

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: AIR-R02

SOC 2030 - SOCS ARE BROKEN, LET'S FIX THEM

Kerry Matre

Head of Security Operations Strategy
Palo Alto Networks



#RSAC

What is a SOC?



What does a SOC do?



Yes!

- Identify
- Investigate
- Mitigate



NO!

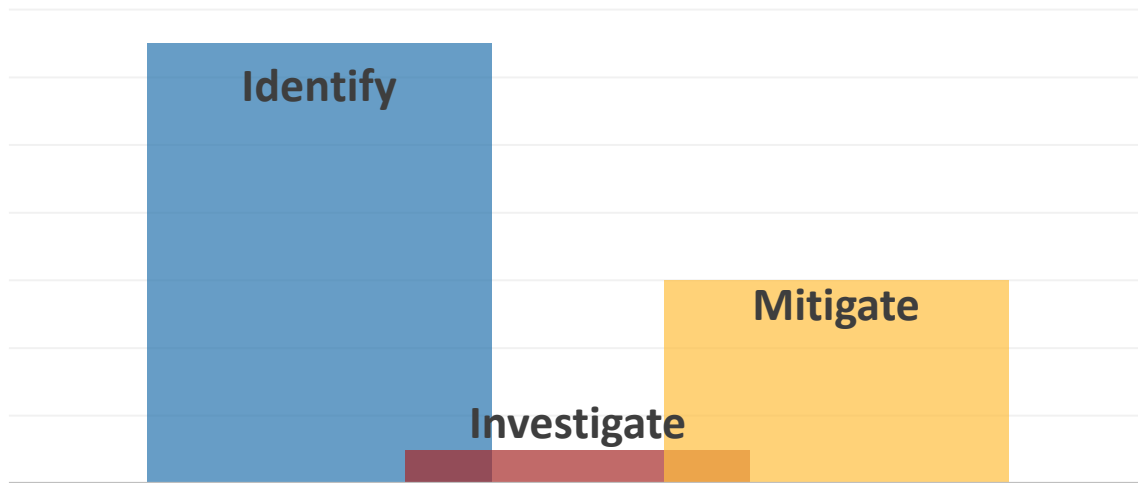
- Engineering
- Network Operations
- Forensics
- Incident Response
- Compliance
- Integrations/Development



