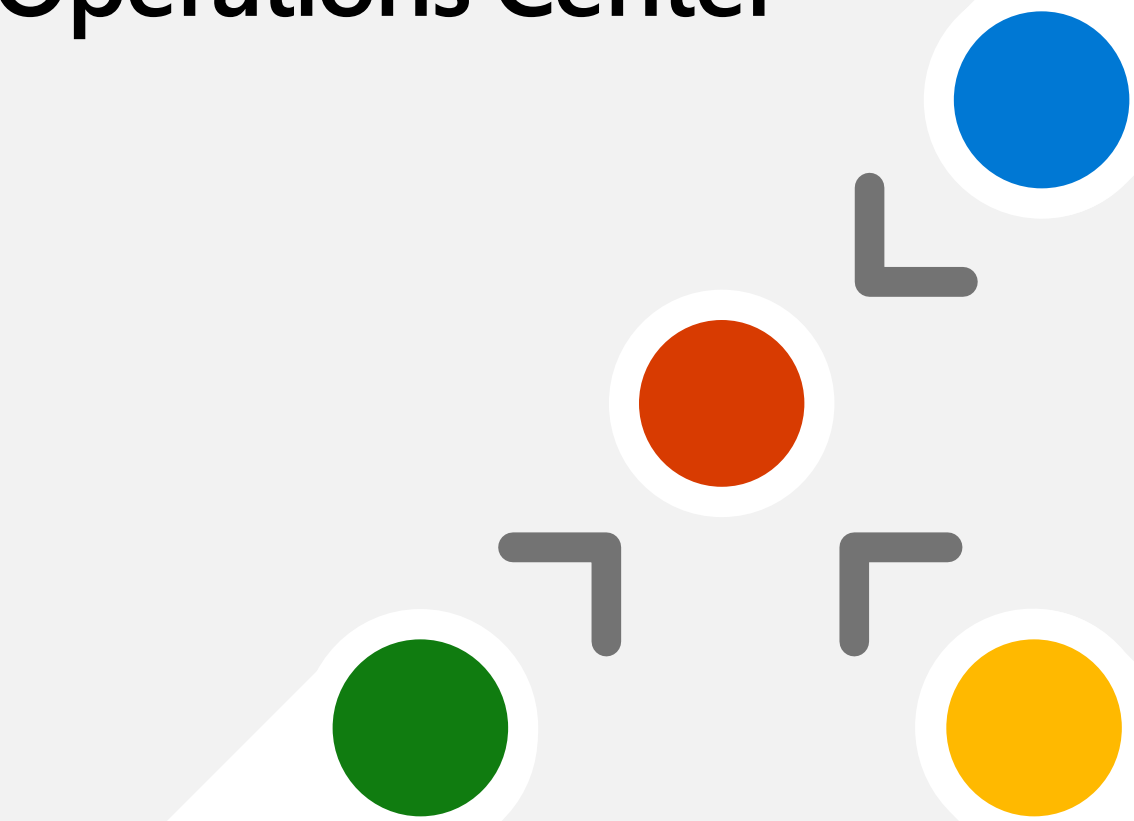
Microsoft Security

Modern Security Operations:

Best Practices and Lessons Learned from the Microsoft Cyber Defense Operations Center



Contents

Security operations overview

As security professionals, you know the threats to your environment are evolving and accelerating.

Cyberattacks today are organized criminal endeavors. Cybercriminals share information with each other about what works and about vulnerabilities. They work to evolve their techniques as the technology evolves.

Cyberattacks are more than just an evolving technological threat. Trends like ransomware-as-a-service (RaaS) are part of an increasingly industrialized and sophisticated economy, where attackers who may not have the skill or technical wherewithal to develop their own tools can now manage ready-made penetration testing and sysadmin tools to perform attacks. These lower-level criminals can also simply buy network access from a more sophisticated criminal group that has already breached a perimeter, and with a successful ransomware and extortion attack, both parties profit.

As attackers continue to innovate, it's imperative that security teams work to continually modernize their security operations to stay prepared for adversaries.

This means addressing your technology stack to ensure you have protection and visibility across all attack vectors. But it also means assessing the processes of your team—is it able to protect, detect, and respond to real threats quickly and accurately, or are team members overwhelmed with too much signal, and chasing false positives?

We've created this guide to help you modernize your security operations and protect your organization in an evolving threat landscape.

Lessons learned from the Microsoft SOC

The learnings and best practices presented here are derived from conversations with Microsoft customers and from our own experience developing and maturing our Security Operations practices at Microsoft.

While it may seem surprising to some, the Microsoft Corporate IT SOC protects a cross-platform environment with a significant population of Windows, Linux, and Macs running Microsoft and non-Microsoft software. Previously, this SOC operated a traditional SOC model similar to what we see in most organizations, and we faced the same set of natural challenges with the model:

- **Event volume**—High volume and growth (on the scale of 20 billion events a day currently) exceeded the capacity of the on-premises SIEM to handle it.
- **Analyst overload**—The static rulesets generated excessive amounts of false positive alerts that led to alert fatigue.
- **Poor investigation workflow**—Investigation of events using the traditional on-premises SIEM was clunky and required manual queries and manual switching to different tools.

Our team knows what you're dealing with because we've been there. Throughout this guide, we'll share with you best practices and key lessons we've learned as we've worked to modernize our own security operations at Microsoft for both ourselves and our customers.

The Microsoft Corporate IT SOC protects a cross-platform environment with a significant population of Windows, Linux, and Macs running Microsoft and non-Microsoft software.

The role of security operations

Security operations maintains and restores the security assurances of the system as live adversaries attack it. Its main functions are described in the NIST Cybersecurity Framework and include:

- **Detect**
- **Respond**
- **Recover**

- **Detect**—Security operations must detect the presence of adversaries in the system that are incented to stay hidden in most cases, as this allows them to achieve their objectives unimpeded. This can take the form of reacting to an alert of suspicious activity or proactively hunting for anomalous events in the enterprise activity logs.

- **Respond**—Upon detection of potential adversary action or campaign, security operations must rapidly investigate to identify whether it is an actual attack (true positive) or a false alarm (false positive) and then enumerate the scope and goal of the adversary operation.

- **Recover**—The goal of security operations is to preserve or restore the security assurances (confidentiality, integrity, availability) of business services during and after an attack.

