BUILD A NEXT-GENERATION SECURITY OPERATIONS CENTER

SPOTLIGHTS

Industry

All

Use Case

Build a Next-Generation SOC

What Is a Next-Generation SOC?

A next-generation SOC is where information systems in the data center, endpoint and cloud are monitored, assessed and defended against cyberattacks following a methodology that utilizes security enforcement points and threat research tools that integrate natively, rather than relying on security point products that do not natively interoperate.

Business Benefits

- Best-in-class prevention of cyberattacks
- Minimal operational expenditures (Opex) – scale the SOC with technology, not people
- Minimal capital expenditures (Capex) – decommission security point products and replace them with the natively integrated Next-Generation Security Platform

Operational Benefits

- Significant shift from manual, human-based processes and event analysis to machine-based automation, resulting in faster response times
- Significant decrease in events per analyst hour, resulting in more effective use of human capital for more sophisticated analysis and threat hunting

Technical Benefits

- Simplified security architecture
- Make actionable use of threat intelligence feeds and subscriptions by automatically blocking malicious IPs

Problems With Traditional SOCs

Security operations centers streamline the security incident handling process, and are used to triage and resolve security incidents efficiently and effectively. The concept of the SOC was invented to enable ease of collaboration among security personnel in a time when cyberattacks were primarily manual in nature. Nowadays, machine-based, automated cyberattacks are the norm and are challenging the SOC models that worked years ago.

As the internet has grown over the past decade, a number of problems have surfaced in the way traditional SOCs operate:

Problem #1: ***Scaling your SOC with people does not work.***

Historically, the answer to the growing problem of rising cyberthreats and the increased number of security incidents has been to hire more people in the SOC and ingest more threat intelligence feeds. This approach actually slows down the response to new threats and has become significantly less effective in today's growing threat landscape.

Problem #2: ***Employing experienced security staff is costly.***

Even larger organizations with SOCs are unable to hire enough experienced people to staff SOC teams capable of keeping up with the events, not to mention their need to take into account future growth of their businesses. Highly skilled SOC staff members are hard to find, hard to retain, and often command some of the highest salaries in IT.

Problem #3: ***Machine-based, automated cyberattacks overload SOCs.***

Malicious actors are increasingly using machine-based automation to conduct cyberattacks. A cyberattack defense that lacks machine-based automation results in more security events than most SOC teams can keep up with.

Problem #4: ***Security point products don't communicate natively, resulting in silos of security information and making automation difficult to implement.***

A decade ago, bleeding-edge security strategies involved the deployment of security point products. Many organizations followed that line of thinking and selected the best-of-breed security devices from the vendor with the best firewall, a different vendor with the best rated IDS/IPS, URL filtering and anti-malware, and so on. However, a core weakness with this security architecture surfaced: It's very difficult for disparate products to correlate their insights and reduce the time to detect an incident, much less prevent it without significant manual processes.

The lack of closed-loop automation and communication between security point products also created IT environments that were difficult to monitor; created silos between IT teams; and led to the reliance on security information and event management (SIEM) products, if they could afford it. SIEMs promised to tie together all the relevant security information into a single interface.

Problem #5: ***It is difficult to manually tune SIEM alerts to eliminate event noise and false positives.***

To a large extent, SIEMs succeeded in consolidating alerts into one interface; however, they focus on reacting to an incident after it has happened and typically don't effectively reduce the number of alerts or highlight the critical ones that require immediate action. They also don't enable the security functions to benefit from and inform one another of their latest insights.

It is common for large companies with SOCs, when they experience a breach, to report that their SOC received an alert, only to lose it in the rest of the noise. The Target breach is a well-known example. In that particular instance, an intrusion at the organization's HVAC contractor was used to gain access to Target's point-of-sale machines. An alert was triggered and sent to their SOC team, but no action was taken. There were too many alerts and far too few SOC analysts to investigate them all.[1]

Problem #6: ***SIEMs are expensive to maintain and are usually accessible only to larger organizations.***

SIEMS are typically implemented at organizations with bigger IT budgets that can afford the staff required to manually maintain the feeds and perform regular maintenance of the system.

Problem #7: ***Third-party intelligence feeds require manual response.***

As threats have grown in volume and sophistication, enterprise security teams have sought more insights on threats from a variety of sources, consuming and often investing in third-party threat intelligence feeds. This has been costly – both in financial resources for any paid subscriptions and in human capital for threat hunters to handle the review, deduplication, correlation and ultimately use of that threat intelligence.

What Is a Next-Generation SOC?

All SOCs are tasked to identify, investigate and mitigate threats within an organization. However, next-generation SOCs differ from traditional SOCs in a few philosophical ways, as well as in the underlying security technologies that drive them.

A next-generation SOC is a facility where information systems in the data center, network, endpoint and cloud are monitored, assessed and defended against cyberattacks. The SOC follows a methodology that utilizes security enforcement points and threat research tools that integrate natively, rather than relying on security point products that do not natively interoperate. Figure 1 shows some additional ways in which traditional and next-generation SOCs differ.

Traditional SOCs	Next-Generation SOCs
• Detect, react, remediate	• Anticipate, automate, prevent
• Security architecture is based on security point products that are difficult to integrate	• Security architecture is based on a next-generation security platform with enforcement points that natively integrate
• Data-driven methodology	• Intelligence-driven methodology
• As number of events increases, scale with people	• As number of events increases, scale with technology
• NOC and SOC work in silos	• NOC and SOC work in collaboration
• Threat intel must be is manually converted into enforceable policies	• Threat intel is automatically converted into enforceable policies

Figure 1: Primary differences between traditional SOCs and next-generation SOCs

[1] http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

Palo Alto Networks Approach Solves Common SOC Problems

Next-generation SOCs, or SOCs based on next-generation security technology, avoid alert overload by taking advantage of the native integration of a security platform. Native integration between components makes it possible to automate the blocking of critical threats more quickly, from the core of the data center and emerging cloud environments to remote endpoints.

Palo Alto Networks® Next-Generation Security Platform helps organizations consolidate the following security functions into a single, integrated architecture to take advantage of the faster detection and prevention of emerging threats through machine learning and automation. Hence, it is common for customers to remove multiple legacy security products, which also results in reduced Capex and Opex by scaling with technology, not people.

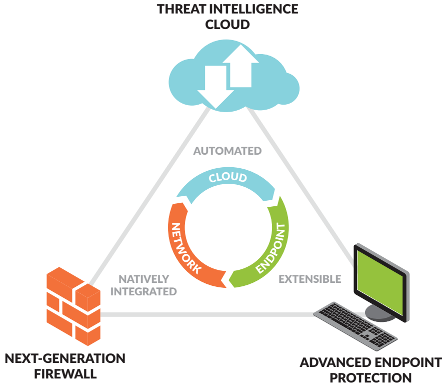


Figure 2: Palo Alto Networks Next-Generation Security Platform

The security platform does not eliminate the need for SOC analysts. Instead, it enables SOC analysts to focus primarily on threat hunting and analysis of only the most critical threats to the organization.

