INDIAN RIVER COUNTY, FLORIDA

MEMORANDUM

TO: Jason E. Brown, County Administrator

DEPARTMENTAL

FROM: Dan Russell, Information Technology Director

SUBJECT: End Point Protection (EPP) / End Point Detection & Response (EDR) and Managed Detection & Response Procurement Recommendation

DATE: January 12, 2021

BACKGROUND:

On October 22, 2020, the Indian River County (IRC) Board of County Commissioners (BoCC) network was the target of a cyber-attack. Fortunately, the IRC Information Technology (IT) Department staff discovered the attack in progress and were able to successfully mitigate the attack with no loss of data. The IRC BoCC staff did experience a limited, self-imposed, loss of certain technology services while a forensic investigation was conducted to ensure that any unauthorized access to the network was eradicated. Subsequent to completing the forensics investigation, the IRC IT staff examined the attack vectors that were deemed contributory to the attack and determined that the current end point protection (EPP) & anti-virus (AV) software should be upgraded to assist with detection and response to future cyber-attacks.

ANALYSIS

The EEP & AV software currently in use is signature based. This type of anti-virus software relies upon pre-distributed malware signatures to detect anomalous computing or network behavior. Signatures are updated on a recurring basis; however, the detection capabilities of this type of legacy software are limited to known malware attacks and do not provided protection against new or previously unknown malware attacks. Cyber criminals are constantly innovating the techniques used to conduct their attacks. Legacy AV software is inherently disadvantaged when it comes to detecting attacks for which signatures have yet to be developed. Next generation (Nextgen) EEP & AV software solves this dilemma via the additional of Extended Detection & Response (EDR) functionality.

EDR is an integrated end point security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities to enable cyber security teams to quickly identify and respond to threats. The primary functions of an EDR security system are to:

1. Monitor and collect activity data from end points that could indicate a threat.
2. Analyze that data to identify threat patterns.
3. Automatically respond to identified threats to remove or contain them, and to notify cybersecurity personnel.
4. Provide forensics and analysis tools to search for/research suspicious activities.

EDR tools work by monitoring endpoint and network events and recording the information in a central database where further analysis, detection, investigation, reporting, and alerting take place. A software agent installed on the host system provides the foundation for event monitoring and reporting. Most EDR tools address the “response” portion through sophisticated analytics that identify patterns and detect anomalies, such as rare processes, strange or unrecognized connections, or other risky activities flagged based on baseline comparisons. This process can be

automated so that anomalies trigger alerts for immediate action or further investigation. Many endpoint detection and response tools also allow for manual or user-led analysis of data as well.

New features and services are expanding EDR solutions' ability to detect and investigate threats. For example, third-party threat intelligence services increase the effectiveness of endpoint security solutions. Threat intelligence services provide an organization with a global pool of information on current threats and their characteristics. That collective intelligence helps increase an EDR's ability to identify exploits, especially multi-layered and zero-day attacks. Many EDR security vendors offer threat intelligence subscriptions as part of their endpoint security solution.

Additionally, new investigative capabilities in some EDR solutions can leverage AI and machine learning to automate the steps in an investigative process. These new capabilities can learn an organization's baseline behaviors and use this information, along with a variety of other threat intelligence sources, to interpret findings.

Another type of threat intelligence is the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) project underway at MITRE, a nonprofit research group that works with the U.S. government. ATT&CK is a knowledgebase and framework built on the study of millions of real-world cyberattacks. ATT&CK categorizes cyberthreats by various factors, such as the tactics used to infiltrate an IT system, the type of system vulnerabilities exploited, the malware tools used, and the criminal groups associated with the attack. The focus of the work is on identifying patterns and characteristics that remain unchanged regardless of minor changes to an exploit. Details such as IP addresses, registry keys, and domain numbers can change frequently. But an attacker's methods—or "modus operandi"—usually remain the same. An EDR can use these common behaviors to identify threats that may have been altered in other ways.

In preparation for making this recommendation, the IRC IT staff reviewed a number of EPP and EDR tools from various suppliers. The list software products considered for recommendation was reduced to the list below because these particular products each met all of the criteria of an EDR solution, as described above.

1. Sentinel One; 2. Carbon Black; 3. Crowdstrike; 4. GreyMatter; 5. Rapid7; 6. Secureworks

Of the products reviewed the Sentinel One EPP & EDR product was deemed to best meet the County’s requirements based on a combination of functionality and price.

As previously noted, it is possible to automate the EDR system response to many, but not all, of the alerts generated by end points. The EDR system must be actively monitored to ensure that all alerts are responded to appropriately. The IRC IT staff considered three options for monitoring the EDR system.

1. Monitor the EDR system with IRC IT Staff
2. Managed Detection and Response (MDR) through a professional services supplier
3. MDR & prepaid cyber Incident Response (IR) through a professional services supplier

The options above are presented in order of risk reduction with option #1 carrying the most risk and option #3 the least. They are ordered in a good, better, best format.

