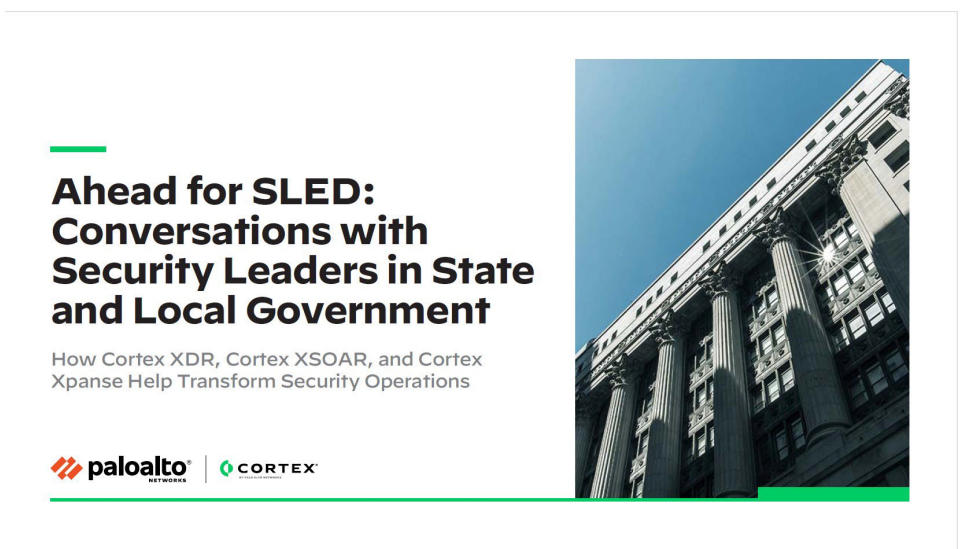
Ahead For SLED: Conversations with Security Leaders in State and Local Government

How Cortex XDR, Cortex XSOAR, and Cortex Xpanse Help Transform Security Operations



For more information, contact Carahsoft or our reseller partners:
PaloAltoNetworks@carahsoft.com | 855-6NEXTGN

Thank you for downloading this Palo Alto Networks' presentation.Carahsoft is the Master government aggregator and distributor for Palo Alto Networks' Cybersecurity solutions available via GSA, The Quilt, NUSBA and other contract vehicles.

To learn how to take the next step toward acquiring Palo Alto Networks Solutions, please check out the following resources and information:

For additional resources:

carah.io/PANWResources

For additional Palo Alto Networks solutions:

carah.io/PANWSolutions

To purchase, check out the contract vehicles available for procurement:

carah.io/PANWContracts

For upcoming events:

carah.io/PANWEvents

To set up a meeting:

PaloAltoNetworks@carahsoft.com or

855-6NEXTGN

carahsoft

For more information, contact Carahsoft or our reseller partners:

PaloAltoNetworks@carahsoft.com | 855-6NEXTGN

Ahead for SLED: Conversations with Security Leaders in State and Local Government

How Cortex XDR, Cortex XSOAR, and Cortex Xpanse Help Transform Security Operations

paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

The National Association of State Chief Information Officers (NASCIO) recently released State CIO Top 10 Priorities: Priority Strategies, Management Processes and Solutions for 2023. Topping other issues on the list, such as cloud services, digital government, and legacy modernization, was cybersecurity and risk management, which includes:

- Governance
- Budget and resource requirements
- Security frameworks
- Data protection
- Training and awareness
- Insider threats
- Third-party risk

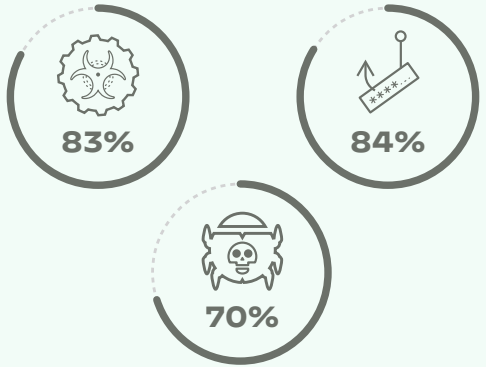
In January 2023, NASCIO also released its 2023 federal advocacy priorities that reflect the importance of collaboration between states and the federal government, consisting of:

- Expanding and strengthening the state cyber workforce.
- Harmonizing disparate federal cybersecurity regulations.
- Ensuring responsible implementation of the state and local cybersecurity grant program.
- The continuing adoption of the .gov domain.

