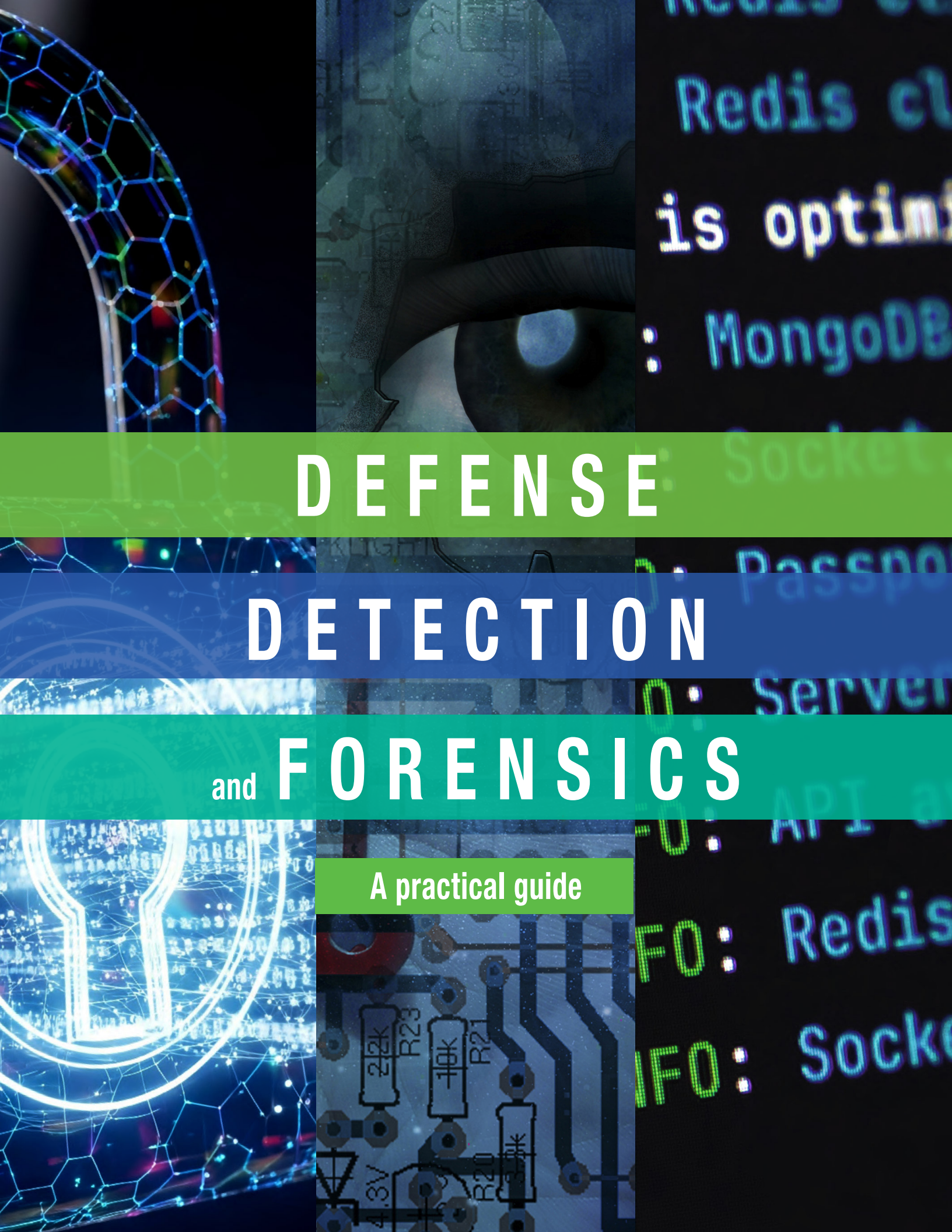

DEFENSE
DETECTION
and FORENSICS
A practical guide

A way to think about security

On a Tuesday: emails came in, the CRM was working, projects were assigned, responses went out, onsite and remote employees were checking in on their work. Everything seemed fine.

Yet there was an uninvited and hidden observer to all that normalcy – exfiltrating data, installing tools, gathering credentials, preparing for an attack. According to Mandiant, the average dwell time – the period of surreptitious criminal activity on a network before detection – is 14 days. Two weeks of unseen access, on what looked like a perfectly ordinary network.

Above: The average time of surreptitious criminal activity on a network before detection is 14 days.

.

This is the situation many small businesses are in without realizing it. The attackers are professionals. Many operate with quotas for how much they need to collect. They are good at what they do and what they do is steal.