Option #1 - using the IRC IT staff to monitor the EDR system is the option that carries the most residual risk as the IRC IT staff is not staffed to provide 24 x 7 monitoring support and does not specialize in cyber incident detection and response. Option #2 - using an MDR service through a supplier reduces this risk by providing 24 x 7 monitoring and response provided by cyber security professionals that perform this function daily and as such are intimately familiar with current and evolving cyber-attack techniques. Option #3 - using an MDR supplier to perform monitoring & detection and prepaying for cyber incident response (IR) support has the added benefit of having a cyber incident response team available to support immediately upon detection of a cyber breach

rather than having to contract that support after detection. Cyber incident mitigation is a time critical activity and having IR support already in place provides the most risk reduction to the County.
IRC IT staff has obtained quotes from multiple suppliers for the Sentinel One product without MDR, with MDR, and with MDR & prepaid IR. The tables below summarize the cost of each of these options from the 3 least expensive suppliers. In all cases the quotes are based on 750 end points; which includes all County managed servers, desktops and laptop computers. All quotes all include the option for one additional month of event data retention. The default event data retention supplied by Sentinel Labs is 14 days. The additional month is required to ensure that sufficient event data is available to conduct forensic analysis in the event that IRC experiences a cyber incident. Event data is overwritten on a first in first out basis. Without sufficient historical event data is it often not possible to complete a forensic investigation and to ensure that a cyber breach is completely eradicated.

Table 1.0 – Option #1 – End Point Protection (EPP) and Extended Detection & Response (EDR) Software Only – Monitoring Performed by IRC IT Staff on an 8 x 5 Basis

Supplier	**Product**	**Quantity**	**Cost per end point (12 Months)**	**Extended Cost (12 Months)**	**Total Extended Cost (12 Months)**
True Digital	Sentinel One EPP+EDR; 14-day retention	750	$40.55	$30,412.50	
	Additional 1-month data retention	750	$12.40	$9,300.00	
					$39,712.50
SHI	Sentinel One EPP+EDR; 14-day retention	750	$44.76	$33,570.00	
	Additional 1-month data retention	750	$12.15	$9,112.50	
					$42,682.50
Compuquip	Sentinel One EPP+EDR; 14-day retention	750	$46.26	$34,695.00	
	Additional 1-month data retention	750	$12.55	$9,412.50	
					$44,107.50

Table 2.0 – Option #2 – End Point Protection (EPP) and Extended Detection & Response (EDR) with 24 x 7 Managed Detection and Response

Supplier	**Product**	**Quantity**	**Cost per end point (12 Months)**	**Extended Cost (12 Months)**	**Total Extended Cost (12 Months)**
SHI	Sentinel One EPP+EDR; 14-day retention	750	$38.37	$28,777.50	
	Addition 1-month data retention	750	$12.01	$9,007.50	
	Vigilance Respond 24x7 MDR	750	$16.45	$12,337.50	
					$50,122.50
Compuquip	Sentinel One EPP+EDR; 14-day retention	750	$39.65	$29,737.50	
	Addition 1-month data retention	750	$12.41	$9,307.50	

	Vigilance Respond 24x7 MDR	750	$17.00	$12,750.00	
					$51,795.00
True Digital	Sentinel One EPP+EDR; 14-day retention; Additional 1-month data retention	750	$4,500.00	$54,000.00	
	True Digital 24x7 MDR	750	$0.00		
					$54,000.00

Table 3.0 – Option #3 – End Point Protection (EPP) and Extended Detection & Response (EDR) with 24 x 7 Managed Detection and Response & Prepaid Incident Response (IR)

Supplier	**Product**	**Quantity**	**Cost per end point (12 Months)**	**Extended Cost (12 Months)**	**Total Extended Cost (12 Months)**
True Digital	Sentinel One EPP+EDR; 14-day retention; Additional 1-month data retention	750	$4,500.00	$54,000.00	
	True Digital 24x7 MDR (1 year)	750	$0.00		
	True Digital 40 hours IR Consulting	1		$10,000.00	
					$64,000.00
SHI	Sentinel One EPP+EDR; 14-day retention	750	$35.62	$26,715.00	
	Addition 1-month data retention	750	$11.32	$8,490.00	
	Vigilance Respond Pro24x7 MDR and incident response (up to 20 hours)	750	$34.66	$25,995.00	
	Vigilance Respond 40 hours IR Consulting	1		$10,322.59	
					$71,522.59
Compuquip	Sentinel One EPP+EDR; 14-day retention	750	$36.82	$27,615.00	
	Addition 1-month data retention	750	$11.70	$8,775.00	
	Vigilance Respond Pro24x7 MDR and incident response (up to 20 hours)	750	$35.81	$26,857.00	
	Vigilance Respond 40 hours IR Consulting	1		$10,666.68	
					$73,913.68

Staff recommends SHI as the supplier for this work. Both SHI and Compuquip prepared their quotes using Sentinel Labs as the supplier for the MDR and IR services. Sentinel Labs is the company that produces the Sentinel One EEP & EDR software product. True Digital opted to

quote their own MDR & IR services. Staff believes that the depth and breadth of the technical talent present within the Sentinel Labs organization far exceeds that of the True Digital organization based on the differences in the market capitalizations of the two organizations and the resources available to each. SHI submitted the least expensive quote using Sentinel Labs as the supplier for MDR & IR services. The quotes submitted by each vendor are available for review in the IT Department.

FUNDING

The funding for Option #3 EPP, EDR, and IR in the amount of $71,522.59 will be provided by a budget amendment from IT Fund/Cash Forward October 1st.

RECOMMENDATION

Staff recommends that the Board of County Commissioners approve Option #3 – End Point Protection (EPP) and Extended Detection & Response (EDR) with 24 x 7 Managed Detection and Response & Prepaid Incident Response (IR). Staff further recommends the Board waive the requirement for bids for these services and authorize the Purchasing Division to issue a Purchase Order to SHI International Corp. in the amount of $71,522.59. Finally, Staff recommends the Board Authorize the County Administrator to execute any agreements necessary for these services after the County Attorney has approved them as to form and legal sufficiency.

ATTACHMENTS

None

DISTRIBUTION

Kristin Daniels, Director Management and Budget