Security Function	Product
• Layer 7 firewall (physical and virtual) • Application whitelisting (including ICS/SCADA and SaaS) • URL filtering • Intrusion protection system (IPS) including anti-exploit • Intrusion detection system (IDS) • Network-based polymorphic anti-malware • Polymorphic command-and-control prevention • Credential theft prevention	• Next-Generation Firewall • URL Filtering subscription • Threat Prevention subscription
• Malware analysis environment (sandboxing) with automatic signature creation for closed-loop protection from new threats at security enforcement points	• WildFire subscription or appliance
• Device and policy management and threat visibility	• Panorama
• Endpoint-based anti-exploit (signature-less) • Endpoint-based anti-exploit	• Traps
• Threat intelligence analysis, hunting and response • Closed-loop preventive automation of threat intelligence feeds	• AutoFocus • MineMeld as stand-alone or part of AutoFocus
• SaaS application visibility, intellectual property protection and threat prevention	• Aperture

Figure 3: Core security functions provided by the Next-Generation Security Platform

These functions integrate with each other out of the box (where appropriate) and, when blocking of high-severity events is enabled, can significantly reduce the number of events on which SOC teams need to take action.

The next sections will help you understand how the products behind the Next-Generation Security Platform are used in concert by a next-generation SOC to solve the common SOC problems outlined earlier.

Easier Threat Hunting With the Automated Correlation Engine

The Next-Generation Security Platform uses a powerful automated correlation engine to quickly identify suspicious patterns and network anomalies in network traffic and, assuming blocking is configured, take action to stop them.

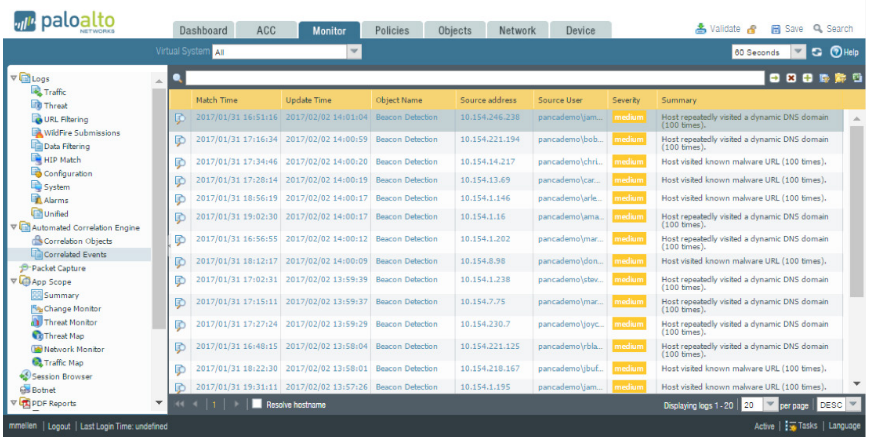
The next sections will help you understand how the products behind the Next-Generation Security Platform are used in concert with a next-generation SOC to solve the common SOC problems outlined earlier.

The automated correlation engine is an analytics tool that verifies compromised hosts in your network and cuts back on manual data mining requirements within your organization. It scrutinizes isolated events automatically across multiple logs, queries the data for specific patterns and correlates network events to identify compromised hosts. The engine includes correlation objects that identify suspicious traffic patterns or a sequence of events that indicate a malicious outcome. These objects can then trigger correlation events when they match on traffic patterns and network artifacts that indicate a compromised host on your network. Some correlation objects can identify dynamic patterns that have been observed from malware samples in WildFire™ cloud-based threat analysis service. The objects are delivered automatically with weekly updates to the Next-Generation Firewall and Panorama™ network security management as part of the Threat Prevention subscription.

Faster Responses. Also Less Expensive?

It is common for customers to decommission multiple legacy security products, resulting in reduced Capex, and to reduce Opex by scaling with technology, not people.

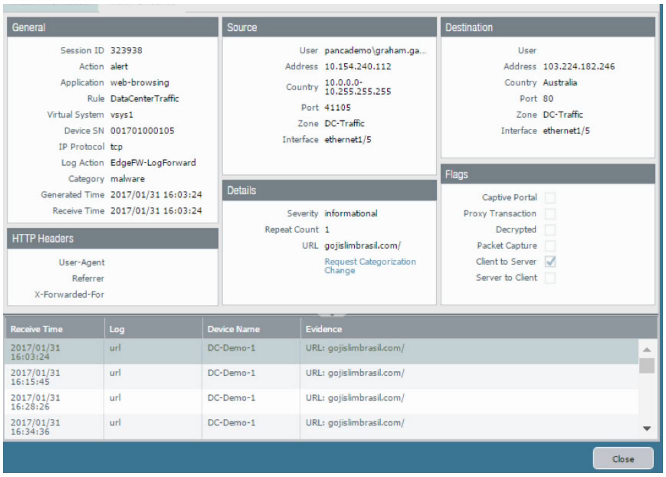
Figure 4 shows a screenshot of some correlated events within the Monitor tab. You can see here that the correlation engine discovered a number of endpoints that meet the criteria for the correlation object titled "Beacon Detection." In these medium-severity events, the host visited a known malware URL over 100 times.



Match Time	Update Time	Object Name	Source address	Source User	Severity	Summary
2017/01/31 16:51:16	2017/02/02 14:01:04	Beacon Detection	10.154.246.238	pancademo\jam...	medium	Host repeatedly visited a dynamic DNS domain (100 times).
2017/01/31 17:16:34	2017/02/02 14:00:59	Beacon Detection	10.154.221.194	pancademo\bob...	medium	Host repeatedly visited a dynamic DNS domain (100 times).
2017/01/31 17:34:46	2017/02/02 14:00:20	Beacon Detection	10.154.14.217	pancademo\chri...	medium	Host visited known malware URL (100 times).
2017/01/31 17:28:14	2017/02/02 14:00:19	Beacon Detection	10.154.13.69	pancademo\car...	medium	Host visited known malware URL (100 times).
2017/01/31 18:56:19	2017/02/02 14:00:17	Beacon Detection	10.154.1.146	pancademo\arle...	medium	Host visited known malware URL (100 times).
2017/01/31 19:02:30	2017/02/02 14:00:17	Beacon Detection	10.154.1.16	pancademo\ama...	medium	Host repeatedly visited a dynamic DNS domain (100 times).
2017/01/31 16:56:55	2017/02/02 14:00:12	Beacon Detection	10.154.1.202	pancademo\mar...	medium	Host repeatedly visited a dynamic DNS domain (100 times).
2017/01/31 18:12:17	2017/02/02 14:00:09	Beacon Detection	10.154.8.98	pancademo\don...	medium	Host visited known malware URL (100 times).
2017/01/31 17:02:31	2017/02/02 13:59:39	Beacon Detection	10.154.1.238	pancademo\stev...	medium	Host repeatedly visited a dynamic DNS domain (100 times).
2017/01/31 17:15:11	2017/02/02 13:59:37	Beacon Detection	10.154.7.75	pancademo\mar...	medium	Host repeatedly visited a dynamic DNS domain (100 times).
2017/01/31 17:27:24	2017/02/02 13:59:29	Beacon Detection	10.154.230.7	pancademo\joyc...	medium	Host repeatedly visited a dynamic DNS domain (100 times).
2017/01/31 16:48:15	2017/02/02 13:58:04	Beacon Detection	10.154.221.125	pancademo\rbla...	medium	Host repeatedly visited a dynamic DNS domain (100 times).
2017/01/31 18:22:30	2017/02/02 13:58:01	Beacon Detection	10.154.218.167	pancademo\jbuf...	medium	Host visited known malware URL (100 times).
2017/01/31 19:31:11	2017/02/02 13:57:26	Beacon Detection	10.154.1.195	pancademo\jam...	medium	Host visited known malware URL (100 times).