Effectiveness in these areas reduces risk by limiting how much time and access attackers have in the organization. This ultimately increases the attacker's cost and decreases the benefit, which damages their return on investment (ROI) and motivation for attacking your organization. Additionally, security operations teams drive overall security maturity.

Everything in your security operations should be oriented toward limiting the time and access attackers can gain to the organization's assets in an attack to mitigate business risk.

Security operations is also often an advocate for increasing security maturity across the organization because any weaknesses in security posture can lead to incidents that have to be handled by security operations.

Business relationships

Building and maintaining relationships with the business side of the organization improves the effectiveness of the security team. This includes making an effort to understand business strategies and involving leaders in ways that help them understand what your team does to prevent and mitigate attacks.

At Microsoft, we focus on four primary functional integration points with the business:

- **Business context**
- **Joint practice exercises**
- **Major incidents updates**
- **Business intelligence**

- **Business context**—Understanding what is most important to the organization helps the team apply that context to fluid real-time security situations. What would have the most negative impact on the business? Downtime of critical systems? A loss of reputation and customer trust? Disclosure of sensitive data? Tampering with critical data or systems? We've learned it's critical that key security operations leaders and staff understand this context as they wade through the continuous flood of information and then triage incidents and prioritize their time, attention, and effort.

- **Joint practice exercises**—Practicing response to major incidents together builds the muscle memory and relationships that are critical to fast and effective decision-making in the high pressure of real incidents, reducing organizational risk. This practice also reduces risk by exposing gaps and assumptions in the process that can be fixed prior to a real incident.

- **Major incidents updates**—Providing updates to business stakeholders for major incidents as they happen allows business leaders to understand their risk and take both proactive and reactive steps to manage that risk.

- **Business intelligence**—Sharing discoveries of unexpected targets with business leaders may trigger insights such as outside awareness of a secret business initiative, or the relative value of an overlooked dataset.

How does security operations work with the other teams in the organization, especially the business side of it?

Your team should be aware of key business priorities so that they can identify the critical assets and set security priorities accordingly. This allows you to focus on the most critical assets and put the necessary defense systems, policies, and automated investigation around them, so they are aligned to the business team.

Knowing who the key stakeholders are and informing them immediately allows the whole business to respond, including:

- **Security operations**
- **Operations**
- **Logistics**
- **PR/communications**
- **Business leadership**

One of the best ways to build the necessary relationships with business is tabletop exercises for practicing incident response. During the tabletop exercises, leadership teams—as well as incident response stakeholders—all take part. This allows security and business stakeholders to build relationships. The two functions will learn how to work best together so that when there's an incident, everybody knows who the other parties are, how to engage, and what to do to address the emergency.

Typical security operations functions

The most common component of security operations is incident investigation and response, and this is where most security operations teams will begin their development. Typical functions include the following.

- **Incident investigation and response**—This includes looking into alerts from the security tools (e.g., SIEM, XDR, EDR), investigating, and remediating. In larger organizations, every aspect of incident response is likely to be handled in-house. But in smaller organizations, or those with less developed security functions, sometimes these duties are entirely outsourced to a managed security services provider (MSSP). In other instances, a hybrid model will develop with triage and high-speed remediation outsourced to the MSSP while advanced investigation is kept in-house.

- **Tactical threat intelligence**—Most common in larger organizations, tactical threat intelligence focuses on technical things like indicators of compromise (IOCs), malicious IP addresses, bad DNS names, and file hashes. In some cases, the organization will consume information from a threat intelligence service to address this function, while other organizations will produce their own and do their own research. The tactical threat intelligence is very much a support function of the investigation response function and deals with alerts and investigations in progress.

- **Incident/crisis management**—When a major incident or significant crisis puts the business at risk, organizations may employ the specialized role of Incident Manager or Crisis Manager. This is an individual who is adept at managing crisis response, assessing regulatory or compliance effects of incidents, and maintaining communication with business leaders throughout the incident. Large organizations will likely have a full-time incident manager, while smaller organizations may handle this as a temporary, as-needed role. This role requires a specialized skill set different from the technical investigative skills of other analysts.

- **Dedicated SIEM infrastructure management**—Organizations that rely on on-premises, infrastructure-intensive SIEMs may have an in-house team to maintain the SIEM infrastructure. The infrastructure of legacy on-premises SIEMs can become very large and complex. In those instances, supporting the analyst teams in their advanced queries and hunts for attackers might require additional personnel. As organizations migrate to cloud-based SIEMs, like Microsoft Sentinel, we would expect this function to phase out or be redirected to other infrastructure needs as there is no infrastructure management needed with a cloud-based SIEM.

The tactical threat intelligence is very much a support function of the investigation response function and deals with alerts and investigations in progress.

For more advanced security operations teams:

- **Proactive hunting**—A talented and determined adversary can sometimes find a way around your detections. Once inside, adversaries hide in the noise to look like a lower priority. They evade and can get missed by normal processes. The industry is recognizing that there is a need for proactive hunters to go look for adversaries to find and eliminate those that have found their way around the primary defenses. We'll talk more about proactive hunting in the section on best practices.

- **Strategic threat intelligence**—This threat intelligence function is distinct from the tactical threat intelligence function we discussed earlier that provides the technical indicators of compromise. Strategic threat intelligence is forward-looking and provides strategic guidance, intelligence, and research on the kinds of threats and attacks the business may face, and consideration of the risks and consequences to the business if those attacks occur. Strategic threat intelligence personnel are there to advise the CISO or business leaders so they understand the current threat landscape and how to interpret the news they see from a cybersecurity standpoint, then add it to their strategic planning.

Realistically speaking, at the current time, there is a talent shortage for security analysts. For any company that has an in-house security operations team, the main focus of the team must be incident investigation and response. As this baseline need is met and the team matures and expands, the team's functions can also expand and move more toward proactive hunting and strategic threat intelligence. But if you have only a small team, your focus must and should be on identifying and responding to incidents.

Modernizing security operations

Modernizing security operations requires maturing your tooling and processes to support an evolution from a reactive stance to a proactive stance and from a network perimeter model to a security model that uses identity as the primary control plane for security.

From reactive to proactive

Increase visibility

Deep tooling and automation provide your analysts the visibility and time savings they need to be able to shift from purely reactive responses to proactively preparing for—and searching for—adversaries. This type of tooling is often referred to as extended detection and

response (XDR) and is focused on providing high-quality detections and other capabilities for specific resources like endpoints, identities, cloud storage accounts, and so on.

