MAY 2020

SIEM
& THE CLOUD

by NETWORK BOX USA
cybersecurity done right

LET'S TALK ABOUT THE CLOUD

The conversation about Cloud, be it public or private or hybrid, has been going on for at least 10 years now. As we ease our way into full scale adoption, and with more people realizing that this is the direction things are advancing towards, other conversations become important.

Without debating how and why the public Cloud will eventually replace traditional IT altogether, let us, for the purposes of this document, assume this to be the case.

As security goes, we now find ourselves managing an environment that is apparently not under our complete control.

We may feel a bit lost as to how we would go about securing it.

The first thing we notice is that we appear to have lost visibility over what is going on with those servers.

AN IMMEDIATE EXAMPLE

When you had Exchange, you could easily look at the logs any time you wanted

To see if someone was trying to login as one of your users. Just brute-force his way into your system, and possibly escalate credentials. Now, with emails being in O365, if someone tries to force their way into the account, we will never know.

The only way for us to actually discern this is if we set up 2FA. So, the phone rings in the middle of the night, asking us to accept authentication to our account, well, let's just say alarm bells would go off instantly.

HOLD UP, WAIT A MINUTE

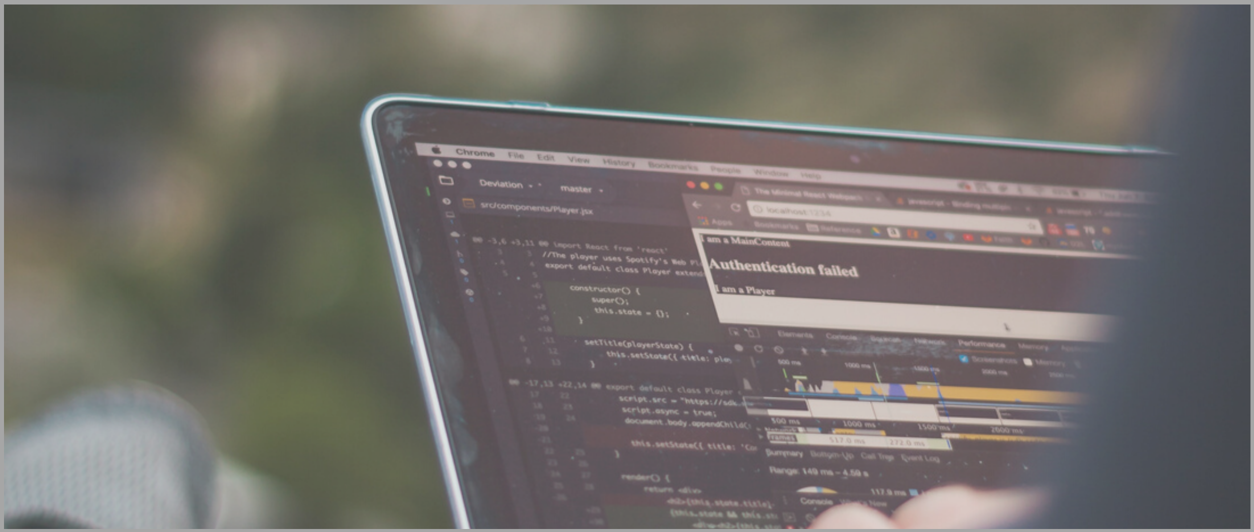
Truth be told, we all know that 2FA alone isn't going to be enough.

WE NEED MUCH MORE

And that is the cold hard truth of the matter

We know we can't count on 2FA to be our sole means of knowing when foul play is attempted. We need a way to constantly monitor every event, and be instantly alerted of any occurrence that appears out of the ordinary. This is where a SIEM comes in since this is what a SIEM was designed for. It's evident how the adoption of a SIEM (*useful for a traditional LAN environment*) becomes mandatory when moving to the cloud.

A SIEM will log monitor every event occurring on each server. It has rules to recognize what we deem "*normal*" and alert us when there is an anomaly.



WHAT ELSE?

Machine Learning

"It should also have the ability to use machine learning."

To be able to infer from "*experience*" when an event may be an anomaly even if we ourselves haven't thought of it, and/or created a rule for it. To be clear, many out there talk about using AI for this. AI is a stretch, and it needs to be very clear that to be AI, it must have the ability to predict behavior.

SIEM products do not do that.

They look at events that have already occurred. In fact, one could say that SIEM products adopt a retrospective approach and they look at the past. Yes, even if "*past*" in this case means a scant milliseconds ago. And with knowledge of the more remote past, they are able to correlate events of the present, to determine if something is out of normal behavior.

AI & ML

Distinguishing between the two

"They do not predict behavior and therefore, they are not AI."

This is irrefutable.

They do not predict behavior, and therefore they are not AI.

They do not make automatic adjustments based on trajectories, trends and patterns.

They do not make decisions.

Without seeming to downplay their significance (*and, at the same time, in an attempt to clarify the distinction*), these are not AI.

Rather, they are ML (*or Machine Learning*) which, in itself, is also a fantastic and very welcomed addition.