Figure 4: Example view of compromised hosts in the Correlated Events tab. Correlated events are triggered automatically based on indicators of compromise defined in Correlation Objects

In this example, the SOC could investigate these events further by drilling down deeper into the event details and determining if these PCs need to be tagged as compromised hosts and isolated for further investigation, as shown in Figure 5.



General

Session ID 323938
Action alert
Application web-browsing
Rule DataCenterTraffic
Virtual System vsys1
Device SN 001701000105
IP Protocol tcp
Log Action EdgeFW-LogForward
Category malware
Generated Time 2017/01/31 16:03:24
Receive Time 2017/01/31 16:03:24

HTTP Headers

User-Agent
Referrer
X-Forwarded-For

Source

User pancademo\graham.ga...
Address 10.154.240.112
Country 10.0.0.0-10.255.255.255
Port 41105
Zone DC-Traffic
Interface ethernet1/5

Details

Severity informational
Repeat Count 1
URL gojislimbrasil.com/
Request Categorization Change

Destination

User
Address 103.224.182.246
Country Australia
Port 80
Zone DC-Traffic
Interface ethernet1/5

Flags

Captive Portal □
Proxy Transaction □
Decrypted □
Packet Capture □
Client to Server ☑
Server to Client □

Receive Time	Log	Device Name	Evidence
2017/01/31 16:03:24	url	DC-Demo-1	URL: gojislimbrasil.com/
2017/01/31 16:15:45	url	DC-Demo-1	URL: gojislimbrasil.com/
2017/01/31 16:28:26	url	DC-Demo-1	URL: gojislimbrasil.com/
2017/01/31 16:34:36	url	DC-Demo-1	URL: gojislimbrasil.com/

Figure 5: Example of a drill-down view into a correlated event

Below are a few examples of correlation objects that are used by SOCs to automatically identify compromised hosts:

Name	Category	Description
Exploit Kit Activity	Compromised-host	This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
Compromise Activity Sequence	Compromised-host	This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
WildFire Correlated C2	Compromised-host	This correlation object detects hosts that have received malware detected by WildFire and have also exhibited command-and-control (C2) network behavior corresponding to the detected malware.

Traditional SOCs rely on point security products or a SIEM to tie disparate information together and identify potentially infected hosts. Any correlation that occurs across the point security products in a SIEM is achieved through a significant amount of human effort.

Next-generation SOCs seldom need to dedicate human effort to security event correlation activities like defining correlation objects. Instead, they rely on the shared collaborative nature of a security platform. Palo Alto Networks Unit 42 threat intelligence team does the hard work by regularly updating correlation objects like those previously listed and making the objects available to all customers.

Comparison of Compromised-Host Remediation Processes by Traditional SOCs Versus Next-Generation SOCs

Not only do next-generation SOCs require less hunting effort; they also greatly improve remediation efforts. A constant output of event correlation activities in a SOC is a list of compromised endpoints. Compromised endpoints are remediated by a process that blocks network access and remediates the issue, typically a malware infection.

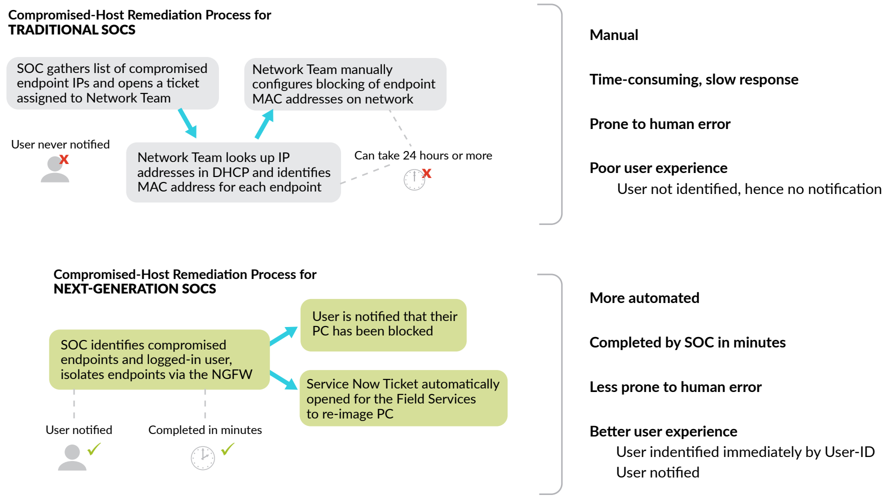

Compromised-Host Remediation Process for
TRADITIONAL SOCS
SOC gathers list of compromised endpoint IPs and opens a ticket assigned to Network Team
Network Team manually configures blocking of endpoint MAC addresses on network
User never notified
Network Team looks up IP addresses in DHCP and identifies MAC address for each endpoint
Can take 24 hours or more
Manual
Time-consuming, slow response
Prone to human error
Poor user experience
User not identified, hence no notification
Compromised-Host Remediation Process for
NEXT-GENERATION SOCS
User is notified that their PC has been blocked
SOC identifies compromised endpoints and logged-in user, isolates endpoints via the NGFW
Service Now Ticket automatically opened for the Field Services to re-image PC
User notified
Completed in minutes
More automated
Completed by SOC in minutes
Less prone to human error
Better user experience
User indentified immediately by User-ID
User notified

Figure 6: Comparison between compromised-host remediation process for traditional vs. next-generation SOCs

The endpoint remediation process executed by a traditional SOC is very different from that of a next-generation SOC. Next-generation SOCs offer a number of advantages as highlighted in this diagram:

SOC Tools

To extend the value of the platform, Palo Alto Networks has developed tools designed to improve or automate key functions that are standard practice within any SOC:

MineMeld™ threat intelligence syndication engine automatically correlates and deduplicates all threat intelligence feeds and automatically translates the insights into enforceable protection.

AutoFocus™ contextual threat intelligence service empowers SOC hunters with deep inspection into malware behavior within their environment and across their industry.

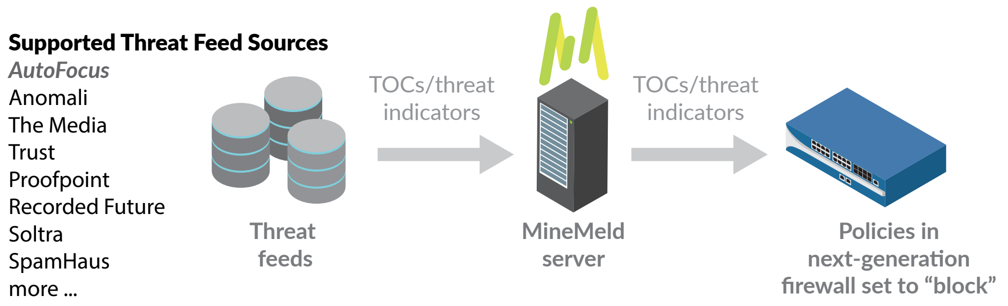
Logging and reports provide clear visibility over all network activity, application usage, users and threats.