Beyond the challenges inherent in creating a comprehensive security strategy, state, local, and education (SLED) organizations must continually navigate prevalent (and in some cases stifling) red tape. Agencies deal with rules and regulations at state and local levels, as well as federal regulations and requirements. Securing their infrastructure is typically the responsibility of understaffed and underfunded cybersecurity teams who are struggling with poorly integrated point products deployed without a strategic approach.

As agencies invest in digital transformation and cloud services, government databases are becoming rapidly digitized as modernization efforts replace legacy systems and operations. Furthermore, state and local governments often store critical and personal information and data about citizens as a part of welfare and administrative functions. That data is an attractive target for cybercriminals who can readily monetize it on the dark web.

In August 2022, the Center for Digital Government conducted a national survey of SLED leaders on the topic of cybersecurity, collecting 141 total responses. The survey's goal was to capture insight into the types of cybersecurity threats organizations face and how they manage resources to combat those threats. The top three cybersecurity threats were **ransomware (83%)**, **phishing (84%)**, and **malware (70%)**.[1]



"State governments are increasingly providing services to county and municipal governments, including endpoint protection, shared service agreements for cyber-defensive tools, incident response, and statewide cybersecurity awareness and training."

– National Association of State Chief Information Officers

A recent Government Accountability Office (GAO) report listed the top obstacles at the federal level, though their findings are relevant to all levels of government. Specifically, agencies across the board face challenges in:

- Maintaining a skilled workforce
- Ensuring cybersecurity
- Procuring cloud services
- Tracking costs and savings

Limited Budgets

Despite forthcoming funding from the Infrastructure Investment and Jobs Act, state and local governments, including K–12 districts and higher education, continually struggle with budgeting and paying for cybersecurity initiatives. The Infrastructure Investment and Jobs Act makes $1 billion available to improve cybersecurity, with a call for each state to develop a comprehensive cybersecurity plan. States that develop plans are eligible for monies to be distributed over three years, and they must consult with localities to align their cybersecurity plan with the needs of local governments. States can then pass some of the funding in the form of grants to local governments within their jurisdictions.

States identify cybersecurity as an area that requires more attention and resources for a reason. Seventy percent of respondents report either the state educational agency (SEA) or at least one local educational agency (LEA) was the victim of a cybersecurity threat or attack in the past year.[2] One respondent shared, "We see thousands of attacks of all kinds yearly. In 2021, we had nearly 1,000 [Distributed Denial of Service] attempts alone. This happens at the LEA, municipal and higher ed levels."[3]

Cybersecurity and privacy were consistently identified as high priorities for technology in survey responses, yet respondents also indicated that resource allocations often don't align with the level of priority.

* Source: State EdTech Trends.

Threats from Ransomware

Key findings in our 2022 commissioned research with the Center for Digital Government (CDG) show nearly 80% of state and local IT leaders believe ransomware is an ongoing threat to their organizations, and it won't diminish anytime soon.[4] **Yet, less than half of the respondents (47%) currently have a ransomware incident response plan in place.**[5]

Cyber extortionists are demanding ransom not only to unlock the data they encrypt but also to prevent that data from being publicly released on the dark web. Survey respondents offered the following insights into the cybersecurity issues currently impacting SLED IT organizations:[6]

- Nearly 80% of survey respondents said they do not think the threat of ransomware will decrease significantly over the next 12 to 18 months.
- Although cybersecurity budgets have increased, respondents may not be as prepared as they need to be to protect against the increasing volume and sophistication of ransomware attacks.
- Recent stimulus funding and the passage of the Infrastructure Investment and Jobs Act present important opportunities to address gaps in cybersecurity. Survey respondents said investing in new technology, augmenting staff capabilities, and working with third-party experts will be crucial to protect against ransomware attacks.
- When asked what organizations could do to better protect against ransomware attacks, the top two answers were providing employees with security for their home networks (41%) and hiring more IT staff (37%).

About SACA—Strengthening American Cybersecurity Act of 2022

The combined bill, known as the Strengthening American Cybersecurity Act, will require critical infrastructure owners and operators and civilian federal agencies to report to the Cybersecurity and Infrastructure Security Agency (CISA) if they experience a substantial cyberattack. It would also require critical infrastructure owners and operators to report ransomware payments to CISA, modernize the government's cybersecurity posture, and authorize the Federal Risk and Authorization Management Program (FedRAMP) to ensure federal agencies can quickly and securely adopt cloud-based technologies that improve government operations and efficiency.