Many organizations continue to rely on legacy, on-premises SIEMs, and a log-centric analysis process. It is important to remember, though, that "collection is not detection"—simply collecting logs won't help you much if there's too much data for your analysts to sift through. You'll miss the signal inside the noise and increase the chances your analysts will waste precious time chasing false positives while real threats go unacknowledged. From the legacy SIEM and log-centric approach, organizations should work to evolve into a model using cloud-based SIEM, like Microsoft Sentinel, and deep tooling, such as an endpoint detection and response (EDR) and other specialized detection tools. When these detection tools are integrated with a cloud-based SIEM that can apply Machine Learning, Behavior Analytics, and Security Orchestration Automated Response (SOAR) technology to the incoming alerts, three things happen:

1. Many alerts are handled via automation without requiring an analyst's time.

2. The quality of alerts making it to your analysts' queues goes up dramatically as the analysts gain the precise visibility into what is really happening, and where, that they need to be successful.

3. As technology increasingly automates security operations' reactive functions, analysts can focus more on the proactive hunting aspect of security and start searching for anomalies and hunting for adversaries in their environment.

This kind of evolution from reactive to proactive, and from on-premises SIEM and tooling to cloud-based, is not always a straight line. But this is generally the maturity trajectory we see historically. We anticipate it will increase in the future, and we recommend it as a model for organizations interested in taking productive steps to modernize their security operations.

Reducing the attack surface is another proactive step you can take. Most attacks against an organization follow the structure of what is known as the cyber kill chain. The kill chain helps us to understand how a typical attack works and what technologies can help mitigate the threats in each section of the chain. By understanding the chain, organizations can place "breaks" into each link of the chain to stop an attack or keep it from spreading.

These are the steps of a typical kill chain:

1. Reconnaissance—Criminals devise ways to exploit an organization or a user within an organization. This activity can include research to uncover information that can be used in a spear-phishing campaign, dark web activity where criminals purchase information on vulnerabilities within an organization, or reconnaissance to uncover the weak spots in an organization's infrastructure or user base.

2. Exploit a vulnerability—Threat actors then launch an attack. It could be a common phishing campaign, or a more sophisticated technique designed to deliver malicious code to an organization's systems.

3. Lateral movement—Once inside, criminals use their access to move, often undetected, through an organization's systems to locate key data. They may take steps to cover their tracks or add other entry points should the original breach be discovered.

4. Data exfiltration—Once they find the data they're seeking, whether it's personal, financial, intellectual property, or other sensitive information, criminals can steal it or encrypt it as part of a ransomware attack.

A lack of orchestration across your tools can put an extra burden on security analysts to decipher threats manually, which slows down responses when time is of the essence.

A traditional perimeter defense strategy is no longer enough to mitigate attacks against an organization. Modern attack techniques such as phishing and password spray are designed to defeat perimeter defenses. Additionally, a growing amount of data exists in the cloud and on mobile devices outside the corporate network. In response, security leaders must move away from perimeter-based protections, which are designed simply to keep the bad actors out, and toward a protect/detect/respond approach designed for today's "assume breach" world.

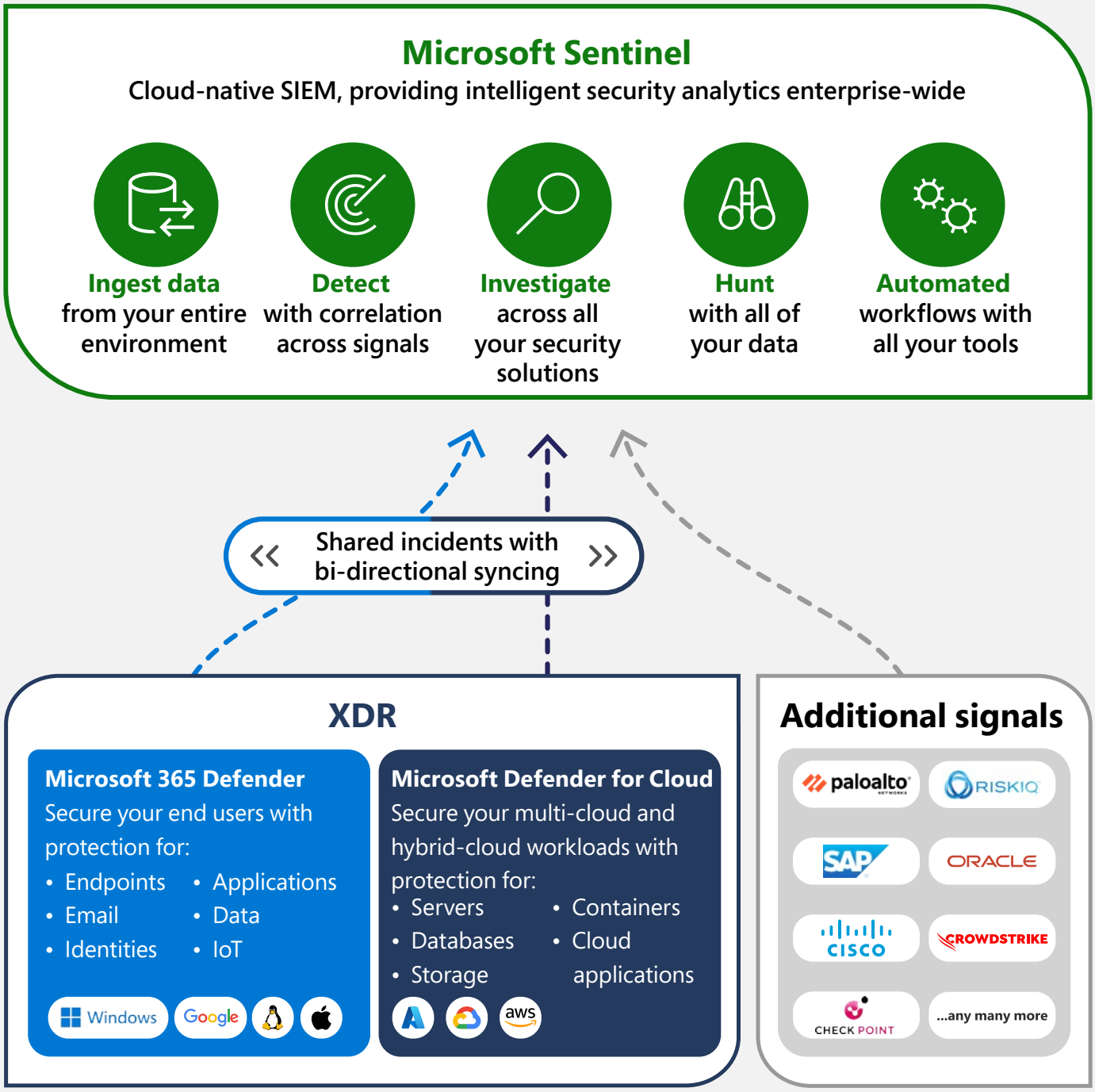
This multi-layered approach, however, is often implemented through point solutions deployed piecemeal to address specific sections of the kill chain and still leaves organizations vulnerable, because the tools are often siloed and must be managed separately. This allows for critical gaps in visibility and coverage—gaps that attackers can exploit.

