Bank's CyberOps Team Wins EDR Buy-In

In 2015, Israel's Supervisor of Banks issued *The Proper Conduct of Banking Business Directives*, a sprawling set of regulations that set "prudential requirements for proper conduct of banking business on various matters."[1] The directives address risk management in Regulation No. 361, Cyber Defense Management, also known as Order #361.[2]

The government's new demands on financial institutions led to an important career experience for Ofir Eitan, a cyber operations manager employed at one of the largest financial institutions in Israel at the time. In January 2016, he was tasked with establishing a new cyberoperations (cyberops) team within the information security (infosec) department to develop a plan for achieving compliance with Order #361, among other responsibilities. Eitan's first step was to conduct a review of the bank's cybersecurity posture.

The review process was intensive. Over a three-month period, Eitan conducted interviews "with a long list of core employees in the company," he recalled, including the head of infosec, the chief risk officer (CRO), the head of IT infrastructure, the head of network administration and the director of business continuity planning (BCP). The department's final product was a report showing Order #361's directives, the bank's compliance status, and a suggested road map for bridging gaps and mitigating risk.

EDR Is Critical

"Endpoints are the battlefield to protect networks against malware attacks," Eitan said. The most worrisome risk he identified was the bank's lack of an endpoint detection and response (EDR)[3] security solution. The focus of the bank's control environment was twofold: prevention and compliance, which required monitoring of critical servers to meet regulatory requirements. Its strategy was based on protecting selected systems rather than on defining a one-stop-shop solution for comprehensive security visibility and response. Endpoint visibility, forensics and malware remediation capabilities were lacking.

A core incident response (IR) tool stack, Eitan said, should consist of a security information and event management (SIEM) system integrated with EDR, intrusion prevention systems (IPSs), intrusion detection systems (IDSs), an email gateway, and a threat intelligence platform (TIP) (**figure 1**).

Compared to other incident response solutions, EDR is the primary one-stop-shop. EDR should be utilized by an organization's blue team[4] as the main battlefield defense against malware and intruders, Eitan maintained. He laid out the core capabilities that a robust EDR solution provides:

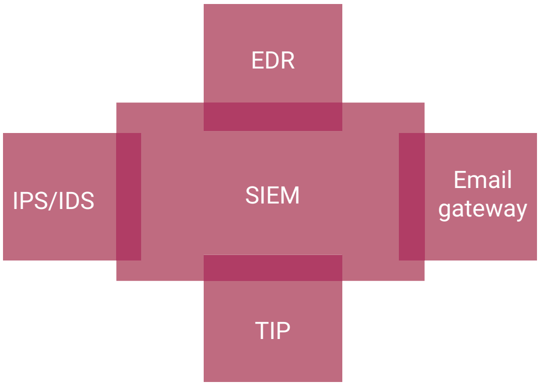
- **Visibility and control**—Different organizations may use different combinations of security tools to design their control environments. However, it is essential to equip security professionals with a single platform that can provide full visibility and control over network endpoints to detect malware threats and execute all phases of the incident response cycle in a comprehensive, timely and

MICK BRADY

Is a freelance technology communicator with more than 20 years of experience editing and writing for technology-focused publications.

FIGURE 1

Core IR Tool Stack

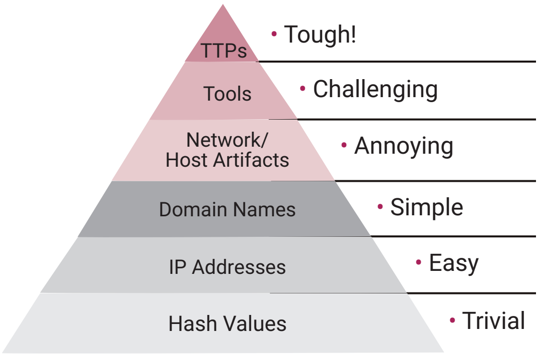


efficient manner, Eitan noted. An organization experiencing a ransomware attack on its network, for example, needs to respond quickly and, preferably, automatically. The old way—that is, physically logging in to each endpoint, copying the memory disk, indexing the data based on predefined components and then running a full forensics investigation—is no longer a scalable solution against cyberattacks. In any case, it is virtually impossible to apply it in a cloud or hybrid environment.