SACA has three parts:

- First, it updates federal cyber laws to improve coordination and communication among federal agencies and requires them to share cyber incident information with CISA.
- Second, it requires the reporting of cyber incidents against critical infrastructure.
- Third, it streamlines the processes for how federal agencies receive approval to use cloud technologies.

About Our Interviews

Palo Alto Networks commissioned Zeus Kerravala of ZK Research to interview the following customers at Ignite '22, our customer-focused conference. Some of the questions and answers have been edited for brevity.

City of Gainesville, Georgia

Snapshot	Product	Objectives	Outcomes
• 800 users • 2 data centers; 15 city facilities • IT Staff of 11 to manage all departments and services in the city (including police and fire services)	Cortex XDR Pro	• Consolidate point products without compromising on key security components • Eliminate redundancy and data silos • Reallocate resources by removing tier 1 analysts to save money • Use all the features on existing investments	• Cortex XDR replaced endpoint protection, detection, and response and the need for a SIEM • Let machines do the work using automation • Tier 1 is automated • Investigations are quicker and easier with Cortex XDR's automated root cause identification and automated correlation • Consolidation of tools and products

Q&A with Jonathan Reich, CIO

Palo Alto Networks Customer for 7+ Years

Q: What were some of the challenges you were seeing with your security team and operations that caused you to go out and look for a different type of solution?

A: Six years ago, the XDR concept was really getting started, and I think, like everybody else, we were using traditional antivirus (AV) at the time. Between traditional AV and next-gen AV, there's some machine learning in that, but it still didn't solve the problem with zero days, and the stuff that's new and nobody knows about. XDR really was a no-brainer once we started to really look into it, and [Palo Alto Networks] did a great job showing us what we needed to see. We had some onsite demos—great tool. We've been using it since it was called Traps 4.0.

We're really starting to think about how we can use the data we get with XDR because it's rich. From those endpoints and from the network side and from the cloud, it provides us lots of data, so now we're trying to figure out how we take it to the next step and automate it.

Q: Has it allowed you to consolidate functions too?

A: We did, but it wasn't done in the way you think. With the smaller budgets and the smaller groups, we were living off the land with regards to an antivirus solution that we won't name. We made the straight jump, and what it did was it allowed us to continue maintaining without asking for really much more money. So our benefit wasn't that I got to repurpose or I got to consolidate; it was now I get to do more with the same.

Q: How have you measured the benefit that it brought you?

A: There's a couple ways. The most obvious is I don't have as many users or staff working to collect the data. We aren't worried about going and fixing the problems anymore. They're stopped. So the level of information we're getting, the protection we're getting, is just awesome. We often do training with staff, but the training only goes so far. We have to be able to fix it or prevent it before it even starts.

So our benefit, again, being a small shop, was I got to really accelerate how we defend, accelerate how we protect, accelerate how we gather that data, and it's been just great. I mean, I can't say enough good things.

Q: Have you been able to quantify the change in threats caught and fixed before and after you deployed XDR?

A: Yes and no. Using the traditional way, we didn't catch a lot of things. We didn't know what we were looking for. We went into a whole cascade of data or an experience that hadn't been quantified really because it was a different breed. And so I think the way we say it is the number of alerts has started to go down. As soon as we made that change, the stuff that we knew about was fine because that was being handled before. Now I'm getting notified on things that are real versus, say, a ton of false positives. Now, we're catching things beforehand, which is huge.

Q: What about from a staffing perspective? There's a lot of talk about the great resignation, skills shortages in cybersecurity, and high attrition rates, especially for SOC analysts who get burnt out. Do you see that, and has this helped?

A: This potential recession and the fact that we are having a hard time finding staff is real. I think everyone would admit that. I think what we're learning is when we get partnered with education, like college and high school and the groups that are learning, we try to catch them then and say, "Intern with us. Let's spend some time." We go educate. We go out and try to help the school systems and the colleges to tweak how they're talking to their students. It helps us, then they automatically call me and go, "Hey, I'm out of school. You got a job?" And I go, "No." Or I do, and we talk from there.

But the world we're living in only makes it so that it's harder without the tools to ensure we're getting all the data we need to. I mean, instead of it taking four hours to do an investigation, I have the data in 10 minutes. The tools are helping us with the staffing because I don't have to have all of this knowledge come in right away.