DO NOT BE DAUNTED

SIEM for cloud services can be fast and smooth to deploy

```
<!--meta-->
<title></title>
<meta name="viewport" content="width=device-width, initial-scale=1.0,
<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">
<link rel="icon" href="/favicon.ico" type="image/x-icon">
<!--css-->
<link type="text/css" rel="stylesheet" href="css/materialize.min.css"
<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4
<link rel="stylesheet" href="/css/animate.css">
<link rel="stylesheet" href="css/theme.css">
</head>
<body>
  <!--  banner-->
  <div class="banner">
    <nav class="nav">
      <div class="nav-wrapper">
        <div class="container">
          <a href="#" class="brand-logo hide-on-med-and-up"><h3><span style="font-weight:
  </div>
```

Any provider, ourselves included, have plugins that can be installed on servers just as one would in one's own private cloud. The collation of data is, we hope, undertaken via AES256 (*otherwise, consider changing SIEM providers*). For multi-tenant SIEMs, the data is uniquely identified by your own private keys, right down to each individual server.

This true real time collection and monitoring of logs enables you (*or your SIEM partner, if you're using a managed service*) to detect anomalies in similarly true real time, and trigger alerts over possible intrusion attempts.

ON CLOUD 9

But (*and perhaps even more importantly*), it will resurrect that sense of assurance and peace of mind that (*very likely*) went MIA the moment you moved to the cloud.

A sense of comfort and relief in the knowledge that your data is being watched upon, and monitored and protected, in true real time.

When we began migrating to the cloud in 2010, it seemed as though many corporations were regressing (*by up to even 10 years*) in terms of their behaviors and mentalities where security was concerned.

Servers were often exposed with minimal, if any, protection.

Or they were subscribed to a misguided notion that the IaaS too was providing security.

GUESS WHAT??

> *A decade has passed and that side of the house is still undergoing repairs.*

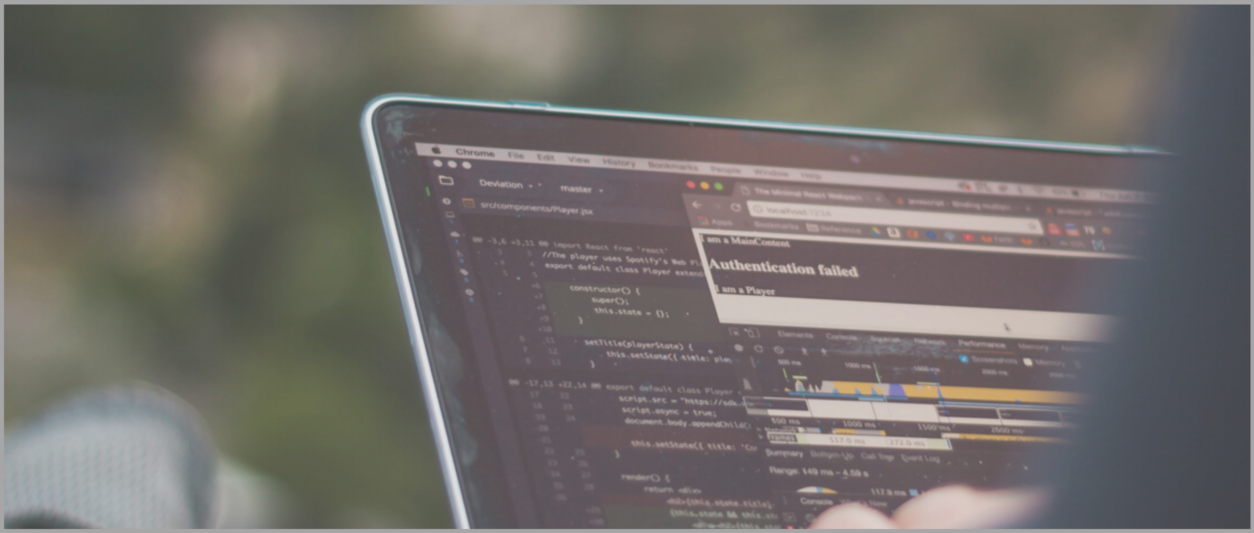
AND THUS WAS THE LESSON LEARNED

Mostly at our own expense

The industry has learned (*to its own detriment*) to protect its servers with a minimal of a firewall and IPS. Let us not today commit that very same travesty when it comes to data and log monitoring. Instead, let us be mindful and learn from our activities in the LAN. And execute it similarly in the cloud.

Yes, a SIEM might seem expensive at first but do take a moment to compare it against the cost of losing the company because of a breach.

The price probably isn't as exorbitant now, is it?



REACH OUT

Should you have questions or need assistance

WEBSITE	www.networkboxusa.com
LINKEDIN	www.linkedin.com/networkboxusa
TWITTER	www.twitter.com/networkboxusa
FACEBOOK	www.facebook.com/networkboxusa
YOUTUBE	www.youtube.com/NetworkBoxUSA
INSTAGRAM	www.instagram.com/networkboxusa
EMAIL	info@networkboxusa.com
CALL	832-242-5757

THE END

about network box usa

Formed in Y2K, we are a fully managed cyber network security services company offering enterprise class security solutions to SMBs. Businesses that are often ill equipped to fend for themselves in the fight against cyber threats. Over time, we have evolved to provide protection to organizations of all sizes across the globe.

Today, we are present in almost all of North and South America, Europe, the Middle East and Asia. We have our very own Security Response Center (*SRC*), 16 Security Operations Centers (*SOC*), and thousands of clients utilizing our network security monitoring services. These range from sole proprietors to prominent names within the Global Fortune 500 list.

We have received over 140 international awards, a clear testimony to the unwavering quality of our network security solutions. A trait which has never diminished over the course of two decades of operations. Our clients trust us with the security of their networks, and we are proud to lay claim to a 95 percent client retention/renewal rate. They stay and continue to purchase new solutions from us as operations expand.