- **Maximum intelligence**—Because the cyberthreat landscape is constantly evolving, defenders are challenged to stay up to date with the latest threats. In addition to incorporating signature-based monitoring and prevention, Eitan said, organizations should pursue near-real-time monitoring using the latest behavioral tactics, techniques and procedures (TTPs) and indicators of compromise (IOCs) (**figure 2**). The cyberops team at his financial institution was able to upgrade its intelligence program through multiple avenues. "Our business case resonated with the bank. We upgraded the program from feed-based to threat intelligence platform-based (TIP-based), which also supported other security teams in the bank, such as the antifraud unit that gets alerts on stolen credit card numbers. Further, my team helped shore up the IT infrastructure through prioritizing and expediting patch management based on the latest exploited vulnerabilities," Eitan said.

FIGURE 2

Pyramid of Pain—IOCs That Can Be Detected and Prevented



Source: Bianco, D. J.; "The Pyramid of Pain" Enterprise Detection and Response, 1 March 2013, *https://detect-respond. blogspot.com/2013/03/the-pyramid-of-pain.html.* Reprinted with permission.

- **Immediate and comprehensive response actions**—In addition to preventive capabilities such as blocking access by Universal Serial Bus (USB) devices and banning hashes based on their reputation, EDR provides a robust first response to malware found in endpoints. Vendors sometimes configure EDR to operate automatically. With a click of a button, the EDR tool may be able to kill suspicious/malicious processes, isolate targeted endpoints, enforce existing policies (e.g., whitelisting) to prevent malicious applications from running, or activate other incident responses that would take valuable time if implemented manually.
- **Sandboxing**—Filtering of files and code strings in an isolated and cloud-based environment is key to implementing a one-stop-shop EDR solution. In addition to sanitizing files, a sandboxing feature can record the various processes and running codes in the network, constantly making comparisons with suspicious scenarios. The rules should trigger alerts based on a scoring method that is aligned with the organization's incident response plan (IRP).

Although the bank lacked sufficient capabilities to detect and eradicate malware threats in a timely manner, its security strategy did have its strengths. Its existing SIEM and other endpoint security tools were advanced solutions with comprehensive capabilities for mitigating compliance risk and insider threats.

"The head of infosec was able to implement a state-of-the-art preventive control environment, which included high-level segmentation, secured Internet access, a strict public-facing server policy and a thorough patch management process," Eitan said.

Those strengths contributed to his most complicated challenge: getting buy-in for a more robust security program that could offer a similar level of protection against malware and advanced persistent threats (APTs). Eitan's primary objective at the time was to demonstrate to leadership that the most prominent threats would likely penetrate the bank's first line of defense, forcing response teams to contain and eradicate attacks on an already breached network.

Four-Pillar Mitigation Plan

To mount an offensive strategy in a war against determined cyberintruders, the bank needed security tools and personnel capable of identifying network compromises and malware insertions and eradicating them, Eitan said. He proposed a mitigation plan based on the MITRE ATT@CK framework's TTPs, an approach that couples extensive intelligence feeds with behavioral detection rules (**figure 3**).

The plan was designed to ensure that every associated project or initiative designated would not only address Order #361 regulatory directives, but also encourage buy-in for the purchase and implementation of a comprehensive EDR solution. It consisted of four key pillars:

1. Establish a three-tier operations model equipped with endpoint discovery and forensics investigation capabilities and based on an IRP.
2. Implement a proactive threat and vulnerability management program combining breach and attack simulation (BAS) with a TIP. Define processes to prioritize mitigation plans based on intelligence and attack simulation findings. Enrich detection and investigation based on tactical intelligence.
3. Institute a training program designed to benefit employees at all levels within the organization: tabletop exercises for C-suite executives, cyberexercises for the IT department, and hands-on training for the responders. (A new computer security incident response team [CSIRT] had recently been formed in the IT department as part of the cybersecurity program.)
4. Conduct a security control policy review and make configuration changes based on the threat landscape to secure the email gateway, vaults, IPS/IDS and web platforms (e.g., enterprise web email platforms, social media accounts).