Q: When you first introduced XDR, did you get any hesitation from your staff about automation or AI capabilities that could potentially take away any job functions?

A: Nothing. In fact, it was so exciting to the team that they turned and said, "Wow, we didn't even know that was happening. Or we didn't know this was a problem." It was really, really culture-changing because we were able to say, "Now we see things you couldn't see before." We were in the dark. Just based on the technology changes. It was so changing to the environment that I think the team was able to start thinking differently, and that's really the key to me.

Q: What's your utopian vision for what the SOC would look like? Would it be something that's fully automated? Would the machines assist your engineers?

A: We want to make it more efficient, and I think there's a combination of automation and humans. I think humans belong in the SOC. I think it's more of a supervisory role and let the machines do what they're supposed to do. I mean, somebody's got to put eyes on it, somebody's got to validate, somebody's got to make notifications and just validate that we're seeing what we're seeing. And I think the more it matures and the more that process can be tuned to the processes we have, I mean, it could be less and less humans, but I still think there is a part that humans need to be the checksum of sorts.

"We were in the dark. Just based on the technology changes. It was so changing to the environment that I think the team was able to start thinking differently, and that's really the key to me."

– Jonathan Reich

Q: What are other things coming that you're excited about or see as promising?

A: I wish there was some way I could say it's the totality of Palo Alto [Networks] data. I'm excited about the way the data's coming together and how we can use it, such as being able to take that machine learning data and tuning it even more. And the more data we put in, the more logic we get out of it. Something I want to talk about is all about knowledge and training, the training of that AI or machine learning; however you want to reference it. And once that becomes more active or more knowledgeable, the logic becomes smarter and faster.

NORTH Dakota
Be Legendary.™

State of North Dakota

Snapshot	Product	Objectives	Outcomes
• Technology and IT services for 800,000 citizens and state organizations	Cortex XDR Prevent, Cortex XDR Pro, Cortex XSOAR, and Cortex Xpanse	• Secure and protect North Dakota's citizens' data and the state's network and systems • Launch a next-generation security operations center • Build resilient security capabilities to detect and defend against cyberthreats • Provide the means to automate, with AI and ML, tasks and processes for added protection and efficiency to free up NDIT engineers and analysts to focus on the most urgent threats with a risk-based response • Resolve a backlog of thousands of items in security operations and introduce tools for keeping abreast of emerging threats • Meet KPIs to provide measurable results, both before and after their SOC was operational	• Their SOC is now operating with a unified framework for cybersecurity to reinforce their security operations and enable the state's digital workforce • Improvement in the strength of their security posture and threat hunting capabilities • Has a more transparent organizational structure, mapping to National Institute of Standards and Technology (NIST) frameworks and activities

Q&A with Michael Gregg, CISO

Q: Give me a sense of what the state of your SOC was when you joined that led you down the path that you felt needed transformation?

A: For us, the real challenge was in 2019, when Senate Bill 2110 was signed into law. After that date, we had cyber authority to engage and defend all of North Dakota's state government. We not only had to protect a very small number of endpoints but provide protection for the entire state. Our challenge was: How do we, in two years, grow from 20,000 endpoints to 200,000 endpoints and do it seamlessly?

Q: What does XDR mean to you? What kind of data are you using to fuel the XDR engine?

A: XDR to me means that I have the toolset rolled out and wired into my SOC. When we have an incident or an event, my team can be alerted, and they can respond quickly. Without tools like XDR in place, think of it as the analogy of a fire department and a fire; the fire could burn very big, and it could spread to many houses before we know or could respond. XDR gives us the ability to respond quickly and isolate it when it's isolated to one endpoint and has not spread to 50 or more.

What we're using, as far as data, is an expansive set of metrics. The analogy I would use: Imagine if you drive your car or truck tonight and you didn't have any headlights, dash lights, you didn't know how fast you were going, and you didn't know how much fuel you had in your vehicle. How could you determine your path forward? When I came on board, one of the very first things I did was develop the dashboards and metrics to measure our progress and to be able to calculate what we needed to do to hit our end goal of protecting all of STAGEnet.

Q: What's the post-XDR environment like now compared to what you had before? Have you been able to quantify the benefits?

A: Oh, it's totally different. We have reduced our response time across the board. Our mean time to resolution is down by more than 90%. We were able to reduce those metrics primarily through automation and machine learning.

Q: Regarding automation, have you seen a change in attitude from the engineers using the products?