The good news is that the tools to address this are no longer reserved for large enterprises. Detection, defense and forensic readiness are now within reach for smaller organizations – and understanding how they fit together is the first step.

The wall: defensive controls

Defense is the lock that gets in the way so a problem does not become a disaster. It is the root of cybersecurity and it remains the fundamental layer that everything else builds on.

A sound defensive posture includes: reliable, tested backups stored off-site; encrypted data; antivirus software kept current; consistent software patching; strong passwords (at least fifteen characters, unique to each site or application) enforced by policy; and multifactor authentication (MFA), where a login is verified by a phone app or similar. These are considered the basic obstacles to criminal intrusion and deployed properly, they all remain valid.

Cover: Three pillars of security: defense, detection and forensics.

Two of these tend to get skipped in practice, and both are worth examining.

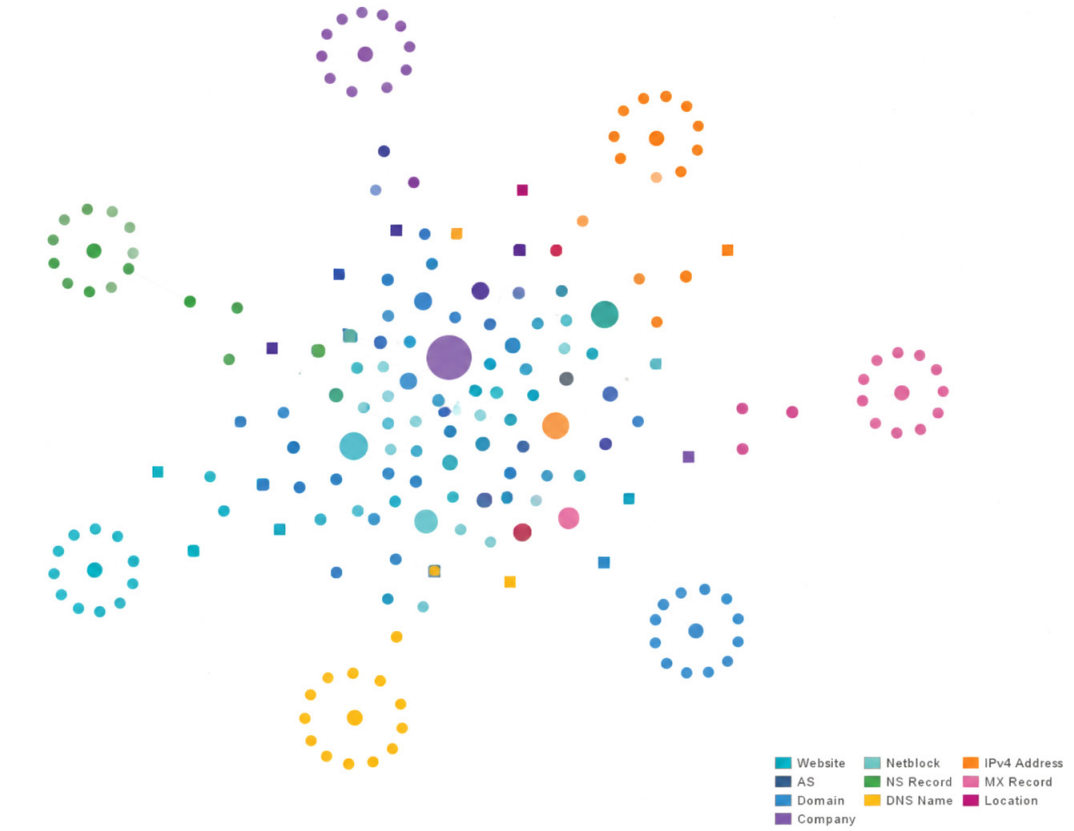
Patching is unglamorous but important. Many attacks get into systems through software that has not been updated. AI tools are now being trained to search for and exploit known vulnerabilities on internet-connected machines. A rarely used machine that has not received updates in months, running an older operating system with a known remote execution vulnerability, can become an attacker's entry point into critical systems. Patching is unending and interruptive, so it tends to be underutilized – but closing those known weaknesses is one of the most important things an IT provider does.

The Principle of Least Privilege – limiting each employee's account access to only what they need to do their job – is similarly under-applied. Should an account be compromised, the damage is contained because the account can only reach certain files. It is a simple concept that applies regardless of the sophistication of your systems. Dormant accounts fall under the same logic: a former employee's access should be revoked immediately. Too often, accounts that should have been closed at the end of a job simply remain open and vulnerable.