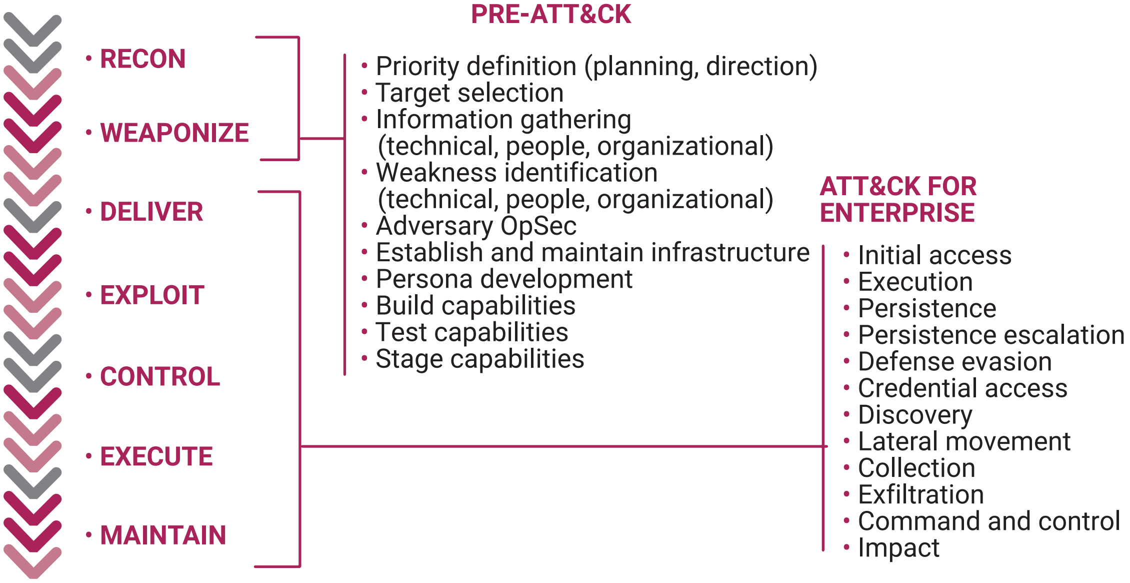
The proposal faced resistance. A new chief information officer (CIO) had been onboarded at the bank just as the cyberops team concluded its review, and he questioned the plan, mainly due to budgetary constraints and other pressing priorities.

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 3

MITRE ATT&CK Framework to Build Use Cases



Source: Burg, S.; "Introducing the MITRE ATT&CK Enterprise Framework Collection," Cyberbit, 17 August 2020, *https://www.cyberbit.com/cybersecurity-training/introducing-the-mitre-attck-enterprise-framework-collection-2/*. Reprinted with permission.

The bank's budget-constrained security plan was a bigger problem, though, because it would allow the deployment of agents only at endpoints where suspicious activity was detected by the SIEM for further forensics and endpoint discovery.

"The head of information security was the acting and primary cybersecurity leader. He reported to the CIO and I reported to the head of the information security department," Eitan explained. "It was the head of information security department's decision to establish a new team dedicated to designing and implementing a revised cybersecurity program. It was approved by the former CIO."

Problems arose when the new CIO chose to rethink the approval his predecessor had already given, Eitan noted. He had not been involved in approving formation of the team. He took note of all the security resources the bank had in place—thanks in large part to the head of information security department's efforts—and challenged the new cyberops team on the need for an EDR solution, given the multiple other agents in use to reduce risk.

To make the team's case, Eitan said he adopted a strategy "based on an intelligence analysis of global and local incidents to showcase how the bank could face similar fatal ramifications without properly defending against similar threats." He conducted a TTP[5] analysis and showed the attack kill chain, demonstrating that the bank's controls were insufficient to protect it.