One word: Overwhelmed



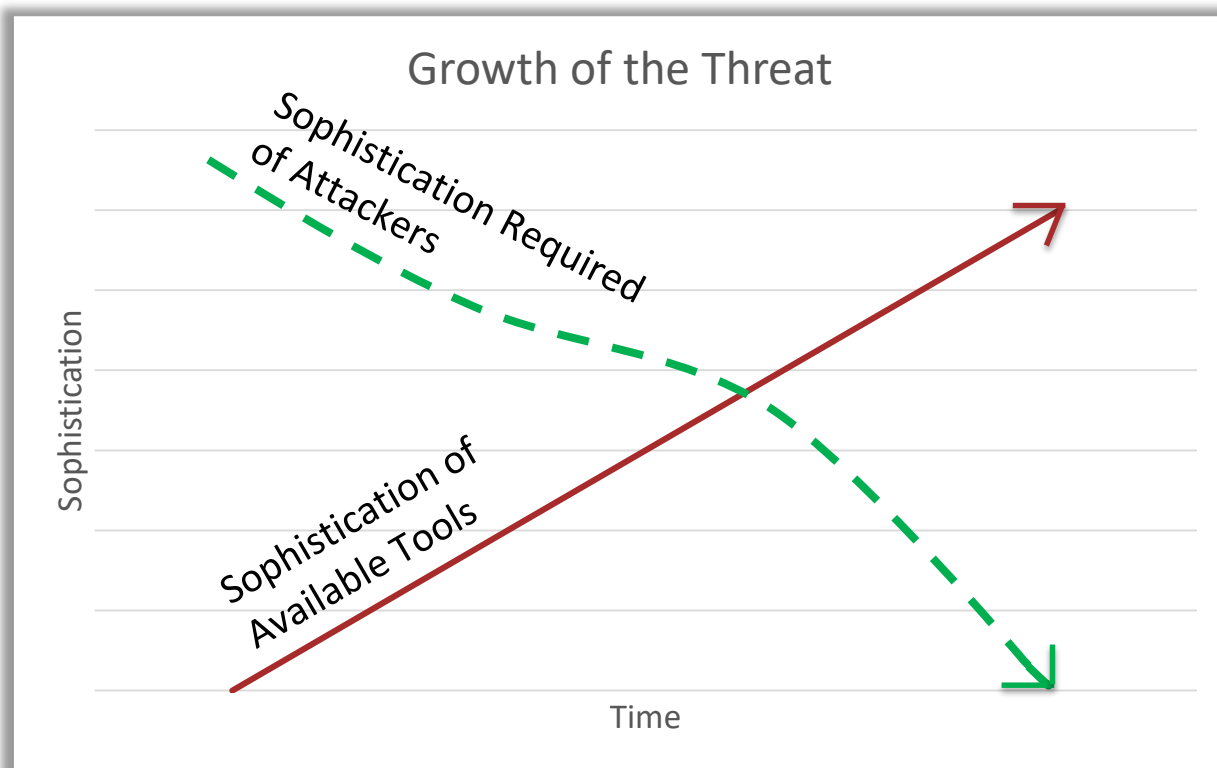
Time Allocation



Today



Machines vs. People



Prevention-based Architecture



Prevention-based Architecture



Consistent Protection
(Network, Endpoint, Cloud)

- 90% reduction in support tickets
- 70+% increase in visibility



Prevention-based Architecture



**Consistent Protection
(Network, Endpoint, Cloud)**

- 90% reduction in support tickets
- 70+% increase in visibility

Centralized Management

- Reduce Administration by 40%
- Decrease time spent on audits/regulations



Prevention-based Architecture



Consistent Protection (Network, Endpoint, Cloud)

- 90% reduction in support tickets
- 70+% increase in visibility

Centralized Management

- Reduce Administration by 40%
- Decrease time spent on audits/regulations

Automated Threat Prevention

- Updated prevention in minutes, not days
- Cut threat resources in half



Prevention-based Architecture



Consistent Protection (Network, Endpoint, Cloud)

- 90% reduction in support tickets
- 70+% increase in visibility

Centralized Management

- Reduce Administration by 40%
- Decrease time spent on audits/regulations

Automated Threat Prevention

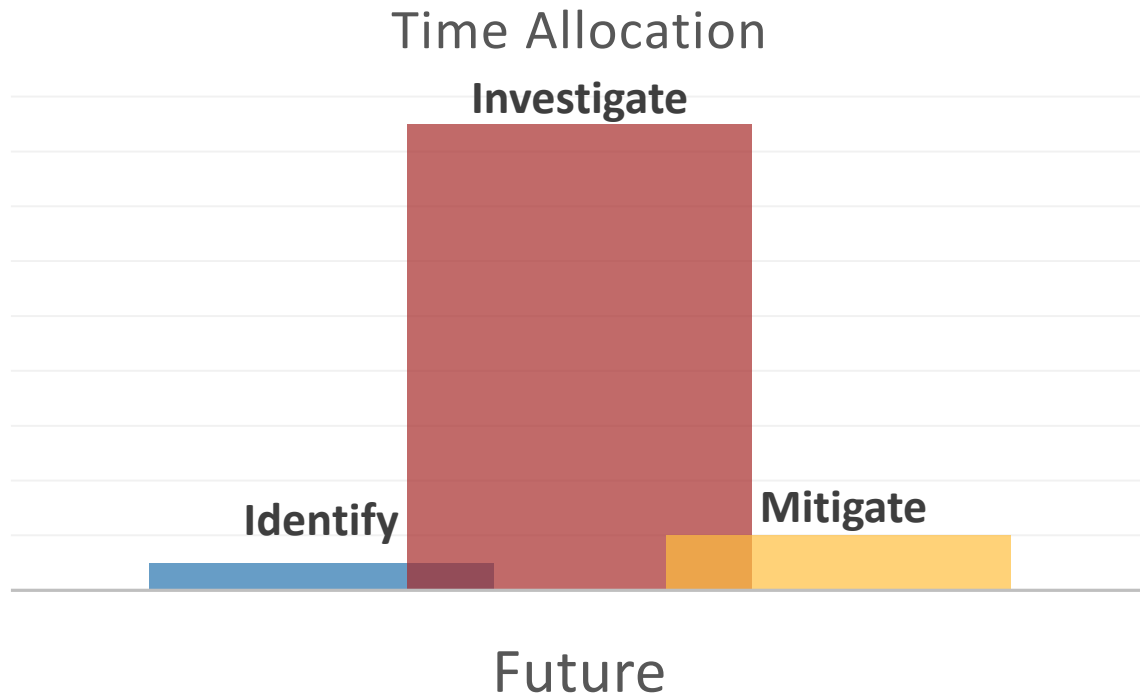
- Updated prevention in minutes, not days
- Cut threat resources in half