Email security and backups

Certain research has shown email is the gateway for up to 90% of breaches. No one argues that the percentage is, if not 90%, at least very high. Spam and malware filtering catches bulk, indiscriminate threats – the tools built into platforms like M365 and Google Workspace intercept a significant volume. But 98% of tested accounts still show malware getting through, which is why additional layers matter: email header analysis, AI systems trained on your employees' normal behavior and filters that flag when, for example, a marketing employee is sending client database information to an unfamiliar address.

Email account takeover is a growing concern. Criminals use stolen credentials to co-opt a staff member's account and attempt to escalate privileges or trick colleagues – sending something like 'Hey, I forgot the login to the shared drive, can you help?' from what looks like a trusted internal address. Good, protective AI catches many of these, but not all.

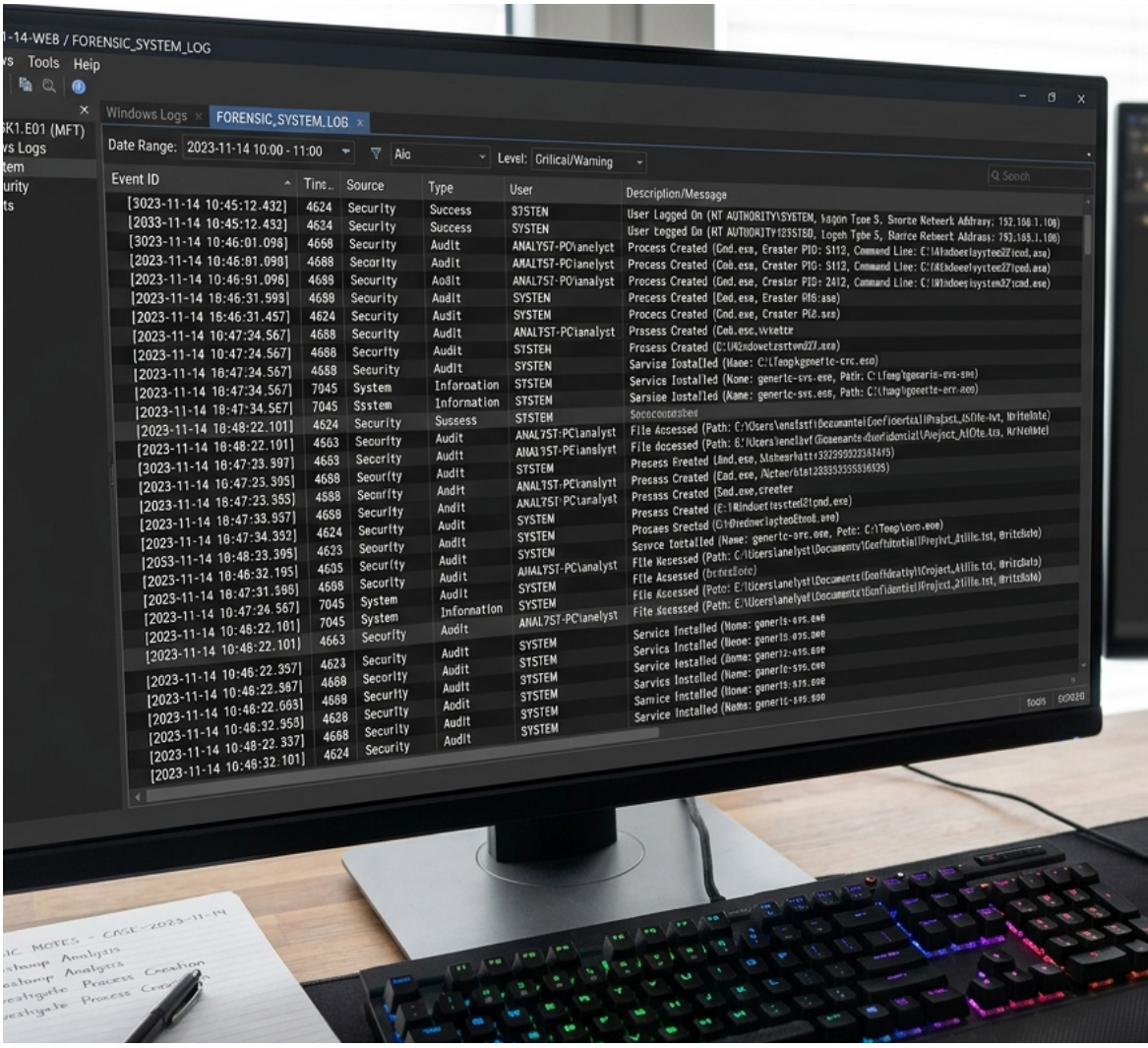


Above: Detection tools know criminals by their behavior, which is a meaningful shift.