At that time, ransomware attacks were just beginning to emerge, and the targets initially were home users. The CIO acknowledged that there were weaknesses in the bank's defensive system, but he believed the alarms raised in industry and media reports over advanced security threats were exaggerated. He said that further due diligence by the infosec team would be necessary to justify an EDR system. In the CIO's view, additional major investments in security tools were not immediately warranted, particularly since temporary financial constraints at the bank were resulting in delays in several initiatives for the following year.

Setting Plan B in Motion

Eitan was directed to focus on developing the incident response plan and training program first, but his team persisted in seeking buy-in for its overall recommendations. "WannaCry[6] was the beginning of the turning point," he recalled.

A ransomware worm that struck in 2017, WannaCry had a devastating global impact, encrypting files on hundreds of thousands of Windows computers and demanding ransom payments in exchange for decrypting them. However, most of those who paid ransoms did not have their access restored, so willingness to pay a ransom as a response tactic was exceedingly risky. Heavily regulated industries, such as banking institutions, were reluctant to do business with unreliable cybercriminals.

The ransomware threat soon mushroomed, demanding fast, effective action. At the bank, Eitan's team was permitted to acquire a low-budget host discovery tool, RSA-ECAT,[7] which was useful in demonstrating that the threat was real and immediate. The new tool detected attempts by prominent ransomware variants to breach the bank's unclassified WiFi network. Although bank operations were not impacted by that attempt, ransom notes and disarmed executables were found at multiple endpoints. Combined with the potential damage associated with WannaCry, that attack helped demonstrate that the threat was real and that attackers were knocking on the bank's doors.

However, there were significant downsides to relying on the RSA-ECAT system, said Eitan. It provided limited CTI feed integration and was not user-friendly. The RSA-ECAT deployment "was designed only for an aftermath threat scenario," Eitan said, "definitely not for a proper mitigation plan against ransomware, which distributes much faster than the bank's ability to reach proper agent saturation before the ransomware can impact the network."

The bank's budget-constrained security plan was a bigger problem, though, because it would allow the deployment of agents only at endpoints where suspicious activity was detected by the SIEM for further forensics and endpoint discovery.

The secondary projects and programs that were part of the original proposal were approved and funded—and their value subsequently demonstrated—but approval for the key piece, the EDR tool, was still on hold.

"We genuinely tried to find secondary alternatives to utilize to achieve similar functionalities," Eitan said. However, as the team implemented those other projects, it used them specifically for the purpose of achieving buy-in for the EDR.

In addition to creating an incident response plan, the team wrote up EDR and SIEM use cases, developed TIP integrations, built tier 1-3 operating models and designed a training program. It reevaluated all current agents and the existing control environment based on the IRP and use cases. Although the team achieved several quick wins with the available tools, such as implementing some threat feeds and blocking malicious hashes, the improvements were far from what a comprehensive EDR solution could offer.

None of the measures were adequate EDR substitutes, but they served to prove the team's business case for stronger threat detection:

- **BAS**—Demonstrated how prominent threats (e.g., ransomware, advanced persistent threats [APTs], behavioral TTP) could potentially breach the network
- **Threat landscape analysis**—Defined the scope of the top priority threats with supporting case studies
- **Training**—Triggered discussions about the bank's ability to mitigate prominent threats

Eventually, the team managed to accomplish everything necessary to go forward with an EDR implementation, including benchmarking for desired solutions and identifying the people, processes and technologies necessary for integration with other tools, such as the SIEM, TIP and email gateway. The only thing left to do was get approval and start the EDR project.

Presenting a united front in support of the business case tipped the balance in favor of acquiring an EDR solution.