A: Yes, because the big thing it did for us was allow us to act on threats quickly. Keep in mind we detect about four-and-a-half billion attacks per year. Most of those are managed through automated means. We manually process about 50,000 per year; half of that 50,000 is actually phishing. Using automation has allowed me to move the team off of many manual phishing activities. Our SOC analysts can take on other, more productive tasks, such as threat hunting, purple team activities, pen-testing, and even sharpening the saw to train and prepare for the next big event. This is only possible because they're not having to manually work these phishing incidents.

Q: What about XSOAR? Are you bought into the vision of the fully autonomous SOC eventually? Or how have you brought that in and integrated that into operations?

A: That's been huge for us because, as I mentioned, we manually respond to about 1% of detected threats. That's about 50,000 incidents we work manually. So really, where I'd like to have my team spend their time is on high-impact events and not items that we can automate resolution for.

XSOAR is also useful in getting basic metrics to evaluate the reduction in response time when we add additional automation. Most of this work, I would describe as small, incremental improvements. Each time we make a change, we evaluate, "Was the juice worth the squeeze." With XSOAR, we are able to get the metrics quickly when we make these incremental improvements. Over time, these small, incremental improvements have gotten us to the point where we can automate almost all phishing. This has allowed us to free up those individuals, so they can do other things. One big item we highlight is training. We have analysts on the cyber range each month to practice and grow their incident response skills. Just as important, this reduces burnout by removing repetitive tasks.

Q: What other things have you been able to automate outside of phishing?

A: What we've done is review all of our playbooks. I had the team do a Gemba Walk. The idea is simple: Get a fresh view, have others break the paradigm, and find new creative ways to automate existing tasks. We brought together our resident engineers, SOC analysts, and our internal automation engineers. I had them work as one for just a few hours each week for three months. The result was that we were able to remove about 2,800 hours worth of work from the SOC analysts. The Gemba Walk was a creative way to find small, incremental improvements of items we could automate and then put them in place in our playbooks.

Why was this so important to me? Because, as a state entity, we have a fixed-size team. It's not like we can change the size of my staff. Imagine being in the private sector and being asked to grow your SOC's coverage from 20,000 to 200,000 endpoints and do it with the same amount of staff. Government funding is set. I did something some may think is impossible: I made a state government entity more efficient.

"Imagine being in the private sector and being asked to grow your SOC's coverage from 20,000 to 200,000 endpoints and do it with the same amount of staff. Government funding is set. I did something some may think is impossible: I made a state government entity more efficient."

– Michael Gregg

Q: Now, what about Cortex Xpanse? How have you used that, and what's your experience been?

A: Xpanse has been a really good tool for us. We've integrated that into our operations, and that's helped us bring all the pieces together—our security infrastructure team, the active defense teams, and our governance risk and compliance team. Improved correlation allows us to react and respond faster.

Q: By introducing these tools, have you had to restructure the security organization? Because often, endpoint security would be one group and network security would be another.

A: Yes. One of the things I did when I came on board about three years ago was to restructure the teams. The idea was to create an environment where the stakeholders could collaboratively work together, gathering information, analyzing data, and respond to indicators of compromise and threat actors quickly. We restructured the teams, which allowed us to put everything in place for the growth we've had.

Q: Palo Alto Networks recently introduced Cortex XSIAM. Are you looking at XSIAM as a replacement for what you're using now?

A: We're actually working with Palo Alto [Networks] as a design partner on XSIAM. We're looking at it very closely because previously, in the state, we had multiple, different SIEMs. So, our goal is to remove these and unify with one product. This is the path we are moving down.

Q: Since you are using all the Cortex tools here, have you found that there's a multiplying effect using them together?

A: Very much so. As I talk about that growth and the journey we've been on, having Palo Alto Networks as a partner has been one of the key things that's helped us do just that. The other great thing about it is as we got ready to grow our tools, such as XDR, to the cities, counties, schools, and other political subdivisions, they wanted specific items from the dashboards that XDR did not provide. I shared this concern with Palo Alto [Networks], and we talked to their development team in Israel.

Well, in less than three months, Palo Alto [Networks] helped us develop those dashboards, which actually became scope-based access control (SBAC) and allowed us to meet our customers' reporting and metrics needs. Together, North Dakota and Palo Alto [Networks] worked as one. Because we listened to our customers and Palo [Alto Networks] listened to us, we were able to reach our goal and meet our deployment numbers. This describes the journey we've had with Palo [Alto Networks].