A holistic approach to risk mitigation for today's evolving threat landscape requires a platform that can give CISOs and their teams integration and visibility across the organization. This integrated approach closes your gaps to reduce the attack surface. This approach is enabled by integrating a cloud-native SIEM system, which provides breadth across platforms with extended detection and response (XDR) solutions. These solutions in turn provide in-depth threat protection across domains to help defenders connect seemingly disparate alerts and get ahead of attackers.

Modern attack techniques like phishing and password spray get around the perimeter and resources increasingly live in the cloud and on mobile devices outside the corporate network.

Microsoft´s approach

In the Microsoft SOC, we enable this breadth and depth visibility with the integrated SIEM + XDR capabilities of Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud.



- **Microsoft Sentinel,** our industry-leading, cloud-native SIEM collects from any source, any data, and any entity. Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing alert detection, threat visibility, proactive hunting, and an orchestrated threat response with built-in SOAR technology.

- **Microsoft 365 Defender** provides an extended detection and response (XDR) across identities, endpoints, applications, and email.

- **Microsoft Defender for Cloud** provides comprehensive multi-cloud protection for IoT, infrastructure, cloud resources, and workloads.

Security operations

Microsoft reference architecture

Our technical vision for security operations has people—analysts and hunters—at the center of it. Our integrated SIEM + XDR security technologies are applied to help the analysts and hunters succeed by delivering deep insights for high-quality alerts that incorporate both depth of signal via XDR and breadth of signal via our cloud-native SIEM, Microsoft Sentinel. Our XDR protection extends from Microsoft products and services to everything else in the environment, and its coordinated detection and response can find and remove even sophisticated chains of attack to stop adversaries from moving across the environment if they do get in.

Learn more about Microsoft integrated threat protection with SIEM and XDR.

Our integrated SIEM + XDR security technologies are applied to help the analysts and hunters succeed by delivering deep insights for high-quality alerts.

Zero Trust and modern security operations

By now, most organizations have good defenses in place for network-based attacks. Recognizing this, attackers have shifted their tactics to identity-based and application-based attacks where defenses are weaker. In addition, devices and apps are now leaving the network, eliminating the perimeter as point of control.

Modernizing means evolving your defense tactics to match the tactics of your adversaries. That's why we strongly recommend adopting a Zero Trust Security model because the Zero Trust model is an identity-first model. We are not saying you should now ignore networks, but you need to focus first on identity-based attack techniques, and we recommend making it your first priority to build identity security skills and capabilities.

Instead of building up strong defenses on the network and then believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. In the Zero Trust model, there is no trusted network—every network is hostile.

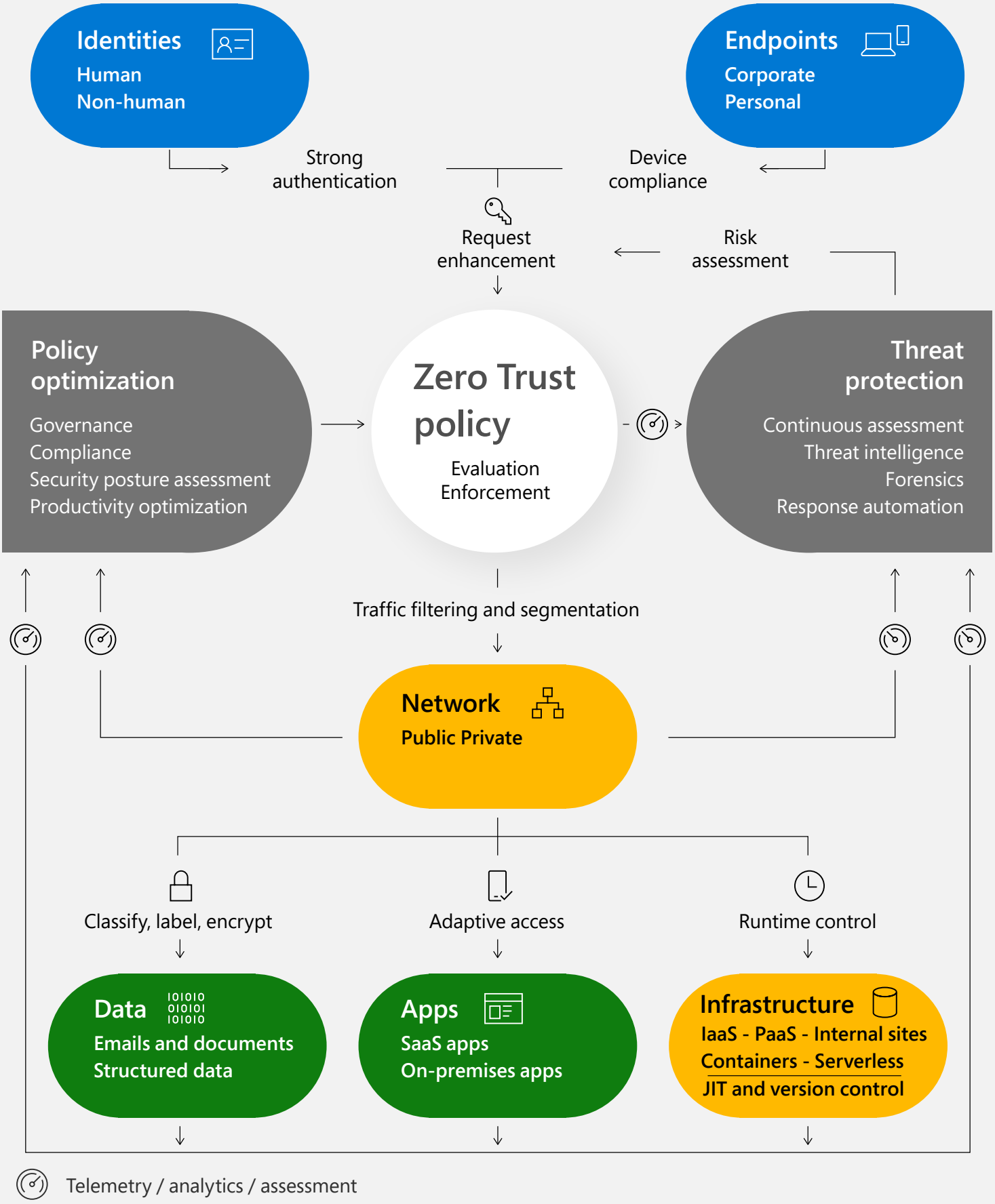
1. Verify explicitly – Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