Revisiting the Case for EDR

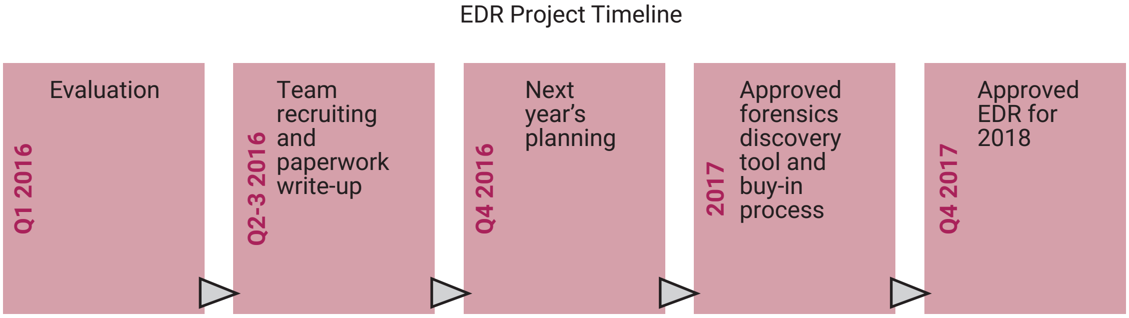
Eitan sought—and obtained—buy-in from other prominent figures at the bank, including the chief revenue officer (CRO), relevant IT directors and the head of the information security department. To underscore the importance of their goal, he and the head of the information security department adopted a motto that likened EDR to antivirus (AV) software: "EDR is the new AV—it's a must for every organization."

Presenting a united front in support of the business case tipped the balance in favor of acquiring an EDR solution. The agenda presented by some of the IT teams involved in maintaining the control environment also helped achieve buy-in. Those team members advocated for the need to acquire and implement an EDR solution and expressed support for all the efforts incorporated in the IR program (i.e., the development of an IRP and a training program, the creation of use cases, and the integration of threat intelligence feeds).

After nearly two years of working toward the implementation of an EDR, Eitan was gratified to see it finally approved (**figure 4**).

FIGURE 4

Timeline for Gaining Approval of the EDR Proposal



EDR Project Timeline

Although Eitan started working in the United States and was no longer with the bank by the time its EDR project was complete, his control mapping report demonstrated two critical findings:

1. The risk assessment was high regarding the top threats to the bank (i.e., ransomware, espionage APT, terror/destructive APT). It demonstrated high severity and probability based on intelligence analysis and security control evaluation.
2. The threat mapping demonstrated that without EDR it would not be possible to detect several key threats. Further, the bank's capabilities for responding to data breaches were not streamlined, and its capabilities for mitigating a ransomware outbreak were insufficient.

With its EDR implementation fully deployed, the bank would enjoy a much-improved security posture, with substantially reduced risk and vastly improved threat detection and response capabilities.

Endnotes

[1] Bank of Israel, "Banking Supervision," *https://www.boi.org.il/en/BankingSupervision/SupervisorsDirectives/Pages/nihultakin.aspx*

[2] Supervisor of Banks, "Proper Conduct of Banking Business Directive (9/21) [2] Cyber Defense Management," Israel, 30 September 2021, *https://www.boi.org.il/media/422h2aed/361_et.pdf*

[3] Wright, G.; A. Gillis; "Endpoint Detection and Response (EDR)," *TechTarget*, April 2021, *https://www.techtarget.com/searchsecurity/definition/endpoint-detection-and-response-EDR*

[4] National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC), "Blue Team," USA, *https://csrc.nist.gov/glossary/term/blue_team*

[5] National Institute of Standards and Technology Computer Security Resource Center, "Tactics, Techniques, and Procedures (TTP)," USA, *https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures*

[6] Fruhlinger, J.; "WannaCry Explained: A Perfect Ransomware Storm," *CSO*, 24 August 2022, *https://www.csoonline.com/article/3227906/wannacry-explained-a-perfect-ransomware-storm.html*

[7] RSA, "New RSA ECAT Release Engineered to Extend Ability to Rapidly Detect and Block Advanced Threats on Endpoints," PR Newswire, 22 July 2015, *https://www.prnewswire.com/news-releases/new-rsa-ecat-release-engineered-to-extend-ability-to-rapidly-detect-and-block-advanced-threats-on-endpoints-300116802.html*