Closed-Loop Threat Intel Automation With MineMeld

Every SOC relies on third-party threat intelligence feeds to build awareness of the latest threats. With **MineMeld,** SOC analysts can automatically translate public, private and commercial intelligence feeds, including results from other intelligence platforms, into new external dynamic lists in Palo Alto Networks and similar controls for other security devices. It is a free, open-source tool – which can also be purchased with full support as part of AutoFocus service, as noted on the following page – and reduces analysis time from analyzing, correlating and otherwise making actionable the numerous indicators within the analysts' overload of threat feeds. MineMeld automatically:

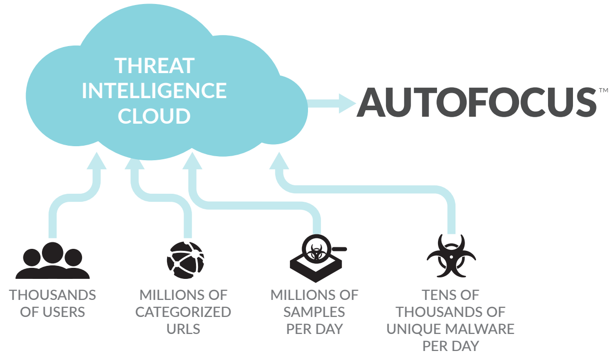
- Filters indicators
- Deduplicates indicators
- Retires indicators
- Consolidates metadata
- Publishes the indicators to network and endpoint points as block lists and/or shares them with the community

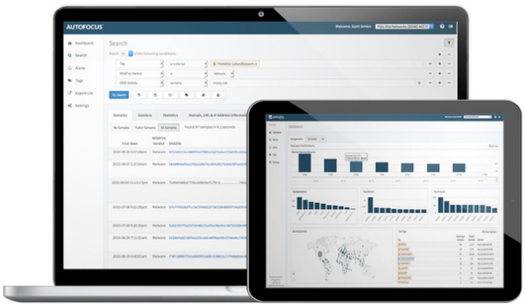
It can also be used to continuously retrieve indicators from Palo Alto Networks platforms and produce feeds that can be consumed by trusted peers and third-party security platforms.



Easy Threat Hunting With AutoFocus

AutoFocus is a threat intelligence analysis database and portal that allows SOC hunters to search on a potential threat seen in their own environment against the tens of thousands of unique malware variants and indicators of compromise (IOCs) in Palo Alto Networks global threat database. For example, a new kind of malware is all over the news – your CIO wants to know if the organization has been impacted. How long would it take your current SOC team to determine whether the same IOC has been seen in your environment? One search in AutoFocus can tell you instantly, so you can inform your CIO with confidence.


THREAT INTELLIGENCE CLOUD
AUTOFOCUS™
THOUSANDS OF USERS
MILLIONS OF CATEGORIZED URLS
MILLIONS OF SAMPLES PER DAY
TENS OF THOUSANDS OF UNIQUE MALWARE PER DAY



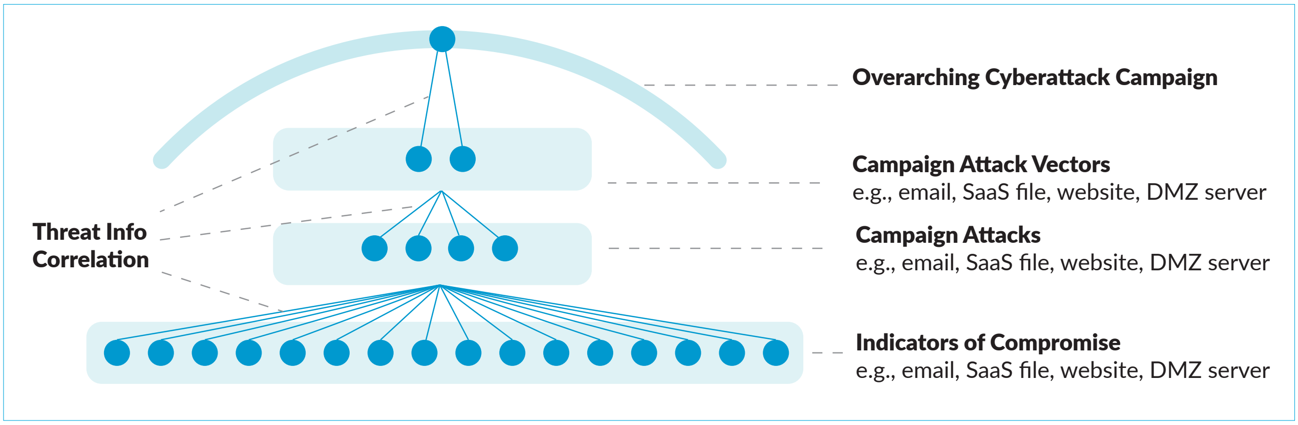

Overarching Cyberattack Campaign
Campaign Attack Vectors
e.g., email, SaaS file, website, DMZ server
Campaign Attacks
e.g., email, SaaS file, website, DMZ server
Threat Info Correlation
Indicators of Compromise
e.g., email, SaaS file, website, DMZ server

Figure 6: AutoFocus uses the platform's automated correlation engine to identify compromised hosts and tag each with additional cyberattack campaign information for improved context

AutoFocus enables your SOC to correlate malicious activities and indicators across all places on your network that could be used as attack vectors. The SOC can match indicators of compromise with particular attack campaign tactics and attack vectors, up to a broader attack campaign level – backward and forward in time.

Automation through the security platform, along with the correlated, full threat visibility in AutoFocus, enables the SOC to be faster at understanding, anticipating and protecting against new tactics or content – individually or as part of an attack campaign.

Reporting and Logging With the Platform's Management Portal

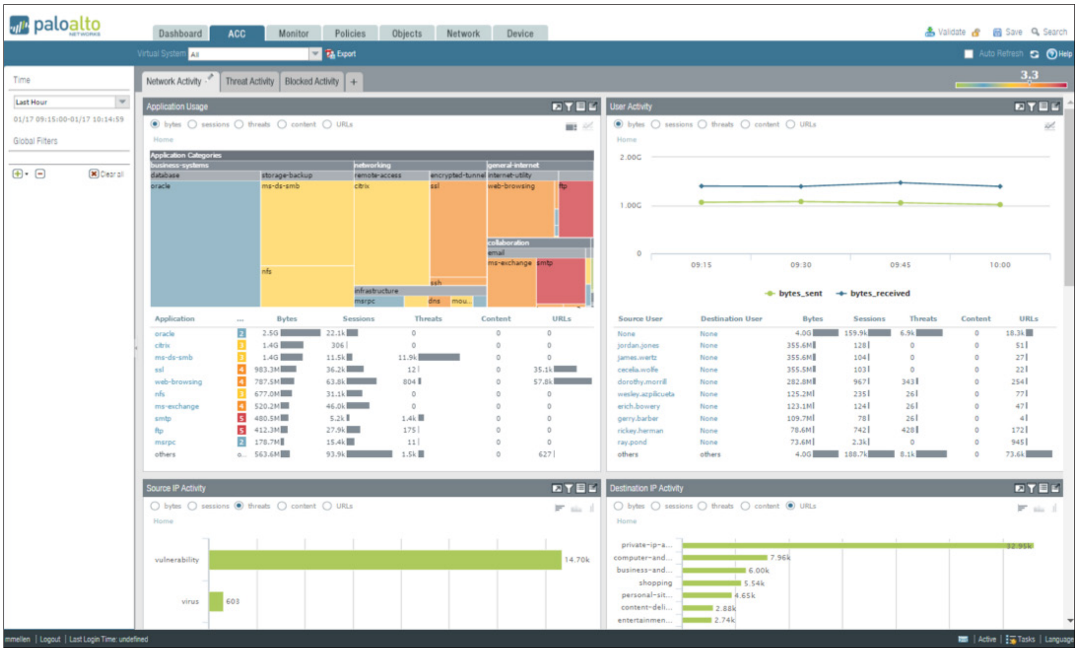
Visibility of critical information is crucial to a successful next-generation SOC. The Application Command Center and the Monitor sections of the management portal provide the SOC with visibility to quickly identify what's important and dig deep into potential threats.