Q: When you're through with this XSIAM deployment, what's your vision for what your SOC will look like then?

A: What I'd like to see our SOC look like in the next three-to-five years: 80% to 90% of the work has been automated, a centralized data lake, and for that team to have the time to grow their skills and services we offer. If we can do this, we can extend the amount of time that people generally spend in a SOC. Normally in a SOC, you'll only get a year, two years out of an individual before they burn out and are ready to go. If we can expand the breadth of the activities they do and the types of activities they do, we can keep them longer. We can benefit from their experience while they advance their skills and abilities.

City of Glendale, California

Snapshot	Product	Objectives	Outcomes
• Fourth largest city in Los Angeles County by population • Sixth largest city in Los Angeles County by area • Information technology department acts as a service provider to 13 different departments within the City of Glendale	Cortex Data Lake and Cortex XDR Prevent; PA-220, PA-220R, PA-850, PA-3050, PA-3250, and PA-5250 Next-Generation Firewalls; Panorama	• Replace legacy firewall, virtual private network, and endpoint protection solutions with Palo Alto Networks Next-Generation Firewall platform (NGFW, GlobalProtect, Cortex XDR, Cortex Data Lake) • Implement Tor and BitTorrent blocking in new library architecture • Implement FIPS 140-2-compliant encrypted tunnels between public safety sites • Establishment of highly available firewall and virtual private network services	• Easily build powerful protection policies • Gain visibility to see what is going on in the background as traffic flows through the city's network • Centralized and analyzed threat intelligence • Unscheduled service interruption risk reduction • Improved network segmentation

Q&A with Eric Brumm, Chief Information Technology Architect

Palo Alto Networks Customer for 6+ Years

Q: Tell me about your security environment. I understand you don't have a traditional SOC. How do you monitor what's going on?

A: We don't have a SOC today. We don't have anybody on staff whose job is primarily security, believe it or not. We've got some tools that actually are helping us look at a few things in our environment. We use Cortex XDR for endpoint protection, and we get a fair amount of alerting out of that for the important stuff that gets caught and knocked down. We've got Logic Monitor in place for doing system-level monitoring, infrastructure monitoring, and we're using Palo Alto [Networks] firewalls in our environment fairly extensively. So we do get some alerting back out of that platform as well.

Q: When you say XDR, what do you think about it?

A: It is so different from the traditional virus protection that was engine and definition driven. It's the ability to find things that are bad going on in your system and really sort of break it down to the fundamentals and stop them.

That, to me, is really the power of the platform. Its ability to use intelligence and figure out what's going on and stop things dead in their tracks without static definitions. To me, that's really the power of the product.

Q: From an XDR standpoint, what sources of data are you using?

A: Well, we utilize Palo Alto [Networks] Cortex Data Lake service, and we're pumping all of our logs that are coming off the nodes in our environment into it. We're also pumping all the firewall logs in there as well. So, we've got all that data that we can go back to and analyze and work with if we have incidents that need to be investigated basically.

Now we're deeply looking at the data. When we have an incident that occurs in our environment, we dig into that data very deeply, and we look at what did the node do, what did it interact with, what websites did they go to, what sort of traffic did it pump across the network? So there's a whole lot more to it than what it can tell you. What did it launch, what executed, who's the user that did it?

There's a whole lot of detail there that doesn't exist with traditional products, and you can't just pull it out of Windows system logs. Oftentimes when we find out about these things, it's days after they've occurred, and oftentimes the Windows system logs are just completely gone by that point.

Q: Even the most seasoned security pros can't look through all those log files and data and information like that to connect the dots manually. So, from a data perspective, what have you seen?

A: Well, I'll tell you, it's nuts. We sized up our firewalls originally when we put them in place, and we sized up the logging that we thought was going to come out of the XDR environment. We invested in Cortex Data Lake, and we started pumping the data in, thinking we were going to get about a year's worth of data in there. And the reality is now we're only getting about three months' worth of logs out of our firewalls and our Cortex XDR environment in there before it fills up.

It's an amazing amount of data it puts in. Part of that is obviously tuning how much we're pumping into the Data Lake, so there's a little bit of work we need to do, tune that down, but I'm surprised at how much data it collects. But I'm also very encouraged. We've done a few investigations where we've had to dig deeply into that data, and it's amazing how much is actually there.