The goal of Security Awareness Training is to give staff enough familiarity with current methods to pause, question and disengage before company data is handed over. Formats include classroom sessions, self-paced cloud-based modules and phishing simulations – and because attack methods keep evolving, the training needs to be ongoing.

Backups deserve a mention here. Redundant backups – including of cloud-resident data – need to be tested that they can be counted on to reliably restore. A 3-2-1 scheme gives you three copies of your

Right: Forensically, logs are how you learn what actually happened, rather than guessing at the cause, so you can close the actual weakness not an assumed one..



data in two locations, including one off-site. This redundancy, done properly, should allow recovery from various kinds of outages without extended downtime. And backups need to be stored beyond the reach of ransomware encryption – something worth discussing specifically with your IT provider.

Adding detection: knowing what is happening on your systems

Defensive controls are like a stone wall – tough to penetrate, representing brute strength. The problem is that today's attackers are not simply trying to break through walls. They wait, test and evade. They work trusted relationships and use human nature against employees.

Detection tools know criminals by their behavior, which is a meaningful shift.

Dark Web Monitoring is a practical starting point. At its root, dark web monitoring software is trained on message boards and marketplaces where criminals connect. It can be set to find evidence of your organization's email addresses being traded. Email addresses are typically part of stolen databases and often come paired with passwords – and sometimes more, like usernames or social security numbers.

And a leaked working email address and password are the criminal's starting point. Bots test stolen credentials across millions of sites – banks, cloud accounts, social media. MFA will block many of these attempts. But the email address still has criminal value: their AI tools scrape your company website, LinkedIn and public data-broker sites, then stitch the results together with the leaked credentials. The outcome is enough to convincingly impersonate your CFO, a supplier or a colleague by phone or email –

Finding security gaps on your own terms is considerably better than finding them through a breach

because the attacker already knows names, roles and relationships. This is the mechanism behind business email compromise, which accounted for $2.77 billion in US losses in 2024.

SIEM (Security Information and Event Management) helps address detection across the network. Many businesses do not know they have been breached until months later, when a third party notifies them. The gap between intrusion and detection is when the damage happens: credentials are stolen, data is exfiltrated, system access is sold. SIEM combines logs from across your environment – email, endpoints, cloud apps, your network – and flags what does not look consistent with normal behavior. A login from an unfamiliar country at 2 AM. An employee account retrieving a type of file it has never accessed before. SIEMs were once the domain of large corporate security teams, but cloud-based versions now exist and a managed services provider can handle the monitoring, triage and response at a budgetable monthly cost.

EDR (Endpoint Detection and Response) operates at the device level. EDR is AI-based software installed on a desktop or laptop that performs real-time analysis of what is happening on the machine. Depending on configuration, it can stop active processes it identifies as dangerous. Because criminal attacks are increasingly evasive, having EDR on employee devices is an important advantage over signature-based antivirus alone. Traditional antivirus is not obsolete – most attacks are relatively straightforward and those files can be recognized and quarantined. But new and emerging attacks are meant to bypass traditional software and EDR is designed to catch behavior that does not match a known signature. EDR tied to a Security Operations Center (SOC) means that when something is flagged, there is expertise available to assess it and get the employee back up and running safely.

After the breach: forensics and what they protect

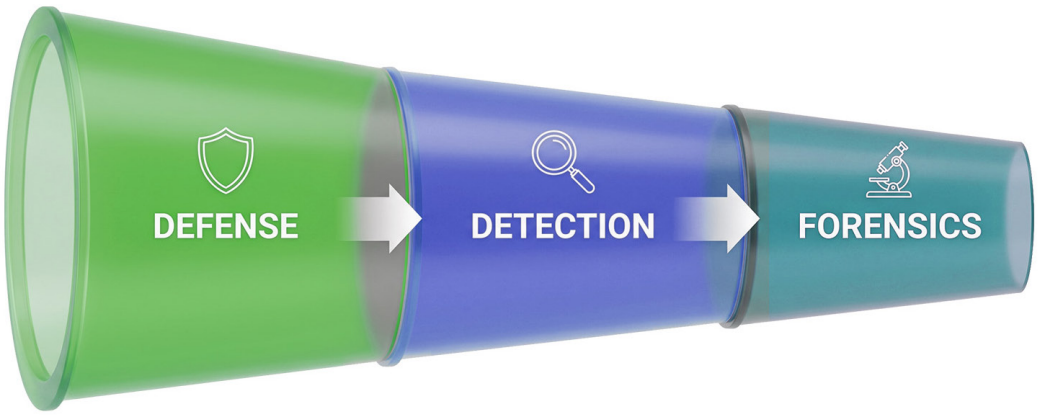
Here is where many businesses find themselves in a difficult position because no one told them this part mattered till it was too late.