Application Command Center

The ACC provides SOCs with a comprehensive view over all network activity, application usage, users and threats. It provides this visibility in a highly visual, customizable and interactive format, making it possible for the user to get answers to important questions fast. Dozens of widgets provide the desired level and visual display of data. Users can choose between different display options, such as tree, line or bar graphs, and can decide on the appropriate unit of measure (e.g., bytes, sessions, threats, content, URLs) by simply clicking the radio buttons on each widget.

Monitor Tab

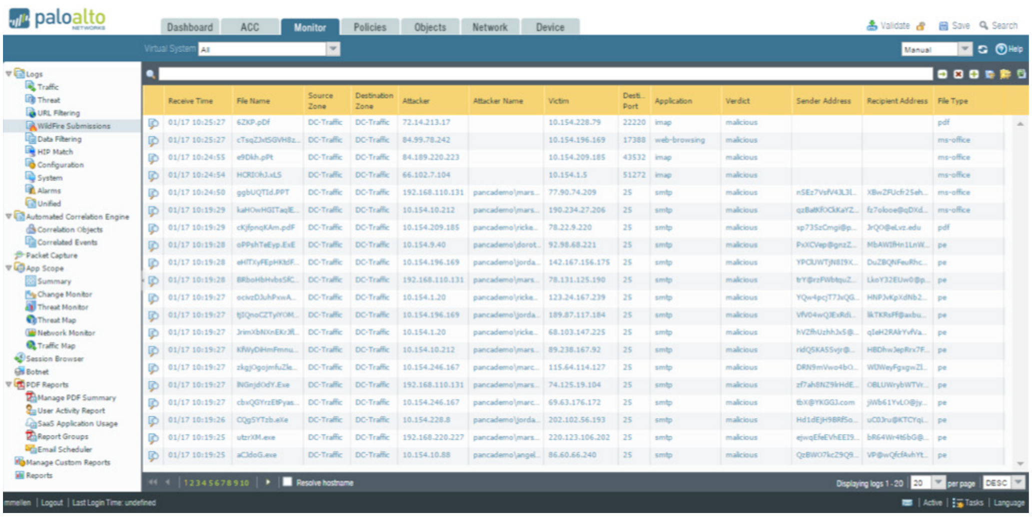
Palo Alto Networks logging, located in the Monitor tab of the UI (Figure 7 below), is divided into overall traffic, threat, URL, WildFire, data filter logging and more, to facilitate the organization of data.



Application	...	Bytes	Sessions	Threats	Content	URLs
oracle	2	2.5G	22.1k	0	0	0
citrix	3	1.4G	306	0	0	0
ms-ds-smb	3	1.4G	11.5k	11.9k	0	0
ssl	4	983.3M	36.2k	12	0	35.1k
web-browsing	4	787.5M	63.8k	804	0	57.8k
nfs	3	677.0M	31.1k	0	0	0
ms-exchange	4	520.2M	46.0k	0	0	0
smtp	5	480.5M	5.2k	1.4k	0	0
ftp	5	412.3M	27.9k	175	0	0
msrpc	2	178.7M	15.4k	11	0	0
others	o...	563.6M	93.9k	1.5k	0	627

Source User	Destination User	Bytes	Sessions	Threats	Content	URLs
None	None	4.0G	159.9k	6.9k	0	18.3k
jordan.jones	None	355.6M	128	0	0	51
james.wertz	None	355.6M	104	0	0	27
cecelia.wolfe	None	355.5M	103	0	0	22
dorothy.morrill	None	282.8M	967	343	0	254
wesley.azpilicueta	None	125.2M	235	26	0	77
erich.bowery	None	123.1M	124	26	0	47
gerry.barber	None	109.7M	78	26	0	4
rickey.herman	None	78.6M	742	428	0	172
ray.pond	None	73.6M	2.3k	0	0	945
others	others	4.0G	188.7k	8.1k	0	73.6k

Figure 7: ACC provides a highly visual, interactive and customizable user experience



Receive Time	File Name	Source Zone	Destination Zone	Attacker	Attacker Name	Victim	Desti... Port	Application	Verdict	Sender Address	Recipient Address	File Type
01/17 10:25:27	6ZKP.pDf	DC-Traffic	DC-Traffic	72.14.213.17		10.154.228.79	22220	imap	malicious			pdf
01/17 10:25:27	cTsqZJxtSGVH8z...	DC-Traffic	DC-Traffic	84.99.78.242		10.154.196.169	17388	web-browsing	malicious			ms-office
01/17 10:24:55	e9Dkh.pPt	DC-Traffic	DC-Traffic	84.189.220.223		10.154.209.185	43532	imap	malicious			ms-office
01/17 10:24:54	HCRIOhJ.xLS	DC-Traffic	DC-Traffic	66.102.7.104		10.154.1.5	51272	imap	malicious			ms-office
01/17 10:24:50	ggbUQTId.PPT	DC-Traffic	DC-Traffic	192.168.110.131	pancademo\mars...	77.90.74.209	25	smtp	malicious	nSEz7VsfV4JL3l...	XBwZFUcfr25eh...	ms-office
01/17 10:19:29	kaHOwHGITaqlE...	DC-Traffic	DC-Traffic	10.154.10.212	pancademo\mars...	190.234.27.206	25	smtp	malicious	qzBaBKfOCkKaYZ...	fz7olooe@qDXd...	ms-office
01/17 10:19:29	cKjfpnqKAm.pdF	DC-Traffic	DC-Traffic	10.154.209.185	pancademo\ricke...	78.22.9.220	25	smtp	malicious	xp73SzCmgi@p...	JrQO@eLvz.edu	pdf
01/17 10:19:28	oPPshTeEyp.ExE	DC-Traffic	DC-Traffic	10.154.9.40	pancademo\dorot...	92.98.68.221	25	smtp	malicious	PxXCVep@gnzZ...	MbAWIfHn1LnW...	pe
01/17 10:19:28	eHlTXyFEpHKtdF...	DC-Traffic	DC-Traffic	10.154.196.169	pancademo\jorda...	142.167.156.175	25	smtp	malicious	YPCUWTjN8I9X...	DuZBQNFeuRhc...	pe
01/17 10:19:28	BRboHbHvbsSfC...	DC-Traffic	DC-Traffic	192.168.110.131	pancademo\mars...	78.131.125.190	25	smtp	malicious	trY@rzFWbtquZ...	LkoY32EUw0@p...	pe
01/17 10:19:27	ocivzDJuhPxwA...	DC-Traffic	DC-Traffic	10.154.1.20	pancademo\ricke...	123.24.167.239	25	smtp	malicious	YQw4pcjT7JxQG...	HNPJvKpXdNb2...	pe
01/17 10:19:27	tjIQnoCZTyiYOM...	DC-Traffic	DC-Traffic	10.154.196.169	pancademo\jorda...	189.87.117.184	25	smtp	malicious	VfV04wQJExRdi...	lkTKRsFf@axbu...	pe
01/17 10:19:27	JrimXbNXnEKrJR...	DC-Traffic	DC-Traffic	10.154.1.20	pancademo\ricke...	68.103.147.225	25	smtp	malicious	hVZfhUzhhJx5@...	qIeH2RAlrYvfVa...	pe
01/17 10:19:27	KfWyDiHmFmnu...	DC-Traffic	DC-Traffic	10.154.10.212	pancademo\mars...	89.238.167.92	25	smtp	malicious	ridQ5KA5Svjr@...	HBDhwJepRrx7F...	pe
01/17 10:19:27	zkgjOgojmfuZle...	DC-Traffic	DC-Traffic	10.154.246.167	pancademo\marc...	115.64.114.127	25	smtp	malicious	DRN9mVwo4bO...	WlJWeyFgxgwZl...	pe
01/17 10:19:27	lNGnjdOdY.Exe	DC-Traffic	DC-Traffic	192.168.110.131	pancademo\mars...	74.125.19.104	25	smtp	malicious	zf7ah8NZ9lrHdE...	OBLUWrybWTVr...	pe
01/17 10:19:27	cbxQGYrzEtPyas...	DC-Traffic	DC-Traffic	10.154.246.167	pancademo\marc...	69.63.176.172	25	smtp	malicious	tbX@YKGGJ.com	jWb61YvLO@jy...	pe
01/17 10:19:26	CQgSYTzb.eXe	DC-Traffic	DC-Traffic	10.154.228.8	pancademo\jorda...	202.102.56.193	25	smtp	malicious	Hd1dEjH9BRfSo...	uC0Jru@KTCYqi...	pe
01/17 10:19:25	utzrXM.exe	DC-Traffic	DC-Traffic	192.168.220.227	pancademo\mars...	220.123.106.202	25	smtp	malicious	ejwqEfeEVhEEI9...	bR64Wr4t6bG@...	pe
01/17 10:19:25	aC3doG.exe	DC-Traffic	DC-Traffic	10.154.10.88	pancademo\angel...	86.60.66.240	25	smtp	malicious	QzBWO7kcZ9Q9...	VP@wQfcfAvhYt...	pe