There is just a plethora of data in its ability to identify what's gone on and where things have touched within the environment. To me, that's super impressive, and I think that there's a lot of advances from it. Part of the reason we invested in the Data Lake was because of the marketplace around it and the ability to have other vendors' products tie in and then apply more intelligence to that Data Lake. We're really committed to continuing to use a centralized repository of logging information with intelligence wrapped around it to glean and garner more information out of that.

Q: What was the process of incident resolution, like pre-XDR versus post-XDR?

A: Well, I can tell you, it's a great example of a change that XDR has made in our environment. We had a lot of malware infections that occurred in our environment. We were using another company's point solution in the past. It supposedly had an enterprise console. But the reality of the matter was we were seeing workstations infected right and left just off of internet browsing, malware-type infections on machines, mostly just annoying slowdowns, systems that didn't run well. But our help desk analysts, our support technicians were basically pulling back about 10 systems a day and having to wipe them out and rebuild them. 10 hours per machine, rebuilding them by hand with no automation.

Just an amazing amount of workload was being chewed up by doing that, and by putting what, at the time we purchased, it was called Traps, but by putting the solution in place, XDR has basically cut it down to next to nothing. We're not doing any node rebuilds because of nefarious stuff. I won't say none; there probably have been a few that we've had to do.

But the reality is, we went from spending thousands of hours a year worth of manpower rebuilding machines simply because of malware infections to basically spending no time on that at all, which has freed us up to do things like put automation for system rebuilds in place.

"But the reality is, we went from spending thousands of hours a year worth of manpower rebuilding machines simply because of malware infections to basically spending no time on that at all, which has freed us up to do things like put automation for system rebuilds in place."

– Eric Brumm

We put more intelligent tools in place to do some of the rote-level functionality you would expect people to normally be able to do within your environment. And it has freed us up to be able to implement automation in our environment where we didn't have it before. It's really allowed our entire group of people to become better and more knowledgeable in modern technologies and to basically articulate the environment with tools that allow us to manage, build, and maintain it better.

Q: I'm assuming that your staff also prefers the work they're doing now versus the mundane tasks of rebuilding?

A: Oh yeah, rebuilding nodes is horrible. It's a giant nightmare of migrating data and putting things back in place. And frankly, putting the automation in place to do those node builds was a godsend because now they can focus on other things. They've learned better and better technologies, newer technologies, new techniques of doing things that just didn't exist in the past. So, it's raised the level of our intelligence organizationally.

When I got into this environment, it was roughly 20 years behind in skillset, about 20 years behind in technology. We were using discrete servers in our data center. Every computer in the data center had a monitor and keyboard and a mouse on it. It didn't matter whether it was a Unix machine, whether it was a Linux machine, or whether it was running Windows on it. They all had that on them. We had water-cooled air conditioning in there, and we had no automation for node building in our environment whatsoever. It was all done by hand. We had a technician who sat in the basement of our building, and he would strip off all the vendor automatic-installed stuff and he would hand-install all the apps on it. And the best I ever saw the guy do was six machines in a single day.

Q: What is your vision for what you want your SOC to be?

A: The reality is having information is great. Having it there and available when you need it is the piece that's really important; put the tooling in place so it's available to you. Part of the challenge we run into in the city is that security is not an ingrained function. It's not something that they've really thought of over time. It is not limited to IT security; it's also in the physical security realm as well.

We don't have a centralized group that does video surveillance that does all the door locks in the city. It's a little bit wacky because of that, but from an IT perspective, the city's never gotten burned really hard with a super bad incident, and hence they haven't really funded it appropriately. So, I look at a SOC in the current formation of what our organization exists as being partial bodies putting part of their time to security with a lot of automation on the back end.

Ultimately, I think the city needs more formality, needs to understand their IT security a lot better than what they do today. And they need to immediately put some more money and funding into it and staff around it as well, whether it's internal staff or whether it's bringing outside entities to help us out. We just don't have enough of the right bodies today to do it, and it doesn't have the focus of senior management because they really haven't seen us get burned hard yet.

Q: So, your vision is really the autonomous SOC where the machines are the first line of defense, and then you bring in people when needed, versus the other way around, which is very manually driven?

A: Yup. When the automation can't connect the dots, then apply manpower to it, and hopefully improve for the future so it does connect the dots in the future.

Q: Since you're an XDR customer, are you looking at XSOAR or XSIAM?