Prevention Based on Users, Applications and Data

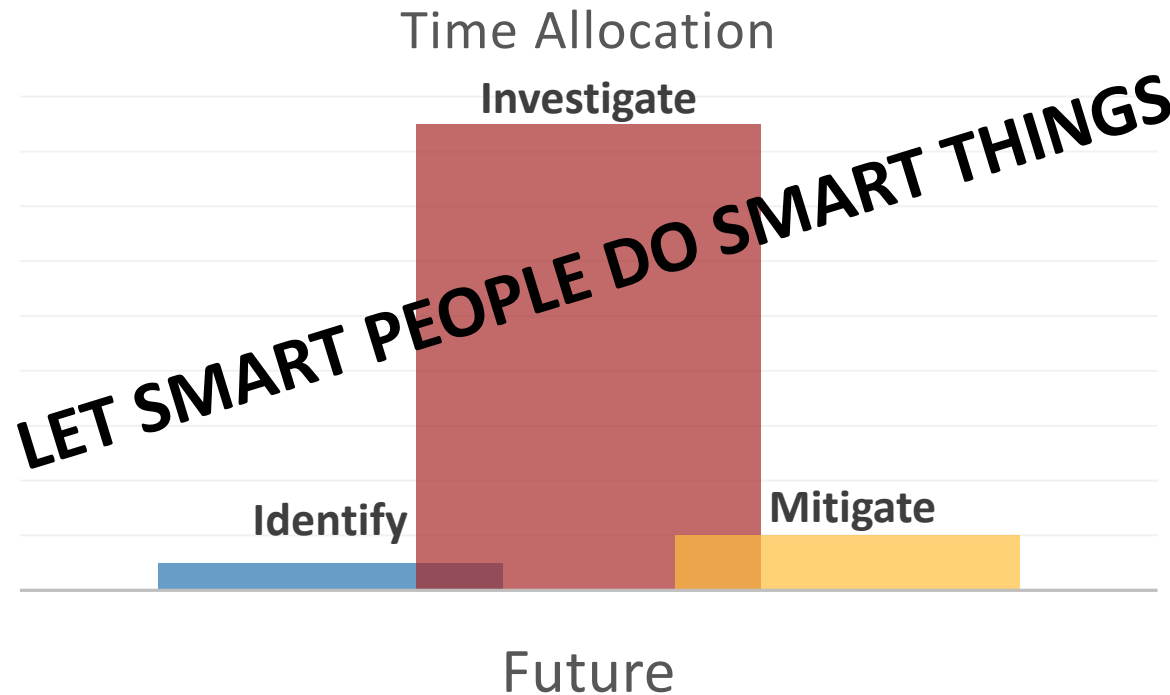
- Reclaim 130 hours/year/employee
- Reduce policy and rule maintenance