Figure 8: The Monitor tab provides detailed views into important information, such as traffic, known threats reported by WildFire, unknown files, malicious URLs, data filtering logs and more

Example SOC Monitoring Scope

Next-generation SOCs are able to see through the confusion of alerts and quickly identify incidents that need more attention. The following table is an example set of high-level policies that an organization can enforce with the security platform – all monitored centrally – out of the box.

Policy	Product	SOC Monitoring
Block unapproved applications/URL categories	Next-Generation Firewall	Centralized monitoring from the ACC and Monitor tabs
Allow whitelisted applications/URL categories	Next-Generation Firewall	
Block known malicious files and known malicious links within email	Next-Generation Firewall	
Block outbound HTTP POSTs containing corporate credentials to unknown URLs (anti-phishing)	Next-Generation Firewall	
Block outbound malicious DNS queries	Next-Generation Firewall	
Block outbound malicious URL categories	Next-Generation Firewall	
Block outbound known C2 IPs/URLs	Next-Generation Firewall	
Block outbound packets w/payloads matching C2	Next-Generation Firewall	
Block outbound UDP traffic categorized as "Unknown"	Next-Generation Firewall	
Transmit the following file types to WildFire for inspection: portable executables, .doc/docx, .xls/xlsx, .ppt/pptx, pdf, .jar/.class, .apk	• Next-Generation Firewall • WildFire	
Reprogram NGFWs with new signatures from WildFire every five minutes	• Next-Generation Firewall • Threat Prevention Subscription	
Enforce above rules on all endpoint traffic when remotely connected (Windows®, Mac®, iOS, Android™).	• GlobalProtect • VM-Series Next-Generation Firewall • Amazon® AWS® or Microsoft® Azure®	
Prevent endpoints from running applications that exhibit malicious behavior of malware or exploits. Perform the following checks on every executed file: • Check admin overrides • Check against trusted publisher list • Send to WildFire for inspection and analysis • Perform local static analysis via machine learning • Detect memory corruption (anti-exploit) • Detect logic flaws (anti-exploit) • Detect malicious code execution (anti-malware) • Evaluate execution restrictions • Restrict execution from tmp directories	Traps	
Quarantine malware in sanctioned SaaS applications	Aperture	
Detect and remove oversharing of sensitive data in SaaS applications	Aperture	
Block outbound malicious IPs received in third-party threat intelligence subscriptions	• Third-party threat intelligence subscriptions • MineMeld • Next-Generation Firewall	

Panorama extends the scope of SOC monitoring beyond Palo Alto Networks products by supporting a plug-in architecture to enable new third-party integrations or updates to existing integrations (such as the VMware® NSX® integration) outside of a new PAN-OS® feature release.

ICS/SCADA Considerations

Like other industries, ICS/SCADA networks have also been impacted by advanced attacks, as well as less targeted but equally damaging malware infections from unwitting users. To effectively and efficiently protect control systems networks, security and network teams require clear visibility into whatever ingresses and egresses these networks. Visibility into the applications, as well as the individuals and/or teams using them is critical, especially since most protocols used in the controlling of these processes are considered to be at-risk. For example, Modbus is a protocol inherently flawed by design as it is unauthenticated and unencrypted.

Next-generation SOCs in ICS/SCADA environments can realize the same advantages of native integration and automated prevention that enterprise IT environments benefit from. With support for protocols like Modbus and others, IT and OT teams can both develop contextual policy-based decisions regarding which applications to block or allow for specific user communities or groups requiring access to the ICS network. Find more details on deploying the Next-Generation Security Platform in ICS/SCADA in our Industrial Control Reference Blueprint.

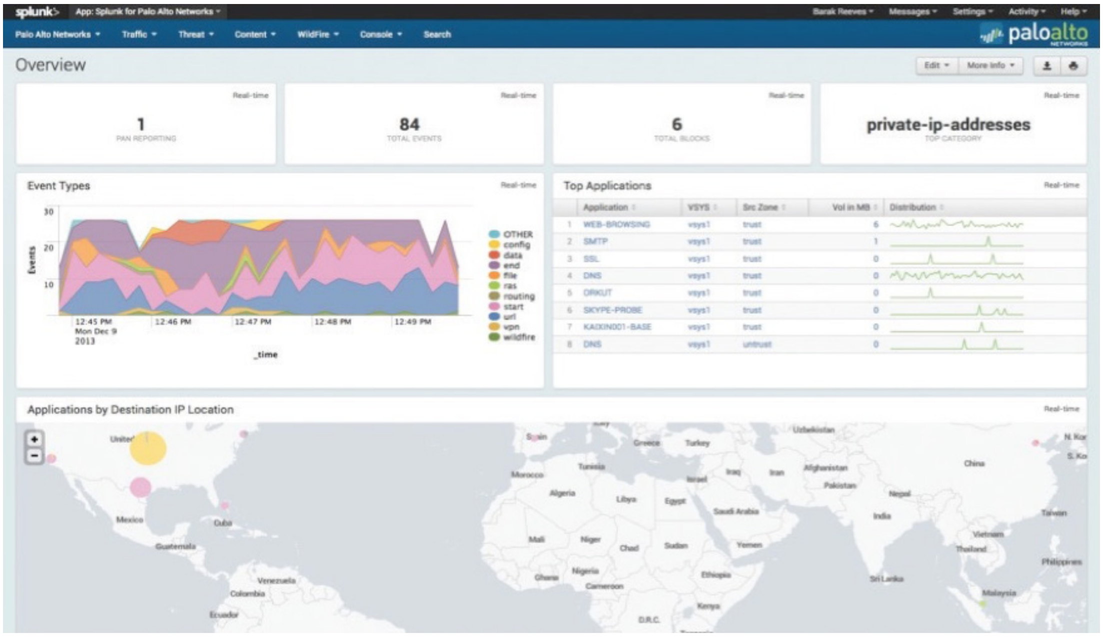
Extending Insights Through Third-Party Integration

Palo Alto Networks provides an open security platform through APIs that enable third-party vendor integrations. The integration possibilities with third-party vendors make it easier to take advantage of existing security investments and further enhance the capabilities of a next-generation SOC.