2. Use least privileged access – Limit user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.

3. Assume breach – Minimize blast radius for breaches and prevent lateral movement by segmenting access by network, user, devices, and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility, drive threat detection, and improve defenses.

A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements: identities, endpoints, applications, data, infrastructure, and networks. Each of these six foundational elements is a source of signal, a control plane for enforcement, and a critical resource to be defended. This makes each an important area to focus investments, starting with identity.

Each of these six foundational elements is a source of signal, a control plane for enforcement, and a critical resource to be defended.


Identities
Human
Non-human
Endpoints
Corporate
Personal
Strong authentication
Device compliance
Request enhancement
Risk assessment
Policy optimization
Governance
Compliance
Security posture assessment
Productivity optimization
Zero Trust policy
Evaluation
Enforcement
Threat protection
Continuous assessment
Threat intelligence
Forensics
Response automation
Traffic filtering and segmentation
Network
Public Private
Classify, label, encrypt
Adaptive access
Runtime control
Data
Emails and documents
Structured data
Apps
SaaS apps
On-premises apps
Infrastructure
IaaS - PaaS - Internal sites
Containers - Serverless
JIT and version control
Telemetry / analytics / assessment

The role of orchestration in Zero Trust

Orchestration is the process of integrating applications and automating a workflow. As already mentioned, Zero Trust is most effective when fully integrated in an end-to-end strategy. But achieving that integration in a way that supports compliance and operational efficiency requires careful orchestration.

This means enforcing clear Zero Trust policies and continuous evaluation of the effectiveness of these policies so that adjustments can be made as needed. Ongoing assessment is vital for optimizing governance, compliance, and productivity while maintaining a strong security posture. Incorporation of a threat intelligence feed makes it easier to adjust policies according to the latest threats, and response automation makes it possible to respond to attacks in real time and drive efficiency.

To help you plan and implement a shift to Zero Trust, this is our recommended roadmap for pursuing a Zero Trust modernization strategy.

Align segmentation strategy and teams

- Unify identity, devices, applications, data, infrastructure, and networks into a single enterprise segmentation strategy. You need everyone on the same page, all pursuing the same strategy, with the same priorities, and speaking the same language.

Build a modern, identity-based perimeter

- Establish your **critical path** using user and device assurances.

  User – Require Passwordless or MFA to access modern applications.

  Device – Require device integrity for access.

We recommend that you roll out your critical path to IT administrators first.

IT admins can give you technical feedback to help you make refinements before wide rollout, and IT admins are targeted by attackers, so a breach of their accounts can have very high impact. Secure IT admins first, then secure regular users.

Finish strategy

- Modernize apps and retrofit strong assurances to legacy on-premises assets via App Proxy.
- Increase protection levels for sensitive data (CASB, CA access control, AIP).
- Retire legacy authentication protocols.

Refine segmentation and network perimeter

- Segment assets with business-critical, life/safety, and operational/physical impact.
- Add microsegmentation to further reduce risk.
- Retire and isolate legacy computing platforms such as those with unsupported operating system and applications.

Getting started with Zero Trust

Zero Trust is a security model, not a specific technology, and achieving Zero Trust is a journey, not an on/off switch. In today's mobile, remote, and hybrid work environments, you can no longer rely on a network perimeter for security—the network perimeter has disappeared. Security operations should align around identity-based protection to lay the groundwork for a Zero Trust model. Users can have multiple devices and can access enterprise resources from a variety of networks and apps. Almost all of these resources require authentication, making identity a common denominator across all access requests, whether from a personal device on a public Wi-Fi network or a corporate device inside the network perimeter. By using identity as the control plane, you can treat every single access request as untrusted until the user, device, and other factors are fully vetted.

Step one of implementing your Zero Trust security model, then, is to connect all your apps to a single cloud identity solution, like Microsoft Azure Active Directory. This allows you to create identity-based security and apply custom policies across your entire environment to control access to every app. With that step complete, you can then implement multifactor authentication (MFA) for all your apps. MFA is a consistent, strong security policy that can block up to 99.9 percent of account compromise attacks.

To evaluate your organization's Zero Trust security posture, take the Zero Trust maturity assessment.

Microsoft's recommended identity solution for Zero Trust is Azure Active Directory, part of Microsoft Entra. To learn how you can begin your Zero Trust journey with Identity and Access Management, read Securing identity with Zero Trust.

Protecting against insider threats

With a Zero Trust security model and an integrated security suite in place, security operations can better protect the organization against external threats. However, you must also guard against insider threats with tools and processes that protect information, users, and devices.

Data now extends well beyond on-premises infrastructure into multi-cloud and hybrid cloud environments, extending your responsibilities across the entire data lifecycle—from when data is created to when it is retired or deleted.

Knowing what data you have, who is accessing it, and what they are doing with it is essential to the security of the organization. But, as with streamlining identity security, a key piece of these efforts is to reduce risk without compromising user productivity across this expanded IT landscape.

Organizations have a variety of technology and tools at their disposal for managing and protecting data at different stages of the lifecycle. While these tools provide flexibility, they also add significant complexity. A recent IDG study found that organizations use an average of nearly five different data management systems for activities such as classification, e-discovery, and records management. Integrated security solutions can also protect against insider threats by closing critical gaps that lead to data leakage and giving you end-to-end visibility throughout the data lifecycle.

We recommend you focus your end-to-end insider threat protection efforts around three key steps:

- **Identifying your data**
- **Classifying your data**
- **Deploying tools and policies to safeguard your data**

The goal should be to help ensure all information is protected—however and wherever it's used.

Knowing what data you have, who is accessing it, and what they are doing with it is essential to the security of the organization.