Shift the workload



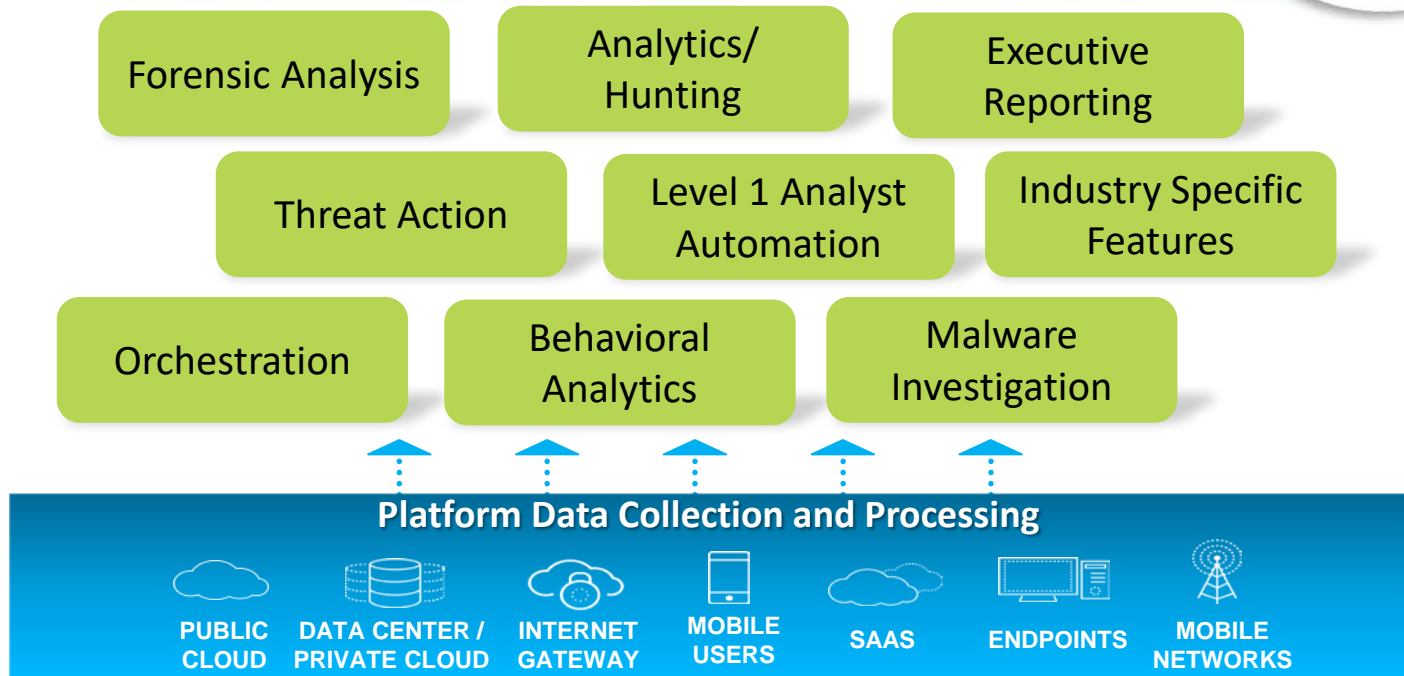
Shift the workload



You work with how many vendors?



Platform Consolidation



You can't affect what you can't measure



Simple as that



Configuration
Confidence

Operational
Confidence





All roses, butterflies and unicorns?





- Next week you should:
 - Identify what features of your technology is being used. (You were sold the dream, now go live it!)
- In the first three months following this presentation you should:
 - Clearly define the mission and scope of your SOC. (and stick to it)
 - Evaluate your metrics. (Do they serve the business and drive progress?)
- Within six months you should:
 - Move towards a Prevention-based Architecture: Consistent controls, Centralized management, Automated Threat Prevention, User/App/Data based controls.
 - Identify what vendors will be able to provide the platform approach necessary for the future.



Final Thoughts



KMATRE@PALOALTONETWORKS.COM
[@KMAYTREE](https://twitter.com/KMAYTREE)