Six weeks after that seemingly normal Tuesday, the breach was discovered. The business filed a cyber-insurance claim. The insurer's investigators needed untouched evidence: logs that documented what happened, when and how. But in the scramble to restore systems, logs had been overwritten. The $300,000 in recovery costs came out of the business rather than from their insurer.

Many smaller organizations, when they become aware of an attack, shut down the affected machine and attempt a reboot. If that fails, they look for a restore point prior to the incident. The problem is that resetting to a recent backup may only take you back to a point where the attack was already visible – still granting the criminal their gateway and without the configuration to retain a complete set of logs.

Logs matter for two reasons beyond insurance. Compliance standards – including CMMC and DFARS for organizations working with the military and PCI for those handling card payments – often require access to logs to reconstruct the circumstances of a breach. And forensically, logs are how you learn what actually happened, rather than guessing at the cause, so you can close the actual weakness not an
assumed one.

Three things need to be in place before a criminal event for forensics to be useful. First, a policy and practice of log retention – how logs will be generated, stored and for how long. Second, a policy of not disturbing the discovered scene of an intrusion – a crime-scene protocol. Third, a clear procedure for how to handle an incident: who to call and what steps preserve the integrity of the evidence.



Above: Detection, defense and forensics can be thought of as a narrowing of focus across an attack timeline. Defensive controls work broadly against diverse threats. Detection tools have the ability to observe an attack that eluded those controls. Forensics examine what the attacker did — preserving evidence, supporting recovery and helping close any exploited weakness.

The tools that support forensic readiness overlap with the detection tools already described. Managed EDR identifies and stops threats from spreading and in its managed form, analysis and reporting is sent to a SOC where generated data is assessed, handled and retained for an agreed period. SIEM consolidates security data into comprehensive logs, drawing from cloud services, firewalls, networked devices and applications. Managed SIEM adds expert analysis and handling at a SOC.

Together, EDR and SIEM produce a whole-picture timeline – what compliance auditors and cyberinsurance examiners need to verify the integrity of your organization's data and calculate risk. The investment in detection, in other words, does double duty: it helps catch an attack in progress and it preserves the evidence trail you may need long after the event.

Putting it together: a practical starting point

Detection, defense and forensics are three aspects of a single posture that reinforce each other. Defensive controls reduce the number of ways an attacker can get in. Detection tools shorten the window between an intrusion and discovery. Forensic readiness means that when something does happen, you have logs that document it, a protocol for not disturbing evidence and a procedure for who to call and what to do next.

A useful first step is an audit of the basics. Are your backups tested for recoverability? Are former employees' accounts closed? Is patching happening consistently? Is there visibility into what is happening across your network or would a 14-day intrusion go unnoticed?

These questions are a starting point. Many businesses find gaps when they look carefully – and finding them on your own terms is considerably better than finding them through a breach.

The tools described in this series – dark web monitoring, security awareness training, SIEM, EDR and the foundational defensive controls – are available at a scale and cost that works for organizations well below the enterprise level. A managed services provider can handle the monitoring, triage and response, making the specialist knowledge those systems require available at a budgetable monthly cost.

Start with the basics if you have not already. Add detection where you can. And make sure that if something does happen, you have the logs and a plan that keeps the evidence in place so as not to make a bad situation worse. Better security is within reach for many organizations – and the time to have it is before a breach.

Sources: zdnet.com/article/diverse-threat-intelligence-key-to-cyberdefense-against-nation-state-attacks/
huntress.com/resources/2024-cyber-threat-report
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf
ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
smashingsecurity.com/459-this-clever-scam-nearly-hijacked-a-tech-ceos-apple-id/
moneywise.com/news/san-francisco-retiree-lost-500000-life-savings-to-romance-scam
cloud.google.com/security/resources/m-trends/
Cyberattacks cost 27% of organizations more than $500,000/year, per Huntress.

bryleysystems™

Bryley • Business Continuity through Managed IT
Bryley Systems Inc, 200 Union St, Clinton, MA 01510n • 978.562.6077 • Bryley.com