Differentiating intentional versus unintentional risk

Internal threats are an inevitable part of every business and sometimes data is put at risk even in the normal course of legitimate work. Think about the number of people who access resources, the natural cycle of people coming and going from a company. With the right processes, capabilities, and controls in place, you can maintain oversight of data and trust with users without undermining productivity.

One important capability to have in place is that of differentiating between an intentional and an unintentional risk from your users. A truly malicious user might try to do things that go against your corporate policies—turning off security controls, for example, or installing malicious software.

Often the intent is to leak or steal data for personal gain or for malicious reasons.

Security operations must be prepared for such events and needs ways to prevent, detect, and contain those types of threats.

But there are other classes of threats where the user may not even know they're breaking corporate policy. A user might be excited about a project and share information about it outside their group, for example, and in the process they commit a data leak not realizing they're sending sensitive information. Tools to stop that inadvertent data leak before it can happen and/or to investigate it and see it in real time, in context, enable you to determine the intent and the impact—and decide if this was a single act of carelessness or part of a larger, potentially malicious pattern.

As you surface risk you need to make sure your focus remains on the genuinely suspicious activity, so you don't cause problems with users or overwhelm analysts with alerts that are false positives.

Learn about Insider Risk Management in Microsoft Purview.

Security operations best practices

As we mentioned earlier, at the center of security operations are people—specifically the security analysts.

As your analysts do their work, they will either formally or informally progress through what is known as an OODA loop:

- **Observe**
- **Orient**
- **Decide**
- **Act**

Your goals should be to empower your people to progress through the OODA loop as quickly as possible, with the best information possible, so they can make the best decisions and take the most effective actions possible.

To make better decisions faster, focus on maximizing visibility, reducing manual steps, and maximizing human impact.

Maximize visibility

- **Internal**—Minimize internal blind spots by ensuring you have good coverage (as close to 100 percent as you can manage) as well as coverage of asset types (including identities, endpoints, email, cloud applications, on-premises datacenters, cloud datacenters, and data on cloud SaaS and PaaS applications).

- **External**—Ensure you have a diversity of threat feeds from external sources that gives you insight and context from the external environment of malware, email attacks, attack websites, compromised passwords/identities, etc. Maximize the freshness and fidelity (relevant details) of the external threat sources you use.

Reduce manual steps (and errors)

Automate and integrate as many manual processes as possible to remove unneeded human actions that lead to slowdowns and potential human errors.

Rapidly sorting out the signal (real detections) from the noise (false positives) requires investing in both humans and automation.

We strongly believe in the power of automation and technology to reduce human toil. But ultimately, the attackers you're dealing with are human operators so human judgment is critical to the process of defending against threats.

Automation should not be about using efficiency to remove humans from the process—it is about empowering humans. Think about how you can automate repetitive tasks from the analyst's job, so they can focus on the complex problems that people are uniquely able to solve.

Automation empowers humans to do more by increasing response speed and capturing human expertise. It reduces the burden and boredom of repetitive tasks, enabling analysts to focus time and creativity on new challenges and threats.

Maximize human impact

For the places in the process where it makes sense to have human interaction (difficult choices, new decisions, etc.), you should ensure that your analysts have access to deep expertise and intelligence to make those decisions better.

Additionally, you should ensure learning is integrated throughout the process, up to and including consideration of when you would watch an attack unfold to learn its objective (long-term value) vs. blocking it (short-term value).

Making better decisions faster

Maximize visibility

Internal – Sensor coverage completeness and diversity

External – Threat Feed Diversity and fidelity

Reduce manual steps (and errors)

Automate – Detection and response tasks

Integrate – Investigation tools

Maximize human impact

Provide analysts with access to **deep expertise and intelligence Continous Learning**—observe attacks and integrate learnings into defenses

Security operations culture

Culture guides countless decisions each day by establishing what the right answer looks and feels like in ambiguous situations, which are plentiful in security operations.

Focusing cultural elements on people, teamwork, and continuous learning helps ensure your team is continually evolving to keep pace with the threats it is there to protect against:

- **Use your human talent wisely**—Our people are our most valuable assets, and we can't afford to waste their time on repetitive, thoughtless tasks that can be automated. To combat the human threats we face, we need knowledgeable and well-equipped humans that can apply expertise, judgment, and creative thinking. This human factor affects almost every aspect of security operations, including the role of tools and automation to empower humans to do more (versus replacing them) and in reducing toil on our analysts.
- **Teamwork**—We recommend that you shouldn't tolerate the "lone hero" mindset on the team. Nobody alone is as smart as the whole team together. Teamwork makes a high-pressure working environment much more fun, enjoyable, and productive when everyone knows they're on the same team and everyone has each other's back. In the Microsoft Security Operations Center, we design our processes and tools to divide up tasks into specialties and to encourage people to share insights, coordinate and check each other's work, and constantly learn from each other.
- **Shift left mindset**—To get ahead and stay ahead of cybercriminals and hackers who constantly evolve their techniques requires continuously improving and shifting your activities "left" in the attack timeline. Focusing on speed and efficiency helps the team get "faster than the speed of attack" by looking at ways they could have detected attacks earlier and responded more quickly. This principle is effectively an application of a continuous-learning growth mindset that keeps the team laser-focused on reducing risk for the organization and customers.

Segregate high-privileged accounts

Not all attacks are created equal from the standpoint of the damage they could do to your business if successful. High profile accounts—board members, CEO, CFO, for example—and administrator accounts present the most risk to you if compromised. Therefore, you should give special attention to proactively protecting these accounts first by segregating them in dedicated computing environments using Privileged Access Workstations (PAWs) that protect these important accounts from Internet attacks and other threat vectors.

Metrics – measuring success

Metrics translate culture into clear measurable objectives and have a powerful influence on shaping people's behavior. It's critical to consider both what you measure, as well as the way that you focus on and enforce those metrics. At Microsoft, we measure several indicators of success in the Security Operations Center (SOC), but we always recognize that the SOC's job is to manage significant variables that are out of our direct control (attacks, attackers, etc.). We view deviations primarily as a learning opportunity for process or tool improvement rather than a failing on the part of the SOC to meet a goal.

These are the metrics we track, trend, and report on:

- **Mean time to acknowledge (MTTA)**—Responsiveness is one of the few elements the SOC has direct control over. We measure the time between an alert being raised and when an analyst acknowledges that alert and begins the investigation. Improving this responsiveness requires that analysts don't waste time investigating false positives while another true positive alert sits waiting. We achieve this with ruthless prioritization. Any alert that requires an analyst response must have a track record of 90 percent true positive.

