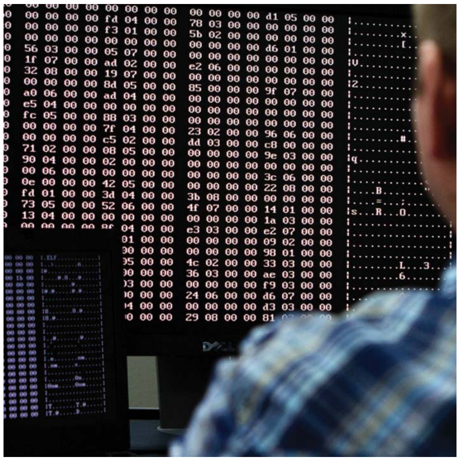

BDO Israel

Micro Focus ArcSight's maturity and scalability enables BDO to save clients hundreds of thousands in CapEx costs, deliver consistent results for demanding MSSP clients, and more.

Overview

BDO Israel is spearheading the global accounting giant's worldwide marketing efforts for a new managed security service focused on detection and response. As a hotbed of cyber security startups and innovations, Israel offers the ideal environment, including a pool of cyber experts to lead the effort.

BDO Israel got off to a fast start by acquiring a market-leading Israeli cyber security consulting firm, SECOZ. In the process, BDO Israel added 30 top cyber security experts, who formed the core of the firm's new Cyber Security Center. The new service, built on the Micro Focus ArcSight security information and event management (SIEM) platform, went live in late 2016 and is now being rolled out to BDO's global client base.

The cyber warriors at the heart of BDO Israel's new Cyber Security Center offer the experience of hundreds of successful SECOZ engagements, many featuring the use of the ArcSight Activate Framework.

> **"With ArcSight, we get the multitenancy we need to serve multiple clients, and we can easily replicate the custom content we've created. I've used ArcSight for 15 years and I know it'll be there tomorrow and can connect to anything. That cleared the table of other considerations."**
>
> **DORI FISHER**
> Head of Managed Cyber Security Services
> BDO Israel

Challenge

Cyber crime is projected to cost the world $2 trillion by 2019, according to a report by Juniper Research. Researchers at Cybersecurity Ventures predict that ransomware—a form of malware made infamous by the May 2017 "WannaCry" attacks—is expected to exceed $5 billion in damages in 2017.

To counter the surge in cyber crime, enterprises are moving away from prevention-only strategies to focus more on detection and response. In a recent report by Gartner, Inc., analysts noted that spending on information security is expected to hit $90 billion in 2017, an increase of 7.6 percent over 2016, and to top $113 billion by 2020. Spending on detection and response is expected to be at the top of the shopping list.

At a Glance

- **Industry**
  Financial Services
- **Location**
  Israel
- **Challenge**
  BDO needed to build and launch a world-class cyber security center to protect clients.
- **Products and Services**
  ArcSight Data Platform
- **Success Highlights**
  + Dramatically reduced false alarms for clients
  + Reduced false positives to a very low percentage
  + Pinpointed the specific location and device where a WannaCry alert comes form
  + Saved clients hundreds of thousands of dollars in capital expenses, compared to building in-house capability

Solution

"We believe that in order to deliver a robust and reliable managed detection and response (MDR) service, we need a core platform that is tested and flexible enough to meet the needs of our clients here and around the world," notes Dori Fisher, Head of Managed Cyber Security Services for BDO Israel. "I'm very familiar with this product segment, so IBM was the only other solution I considered. We want to be able to both create advanced scenarios and rely a lot on correlation. Other solutions don't go there, leaving our analysts with too much to process.

"We use ArcSight to create our own connectors and parsers," Fisher continues. "With ArcSight, we get the multi-tenancy we need to serve multiple clients, and we can easily replicate the custom content we've created. I've used ArcSight for 15 years and I know it'll be there tomorrow and can connect to anything. That cleared the table of other considerations."

The BDO Cyber Security Center implemented Micro Focus ArcSight Enterprise Security Manager (ESM) and ArcSight Data Platform on the Amazon Web Services (AWS) cloud computing platform. Approximately 80 percent of the MSSP/MDR's clients take advantage of the AWS option, while the remaining clients have their own implementations of ArcSight, which BDO monitors.