Bidirectional Splunk Integration

Palo Alto Networks and Splunk® have partnered to extend the powerful visibility into network traffic from Panorama to other network components. The combined solution delivers highly effective, coordinated detection, incident investigation and response for advanced threats. With the Splunk app for Palo Alto Networks, enterprise security teams obtain a powerful platform for security visualization, monitoring and analysis that enables them to fully leverage the extensive application, user, content and threat data generated by Palo Alto Networks devices. The integrated solution not only combines several approaches for identifying advanced threats – including dynamic sandbox analysis, statistical anomaly detection and infrastructure-wide event correlation – but also enables security administrators to expedite incident response by automating the steps needed to block malicious sources and quarantine compromised devices.

The integration is bidirectional, which means Splunk can not only receive dynamic sandbox analysis data, statistical anomaly detection and infrastructure-wide event correlation, but also push data back into the security platform. This enables threat hunters in the SOC to expedite incident response and automate the steps to block malicious sources and quarantine compromised devices.



	Application	VSYS	Src Zone	Vol in MB	Distribution
1	WEB-BROWSING	vsys1	trust	6	
2	SMTP	vsys1	trust	1	
3	SSL	vsys1	trust	0	
4	DNS	vsys1	trust	0	
5	ORKUT	vsys1	trust	0	
6	SKYPE-PROBE	vsys1	trust	0	
7	KADXIN001-BASE	vsys1	trust	0	
8	DNS	vsys1	untrust	0	

Figure 9: **Integration with Splunk extends visibility and prevention capabilities to your entire network infrastructure beyond next-generation firewalls**

Deployment Options

As you plan to build a next-generation SOC, you can consider a few options for deploying the security platform as a core component of the underlying technology. There are two typical deployment scenarios of the security platform in next-generation SOCs: the hybrid approach and the SIEM-less approach. In the hybrid model, the security platform is deployed with prevention enabled and pushes logs into a SIEM for monitoring. In the SIEM-less model, the security platform replaces the SIEM as the single pane of glass for all SOC activities.

Hybrid Deployment Model

The hybrid model involves configuring a feed from Panorama into the SIEM, and the SOC team monitors the SIEM as its primary source of information. The value in this deployment model is in the reduced events per analyst hour (EPAH), when compared to the number of events generated by a feed from a legacy firewall. The security platform automatically prevents the majority of cyberattacks and the SOC team focuses their time on the smaller percentage of events that require further hunting and analysis. This model does not require you to deploy all security platform components.

SIEM-less Deployment Model

The SIEM-less model of deployment removes the SIEM from the picture completely. The SOC team monitors Panorama as its single pane of glass into the environment. This deployment model takes advantage of the full benefits of the security platform and also realizes lower TCO when compared to the hybrid deployment model. The lower TCO is a result of the elimination of the SIEM, which often requires a significant amount of manual work to create and maintain all the required feeds from the disparate systems. The security platform eliminates the feed management since all the components of the platform integrate natively out of the box. Note that for this approach to be successful, all core elements of the security platform, including advanced endpoint protection, are deployed throughout your organization to ensure full coverage from cyberattacks.

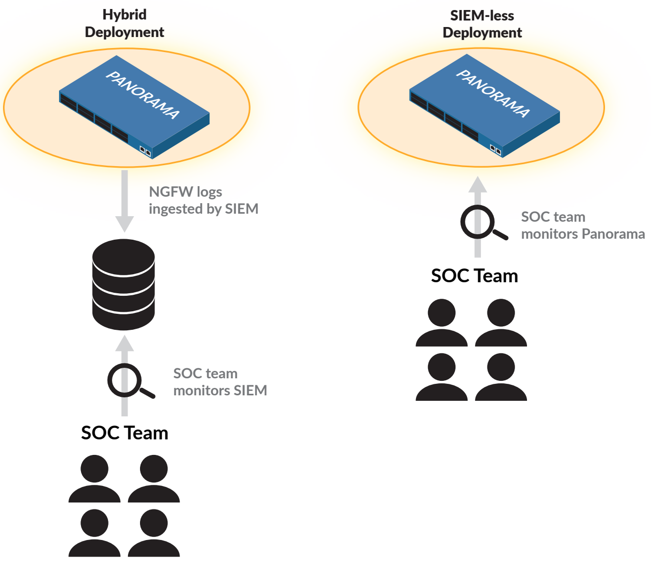


Figure 10: Next-generation SOC deployment models

The next section chronicles a use case of an actual customer who created a next-generation SOC based on Palo Alto Networks Next-Generation Security Platform.

Customer Deployment

A global leader in interactive and digital entertainment approached Palo Alto Networks and requested assistance to improve the operations of their SOC. Millions of the customer's video game units across the globe connect to their network services via the internet to enable functions like online gameplay, video streaming and system updates. Securing these highly distributed network services from advanced cyberattacks is a top priority as they continue to push the boundaries of online gameplay by developing some of the most highly rated online gaming and entertainment experiences.

Customer Business Challenge

The customer's network was targeted by a highly advanced cyberattack, which impacted their customer-facing online services and prompted a comprehensive risk analysis of their security operations that ultimately resulted in significant improvements to both their security program and architecture. They knew they needed a better way to quickly identify cyberattacks on their network and coordinate responses.

The customer built a security operations center, or SOC, intended to be the intelligence backbone of their security responses, and directed their legacy firewall, IPS and proxy logs into a single SIEM. When they first went live with their SOC, their leadership quickly realized that their Level 1 (L1) SOC analysts were trying to handle 200 EPAH. There were so many events that even experienced analysts were overloaded with analysis, SIEM rule-writing and wasting time on false positives. The network engineering team was bombarded with requests to create port- and protocol-based rules (i.e., to black-hole bad IPs) and the overall response time for the legitimate security events was very slow. Sometimes it took days to black-hole a malicious IP address. The customer needed their EPAH to drop from more than 200 to a more sustainable level under 30.

The customer realized that they were unable to hire enough people to staff a SOC team capable of keeping up with the events, not to mention their need to take into account future growth of their business. Highly skilled SOC staff members are hard to find, hard to retain, and often demand some of the highest salaries in IT.

Know your EPAH: A SOC's most important metric.

Measure your SOC's EPAH metric. If it's over 30, your analysts don't have enough time to evaluate events that require deeper analysis.

Deploying the Next-Generation Security Platform:

- Enabled the SOC's EPAH metric to drop from 200 to 20.
- Automatically blocked 95 percent of the events.
- Stabilized the head count on the security/network teams, minimizing the ongoing team Opex with the shift from human to machine automation.
- Customer decommissioned legacy firewall, significantly reducing Capex as well.

At this point, the customer began looking for a solution to automate the process of IPS signature development. Cyberattackers use automation and technology to scale their attacks – it only makes sense that a good cyber defense follows the same strategy.