- **Mean time to remediate (MTTR)**—Much like many SOCs, we track the time to remediate an incident to ensure we're limiting the time attackers have access to our environment, which drives effectiveness and efficiencies in our SOC processes and tools.

- **Incidents remediated (manually vs. with automation)**—We measure how many incidents are remediated manually and how many are resolved with automation. This ensures our staffing levels are appropriate and measures the effectiveness of our automation technology.

- **Escalations between each tier**—We track how many incidents are escalated between analyst tiers to ensure we accurately capture the workload for each tier. For example, we need to ensure that tier 1 work on an escalated incident isn't fully attributed to tier 2.

Maintain critical hygiene

Methods, defenses, and effects may vary, but simply put, attackers exploit vulnerabilities. Which in turn makes your job as security professionals simple: Eliminate your vulnerabilities.

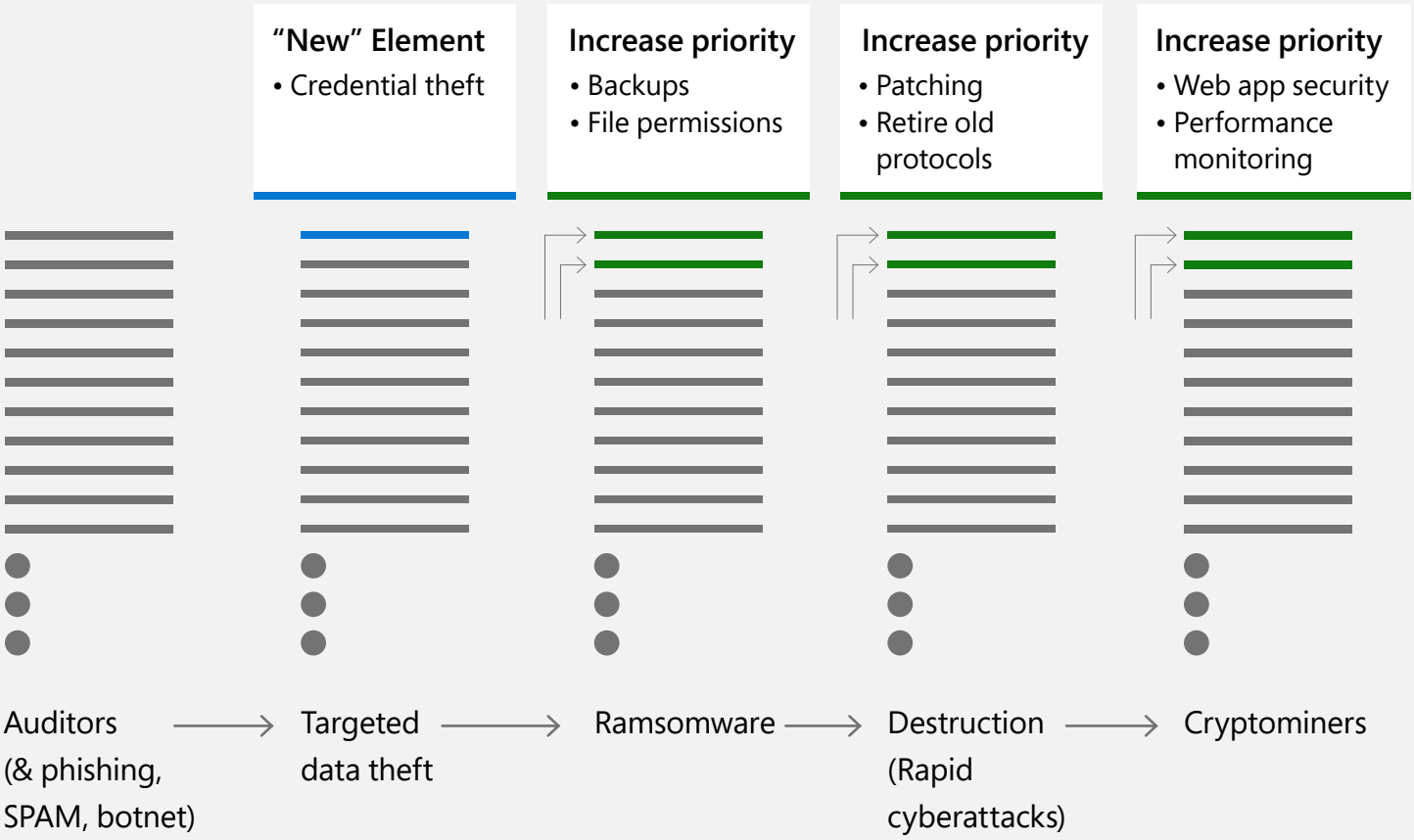
Every team has work to do to update its environment—we refer to this as carrying "technical debt." You need to make backups, or you need to update file permissions. Or there's patching to do, or you have old protocols to retire. These are all well-known best practices.

As attackers find new ways to build a business model or come up with a new attack technique, they are often simply exploiting the same old vulnerabilities, just in new ways. In some cases, they may exploit vulnerabilities you didn't previously know you had. So, while attacker techniques may evolve, the imperative for good old-fashioned technical hygiene remains the same. Keeping your environment up to date in ways you've known about for a long time and learning what else you have to do based on attacker behavior are critical to protecting your organization against attacks—even the newest kinds of attacks.

As attackers find new ways to build a business model or come up with a new attack technique, they often are simply exploiting the same old vulnerabilities just in new ways.

Critical hygiene = Technical debt to pay off

Cloud can speed this up, but some hard work must be done



New monetization models simply reshuffle priorities of the same old hygiene debt:

1. **Look at your critical hygiene needs regularly.**
2. **Prioritize based on what is happening now.**
3. **Revisit your list of best practices and priorities often to ensure it applies to current conditions.**
4. **Continually work to eliminate your "technical debt."**

Proactive hunting

Threat hunting is a powerful way to reduce organizational risk. But it's commonly portrayed as a complex and mysterious art form for deep experts only, which can be counterproductive. The term "threat hunting" simply refers to the process of experienced analysts proactively and iteratively searching through the environment to find attacker operations that have evaded other detections.