The client base for BDO's new cyber security services is immense and growing broader every day. "We were a successful advisory organization for 15 years before we became part of BDO," notes former SECOZ founder and CEO Ophir Zilbiger, now a BDO Israel Partner and Head of the firm's Cyber Security Center. "We have seen an evolution from what was called information security in past years to what is now cyber security. This evolution came early here in Israel due to the fact that we produce so many cyber-trained people, thanks in large part to the training provided in our armed forces. Clients here are very aggressive and early adopters of new security technology. We believe our early experiences in this burgeoning field will help differentiate us in the global market."

Results

Client Base Evolving

Zilbiger notes that not only has the nature of information system security evolved in recent years, so too has the type of clients. "Our largest clients in the past have been financial services, telecom, and the technology sector," he says. "We have seen a shift from what I would call traditional security clients to a wider range of clients, due to the ubiquitous nature of cyber crime today. We are seeing many more government organizations, as well as more manufacturers who are late adopters, but now committed to cyber security."

False Alarms Fading from Client Experiences

According to Fisher, ArcSight ESM and ArcSight Data Platform have enabled the new MSSP/ MDR to dramatically reduce false alarms for their clients. "ArcSight allows the most flexible correlation infrastructure, which means that the majority of false positives that have logged artifacts can be improved and honed," he explains.

"With ArcSight, we create or use scenarios that are based on hypotheses that were created using over a decade of client experiences," Fisher notes. "Once these scenarios are manifested, we are able to reduce false positives to a very low percentage. For instance, we can quickly reduce false positives by tenfold as we hone correlations over a short time."

He notes that for a client with 1,000 users, BDO would use ArcSight Data Platform to collect approximately 30 million log lines (events) per day, and use ArcSight ESM to create an average of less than 10 alerts per day. "Our goal is to chase down false positives once, and then automate the procedure," Fisher says.

He gives this example: "Perhaps we decide that we want to reduce the amount of alerts associated with accessing suspicious websites because we're getting 50 percent false positives. We might use ArcSight to automate the website checkup so that only websites that were considered 'bad' by two antivirus vendors actually invoke an investigation. ArcSight ingests the antivirus result data and our analysts get only sites that are flagged by both threat intelligence and antivirus. The magic here is that we control the amount of false positives by tuning and understanding what works best for us—ArcSight is flexible enough to allow us to do that."

> "Thanks to the technical maturity of ArcSight and our experience with the solution, we are able to provide a service that is applicable anywhere in the world and scalable to meet the needs of even the largest enterprises."
>
> **OPHIR ZILBIGER**
> Partner and Head of BDO Cyber Security Center
> BDO Israel

Contact us at:
www.microfocus.com

Like what you read? Share it.

Protecting Clients from Malware

The BDO Cyber Security Center employs a combination of manual and automated techniques to ingest cyber threat intelligence (CTI) into ArcSight ESM, including indicators of compromise (IOCs) relating to malware such as WannaCry. "The automatic insertion of CTI is based on selected open source feeds ingested daily, parsed, and moved into dynamic lists within ArcSight ESM," says Fisher. "We also manually insert CTI based on reports and artifacts reported in the media or from closed groups, but not widely available in lists of IOCs or indicators of attack (IOAs)."

IOC and IOA lists are cross-correlated within ArcSight with various devices in real time, which could include firewalls, proxies, and mail relays. The night that WannaCry was initially detected, the BDO team read the reports and inserted the indicators into the manual threat intelligence list. Two weeks later, they received a WannaCry alert from a client system. Because the client's locations were mapped in ArcSight, the BDO team was able to pinpoint the specific floor and device. The local helpdesk disconnected the system for further investigation. It turned out that the IP address involved was associated with WannaCry, but not actually infected by the malware.

"We erred on the side of safety in this case due to the potential high impact," says Fisher.

Clients Save Hundreds of Thousands in Capex BDO

Israel's new MSSP/MDR offering can save clients hundreds of thousands of dollars in capital expenses when compared to the investment required to build an in-house capability.

"The number one challenge is the global shortage of skilled cyber security professionals," Fisher notes. "Although MSSPs are popping up everywhere, most are not as deeply focused as we are on detection and response. Clients would have to invest at least three to five times as much as they spend on our service to build their own cyber security organization, that is if they could even find people with the needed skill sets."

Zilbiger concludes, "We have partnered with [Micro Focus] on a global basis to achieve our goals for the BDO Cyber Security Center and our MSSP/ MDR offering. We have worked with [them] for many years and found that [their] experience and willingness to support us as a true partner has been a key to our success. Again, thanks to the technical maturity of ArcSight and our experience with the solution, we are able to provide a service that is applicable anywhere in the world and scalable to meet the needs of even the largest enterprises."