A: I've been looking at XSOAR a bit, and it looks like it may have some potential within our environment to apply automation in areas we're not doing today. Simple stuff like, you have to be pretty smart to run the Cortex XDR console today. You have to really dig in, and it's a little different than some of the other Palo Alto [Networks] products. Putting some of this simple functionality, like the ability to push a button and isolate a node on the network, in the hands of our help desk technicians would be very valuable. Giving them access to everything that's in the Cortex console? Way too much for them.

I think that there's some great potential for us in putting some of the automation in place through that platform. Obviously, it's not as intelligent as things are going to be in a few years, but it's a step forward from where we're at today. And it allows us to do things that don't require people that have in-depth knowledge of the XDR platform to be able to go through and execute it.

It really allows us to focus our system engineers working on the things they need to be working on, and they work on a wide range of things. Security is one of the elements of what they work on. They maintain our serving infrastructure, our SAN [storage area network], our software distribution architecture, you sort of name it. They do all the really sophisticated stuff within our environment. So, having lower-level technicians be able to execute some of the things that need to be done really will free up those higher-end resources to work on better things. And it frankly allows the lower-end people to learn too.

Q: What's exciting about what you've heard here at Ignite?

A: Honestly, hearing them say that traditional SOCs are not going to exist in their current format in five years really energizes me. The reality is we probably can't get the funding internally to operate a traditional SOC as they've existed. But through artificial intelligence and machine learning, I think we can get to the point where we are providing near-world-class protection in our environment that we really can't do today.

It's going to be something very different. It's going to be driven by automation, machine learning. To me, that's really exciting because, ultimately, that's probably something that we can do with a sort of group of people we've got today.

Solve Your Top SecOps Challenges with Cortex

Cortex brings together best-in-class threat detection, prevention, attack surface management, and security automation capabilities into one integrated platform.

About Cortex XDR

Cortex XDR® has the ability to stop attacks at the endpoint and host with world-class EDR for Windows and Linux hosts, providing detection and response that focus on incidents by automating evidence gathering, groups of alerts associated, putting those alerts into a timeline, and revealing the root cause to speed up triage and investigations for analysts of all skill levels. Cortex XDR can be utilized in multiple permutations of SecOps architecture, providing enterprise threat detection and response with prevention capabilities that include EDR/EPP, particularly for organizations that do not require the full feature set of a SIEM. Cortex XDR can also be deployed with a SIEM to deliver EDR/EPP functionality, focused threat detection, response, and prevention.

About Cortex XSOAR

Cortex® XSOAR™ is a single platform for end-to-end incident and security operational process lifecycle management. Security teams of all sizes can leverage the extensive 900+ prebuilt integration content packs and robust security-focused case management with real-time collaboration to orchestrate, automate, and speed incident response and any security workflow or security process across their environment. In addition, with integrated threat intel management, security teams get a central threat library with the ability to automatically map threat information to incidents and operationalize threat intelligence with automation.

About Cortex Xpanse

Cortex® Xpanse™ provides a complete and accurate inventory of an organization's global, internet-facing cloud assets and misconfigurations to continuously and actively discover, learn about, and remediate exposures on an external attack surface, evaluate supplier risk or assess the security of M&A targets.

About Cortex XSIAM

Cortex® XSIAM™ natively integrates XDR, SOAR, threat Intel, ASM, and SIEM capabilities to power the autonomous SOC. Extended security intelligence and automation management (XSIAM) customers can consolidate multiple products into a single, coherent platform, cutting costs and improving analyst experience and productivity.

Learn More

Discover more resources that cover ways to strengthen SLED organizations' security posture and accelerate security maturity:

- A Practical Guide for Federal Agencies Adopting Zero Trust in the SOC
- The Statewide Next-Generation Security Operations Center: Defend Together

Visit our State and Local Government page for more information.

Keep Up with Current Security Trends

Download the 2023 Unit 42 Ransomware and Extortion Report to learn more about today's threat landscape, including:

- Ransomware and extortion trends and predictions
- Most-targeted industries
- Why having backups is no longer enough
- Best practices to protect your organization

References

1. "Top Cybersecurity Concerns in a Rapidly Evolving Landscape," Center for Digital Government, August 2022.
2. Liz Cohen and Evo Popoff, 2022 State of Edtech Trends Report, SETDA, August 2022.
3. Ibid.
4. *Smart Investments for Getting Ahead of Ransomware*, Center for Digital Government, February 21, 2022.
5. Ibid.
6. Ibid.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex_ebook_ahead-for-sled_041823