Hunting is a complement to reactive processes, alerts, and detections, and enables you to proactively get ahead of attackers. What sets hunting apart from reactive activities is the proactive nature of it, where hunters spend extended focus time thinking through issues, identifying trends and patterns, and getting a bigger-picture perspective. A successful hunting program is not purely proactive, however, as it requires continuously balancing attention between reactive efforts and proactive efforts.

Threat hunters still need to maintain a connection to the reactive side to keep their skills sharp, and to keep attuned to trends in the alert queue.

At Microsoft, our SOC approaches threat hunting by applying our analysts to different types of threat hunting tasks:

1. Proactive adversary research and threat hunting. This is what most of our threat hunters spend the majority of their time doing. The team searches through a variety of sources including alerts, external indicators of compromise, and other sources. The team primarily works to build and refine structured hypotheses of what the attackers may do based on threat intelligence (TI), unusual observations in the environment, and their own experience. In practice, this type of threat hunting includes:

- **Proactive search through the data (queries or manual review).**
- **Proactive development of hypotheses based on TI and other sources. (See Operationalize the MITRE ATT&CK Knowledge Base.)**

2. Red and purple teaming. Some of our threat hunters, working as blue teams protecting the environment, coordinate with red teams who simulate attacks and others who conduct authorized penetration testing against our environment. This is a rotating duty for our threat hunters and typically involves purple teaming, where both red and blue teams work to do their jobs and learn from each other. Each activity is followed up by fully transparent reviews that capture lessons learned which are shared throughout the SOC, with product engineering teams, and with other security teams in the company.

3. Incidents and escalations. Proactive hunters aren't sequestered somewhere away from the watch floor. They are co-located with reactive analysts and frequently check in with each other, share what they are working on, share interesting findings or observations, and generally maintain situational awareness of current operations. Threat hunters aren't necessarily assigned to this task full time; they may simply remain flexible and jump in to help when needed.

These are not isolated functions—the members of these teams work in the same facility and frequently check in with each other.

Operationalize the MITRE ATT&CK Knowledge Base

The MITRE ATT&CK Knowledge Base is a treasure trove of information, but the amount of information there can be intimidating. The good news is technology products can help you reduce the effort of deriving value from MITRE ATT&CK. Many tools today, including security solutions from Microsoft, have already done a lot of mapping to the knowledge base. In fact, the Security Stack Mappings for Azure research project recently introduced a library of mappings linking built-in Azure security controls to the MITRE ATT&CK techniques they mitigate. Keep in mind, however, that mappings aren't generally comprehensive. Your organization should assess where the tools cover you by default and where you still have gaps.

Where those gaps exist, you can customize mapping of existing tools and technology to the areas of the MITRE ATT&CK Knowledge Base that best apply to your organization to make sure you're covered. In addition, you probably don't need all of what's in the MITRE ATT&CK Knowledge Base. Look at the knowledge base from an adversary perspective: not every single adversary in the world wants to target your organization or business. Reduce the volume of information

in the knowledge base that you have to track by looking at adversaries that target businesses like yours and understanding what techniques they use in their attacks. You can build your detections based on which adversaries and techniques are most likely to target your organization.

In this way, the MITRE ATT&CK Knowledge Base becomes a tool you can use to conceptualize what attackers are likely to do if they try to exploit your organization and to proactively build detections around those potential attack patterns.

Build rapport with IT

In many organizations, security operations doesn't control the technology environment. It is often up to IT how the environment is tooled. The response and remediation options available to you are often dependent on the technology choices IT has independently made. It can be helpful to build relationships and cross-functional awareness with IT. When each group knows what the other is working on, as well as the challenges and limitations they face in fulfilling their part of the mission to protect the organization, they can accelerate modernization and enhance security. In addition, there will be many occasions when a successful remediation will require action by IT personnel. Having good relationships and knowledge of IT personnel roles, responsibilities, and the skill sets of IT team members can help you get to the right person more quickly when there is an incident.

Continuous improvement

Once an attack is remediated, you must assume that adversaries will try to learn from what happened and they will try again with fresh ideas and tools. Your analysts should also focus on learning from each incident to improve their skills, processes, and tooling. This continuous improvement can occur through many informal and formal processes ranging from formal case reviews to casual conversations where analysts tell the stories of incidents and interesting observations.

As caseload allows, the investigation team can also hunt proactively for adversaries, which can help them stay sharp and grow their skills. Finally, purple-teaming exercises should be designed with continuous improvement as one of the goals. As red teams succeed in evading detection by the defenders in the exercises, embrace those moments as important chances for everyone to learn and get better.

Final recommendations

Modernizing your security operations is a big undertaking. You'll need to involve stakeholders from across the organization and you shouldn't think you can do it all at once. But there are some things you can do right now to reduce your vulnerabilities, increase visibility, and improve efficiency and effectiveness as you defend against advanced attackers:

1. Embrace Zero Trust – The Zero Trust model is about verifying explicitly, utilizing the concept of least privileged access, and maintaining an "assume breach" mindset. Start your Zero Trust journey by shifting the control plane for security from your network perimeters to identity.

2. Segregate high-privileged accounts – Identify the accounts in your organization that would be most desirable to attackers and segregate them using privileged access workstations (PAWs) and secure your administrator accounts. These accounts could do the most amount of damage if compromised, so start your protection efforts there.

3. Shore up your supply chain – This fits into the "shift left" mentality we discussed in the Best Practices section of this guide. Slipping malicious code or components into the software products you receive and trust from suppliers is an increasingly common way that attackers attempt to evade your defenses. Move your awareness further up the attack chain by knowing what your suppliers are doing to stay secure, knowing what you use and where, and continuing to invest in better asset management.

4. Invest in penetration testing – Look before the bad guys do. Use penetration testing to find your fail points before you're attacked. Use the findings of your penetration testing not as a report card, but as an input into a continuous improvement process.

5. Ensure you have comprehensive investigation capabilities – Make sure you have the ability to investigate across your whole environment. Work to get comprehensive visibility from different perspectives—from endpoint to identity, from data to IoT, and across clouds. This will allow you to do the rapid investigation and early detection that is so critical to maintaining your security.

6. Integrate your Security Operations tools – Eliminate silos and gaps in coverage by embracing an integrated approach. Arm your analysts with both breadth and depth of coverage using an integrated, cloud-native SIEM and XDR.

Learn more about how Microsoft's integrated security solutions can help you modernize your security operations and provide the visibility you need to keep your organization protected.

SIEM and XDR: Your ally against ransomware >

An integrated approach for increased SOC efficiency >

Microsoft Security