized but not explicitly blocked
Fail	IP is not authorized likely a spoofed email
TempError	Temporary DNS issue (e.g., timeout)
PermError	Permanent SPF configuration error

6.6 How SPF Works in Practice

Here is the complete flow when SPF is in effect:

- A sender at omar@sendercompany.com sends an email to oways@receivingcompany.com
- The receiving mail server checks if SPF verification is enabled
- If enabled, it looks up sendercompany.com's SPF DNS TXT record
- It compares the sending server's IP against the authorized list in the record
- If the IP matches, the email passes. If not, the SPF policy determines whether to reject, flag, or accept it.

6.7 SPF Limitations and Best Practices

- SPF only works if the receiving mail server enforces it if enforcement is disabled, spoofed emails still get through
- SPF has a DNS lookup limit of 10 queries exceed this and SPF will fail
- Simplify SPF records by using direct IP addresses (ip4) rather than multiple nested include statements
- Each organization is responsible for activating SPF verification on their incoming mail gateway the receiving side controls enforcement regardless of the sender's SPF policy

6.8 SPF Implementation Steps

9. Identify all domains your organization uses to send email
10. Collect the IP addresses of all authorized mail servers
11. Create the SPF record manually or using a tool like spfwizard.net
12. Publish the SPF record in your DNS TXT records
13. Test the SPF record to confirm it is working correctly

7. DKIM DomainKeys Identified Mail

DKIM (DomainKeys Identified Mail) is an email authentication system that uses cryptographic signatures to verify two things: (1) that an email genuinely comes from the domain it claims to be from, and (2) that the email content has not been altered in transit.

Think of DKIM as a digital stamp. When your mail server sends an email, it stamps it with a signature that only it could have created. When the receiving server gets that email, it can verify the stamp is legitimate and that nobody tampered with the message along the way.

7.1 Why Do We Need DKIM?

SPF tells you which servers are allowed to send email for a domain. But SPF has a limitation: it checks the envelope sender, not necessarily the header 'From' address that users actually see. DKIM fills this gap by verifying the content and identity of the message itself, not just its origin server.

- Spam and Phishing Protection DKIM helps receiving servers confirm an email is genuinely from the claimed sender
- Email Integrity ensures the message content was not modified after it was signed

7.2 Public and Private Keys

DKIM relies on publickey cryptography:

- Private Key stored securely on the sending mail server. Used to sign outgoing emails. This is the secret stamp.
- Public Key published as a DNS TXT record under the domain. Available to anyone. Used by receiving servers to verify the signature.

If an email is signed with the private key, only the matching public key can verify that signature. If someone alters the email's content or forges the signature, verification fails.

7.3 The DKIM Process Step by Step

Let's say Omar at sendercompany.com sends an email to Oways at receivercompany.com:

14. The sending server signs the email mail.sendercompany.com uses the private key to generate a unique DKIM signature for the message. That signature is embedded as a special header.
15. The receiving server checks DNS mail.receivercompany.com sees the DKIM signature in the header and looks up the public key from sendercompany.com's DNS records.
16. The signature is verified the receiver uses the public key to validate the signature. If it matches, the email is authentic and unaltered.
17. Delivery decision DKIM Pass means the email is likely delivered to the inbox. DKIM Fail means it may be sent to spam, blocked, or flagged depending on the receiver's policy.

7.4 DKIM vs SPF Complementary Roles

Protocol	What It Checks	How It Works
SPF	Which servers are allowed to send for a domain	Checks sender IP against DNS authorized list
DKIM	Whether the email was signed by the legitimate sender	Verifies cryptographic signature using DNS public key

In modern email security, both SPF and DKIM are deployed together. They cover different aspects of authentication and together form a strong foundation especially when combined with DMARC, which we will cover in the next lesson.

7.5 Why Multiple DKIM Records?

A domain typically has only one SPF record. But it can have multiple DKIM records one for each distinct sending service or server. For example:

- Your inhouse mail server (mail.yourdomain.com)
- A marketing email platform (mail.marketingservice.com)
- A CRM provider sending emails on your behalf

Each distinct sending service gets its own private/public key pair, and therefore its own DKIM record in DNS. This is better for security: if one key is compromised, you can revoke it without affecting the others.

7.6 The DKIM Selector

A selector is a small text string that identifies which DKIM key pair is being used. It is part of the DNS record path:

```
<selector>._domainkey.<yourdomain>
```

Examples from a real domain:

```
google._domainkey.cyberdefenders.org
s1._domainkey.cyberdefenders.org
newsletter._domainkey.cyberdefenders.org
```

Each record stores a different public key. The selector in the email header tells the receiving server exactly which public key to look up in DNS. This is how a domain can manage multiple active DKIM key pairs simultaneously.

7.7 DKIM Verification Results

Result	Meaning
Pass	Signature is valid email is authentic and unaltered
Fail / HardFail	Signature does not match possibly forged or altered
Neutral	Check could not be completed (e.g., malformed header)
None	No DKIM signature present in the email
TempError	Temporary error prevented validation (e.g., DNS timeout)
PermError	Permanent error missing or broken signature headers

7.8 DKIM Is Optional But Should Not Be

Both DKIM signing (on the sender side) and DKIM verification (on the receiver side) are optional configurations. A domain must choose to enable DKIM. A receiving server must choose to verify it.

In practice, any organization serious about email security should have DKIM enabled. The same goes for receiving servers if you are not verifying DKIM, you are leaving an authentication layer completely unused.

7.9 Configuring DKIM on Cisco ESA

To configure DKIM on a Cisco Email Security Appliance, the process follows these steps:

- Create DKIM key pairs navigate to Mail Policies > Domain Keys > Signing Keys > Add Key. Choose a key name and size (2048bit is recommended). The system generates the private and public key pair.
- Publish the public key the public key generated must be added to your domain's DNS records at the correct selector path.
- Create a signing profile associate the key with your domain so the mail gateway knows which key to use when signing outgoing messages.
- Enable DKIM verification for incoming email, navigate to Mail Policies > Mail Flow Policies and enable DKIM verification on the accepted policy.

8. Key Takeaways

- Prevention and detection are not competing priorities they are complementary. Strong prevention makes detection more effective.
- SOC teams spend approximately 73% of their time on investigation and response activities that largely happen because something got through prevention. Investing in prevention directly reduces this burden.
- Email is the number one attack vector in cybersecurity today, responsible for 91% of targeted attacks. It is the highest impact area to address.
- Email spoofing is widespread and easy because SMTP was not designed with authentication. Organizations must implement authentication frameworks.
- SPF defines which mail servers are authorized to send email on behalf of your domain and publishes this as a DNS TXT record.
- DKIM uses cryptographic signatures to verify both the sender's identity and that the message was not altered in transit.
- Both SPF and DKIM play complementary roles and should be deployed together. DMARC builds on top of both to enforce policy and provide reporting covered in the next lesson.