Customer Solution

The customer deployed Palo Alto Networks next-generation security appliances with WildFire in-line with their user traffic. The solution architecture provided the visibility the team required to automate the prevention from the cyberattack hitting their network while maintaining the high performance requirements of their customer-facing network. Panorama provided the team with policy synchronization and integrated logging.

The customer also realized the value of the platform's unique user and application visibility (with features like User-ID™ and App-ID™ identification technologies) to get more granular control and better risk reduction. With full visibility into user and application traffic, the customer was able to stop active attacks automatically. The impact on the SOC team was dramatic.

Customer Results

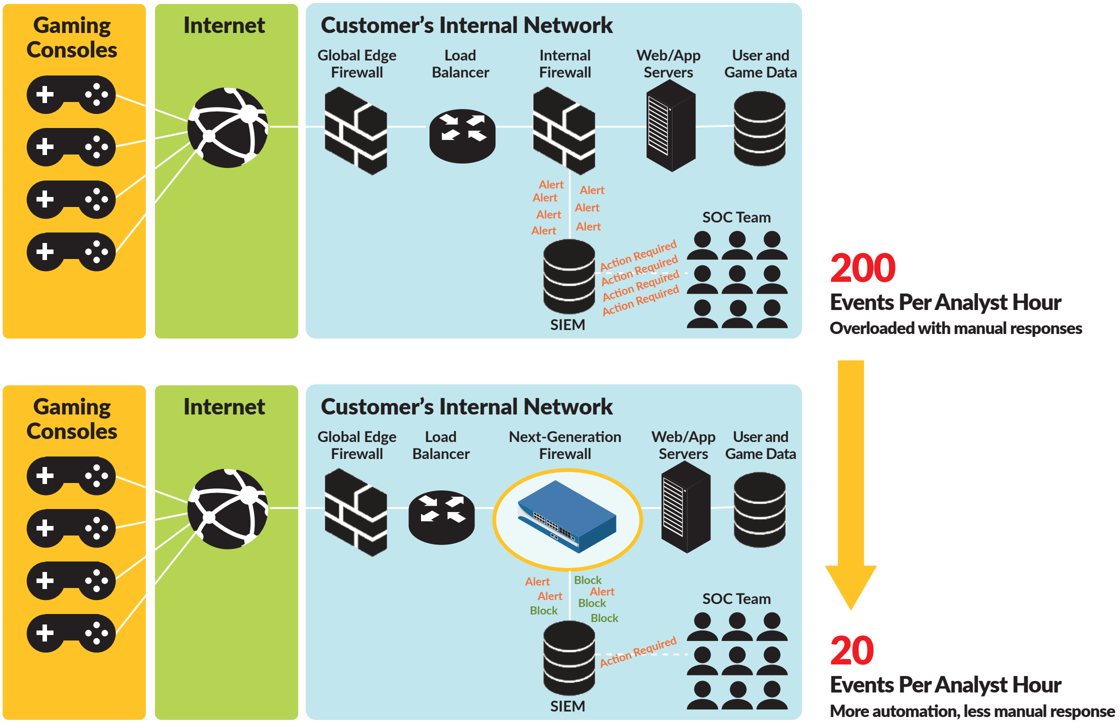


Figure 11: Customer deployed Palo Alto Networks Next-Generation Firewall and experienced an immediate decrease in events per analyst hour from 200 to 20

Shift to Machine-Based Automation

With the next-generation appliances and Panorama in place, and with blocking enabled, the customer had deployed a next-generation SOC. The next-generation appliances dramatically reduced risks to the customer's network and became their SOC's primary source of threat intelligence. Operational efficiencies increased dramatically within the SOC team, which in itself reduced risk: EPAH dropped from 200 to 20. The number of events requiring analyst attention dropped significantly. The SOC team shifted their efforts to the most critical, complex events, and spent more time on strategic, proactive efforts to improve security within their customer-facing environments.

Minimal Opex

The customer scaled with technology, rather than people, to drop their EPAH from 200 to 20. They found that they didn't require highly experienced senior SOC analysts to operate the Palo Alto Networks portion of their security infrastructure. Ninety-five percent of the events the SOC blocked were blocked automatically by the Next-Generation Security Platform. The shift from human to machine automation stabilized the headcount on the security/network teams, minimizing the ongoing team Opex.

The customer was suffering from the most common problem SOCs face: security-event overload

Level 1 SOC analysts were trying to handle 200 EPAH. Experienced analysts were overloaded with analysis, SIEM rule-writing and false positives. Sometimes it took days to black-hole a malicious IP address.

Minimal Capex

With the Next-Generation Security Platform, the customer was able to decommission their incumbent legacy firewall vendor, resulting in significant savings in technology costs. They replaced legacy physical firewall appliances with physical Palo Alto Networks appliances to achieve this outcome. They are also developing plans to decommission their incumbent URL filtering vendor and instead consolidate and simplify other areas of their security architecture based on the Next-Generation Security Platform – which will further minimize Capex.

Conclusion

The customer now runs one of the most sophisticated next-generation SOCs in the world, vastly improving the protection of their high-profile enterprise network and their intellectual property, based on Palo Alto Networks Next-Generation Security Platform. They drastically cut the threats – with automation – and drastically cut the events to which the team had to respond, freeing up resources to focus on what is most critical. They scaled with technology, rather than people, to increase their SOC's effectiveness while decreasing Capex and Opex. Their investment in Palo Alto Networks is an extension of their strategy to continue to be the global leader in interactive and digital entertainment, remaining competitive while protecting precious intellectual property, by taking a prevention-oriented approach to cyberattacks.

Organizations that adopt a next-generation platform as the core of the security architecture realize true cyber risk reduction and many other benefits over architectures based on disjointed point-products. Native integration of security components at the network, endpoint and cloud results in faster correlation and a much faster, automated response to cyberattacks – greatly increasing the effectiveness of their security and thus the SOC that oversees all these activities.

Next-generation SOCs based on the Palo Alto Networks platform typically experience a significant decrease in the number of events per analyst hour compared to their previous legacy SIEM-based SOC. Human efforts are focused instead on more sophisticated analysis and threat hunting. Next-generation SOCs minimize Opex and Capex by scaling with technology instead of people, and decommissioning security point products replaced by the security platform.

Visibility into complex data and automation are key requirements in today's security SOC infrastructure. These requirements are present in the Palo Alto Networks platform user interface. The Application Command Center makes sense of vast amounts of data and displays it in a highly visual and interactive format for the administrator. Dashboards can easily be customized to the individual needs of an administrator while extensive drill-down, filter and search capabilities help SOC professionals find answers to crucial questions for a rapid response. The added ability to incorporate Palo Alto Networks platform ACC and integration with third parties for additional improvements within their networks further enhance the capabilities of the platform by extending unified security and visibility to all network components.

Business Benefits

- Best-in-class prevention of cyberattacks
- Minimal Opex – scale the SOC with technology, not people
- Minimal Capex – decommission security point products and replace them with the natively integrated Next-Generation Security Platform

Operational Benefits

- Significant shift from manual, human-based processes and event analysis to machine-based automation, resulting in faster response times
- Significant decrease in events per analyst hour, resulting in more effective use of human capital for more sophisticated analysis and threat hunting

Technical Benefits

- Simplified security architecture
- Make actionable use of threat intelligence feeds and subscriptions by automatically blocking malicious IPs

Palo Alto Networks streamlines SOC activities, makes vast amounts of data actionable, and provides invaluable tools that help you prevent successful cyberattacks.

4401 Great America Parkway
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com