merlin
User Journey Map

SOC of the Future - Leveraging Automation, Orchestration & Machine Learning

Asset Transparency + ML-based Threat Management (UEBA) + SIEM + SOAR - Leveraging Machine Learning (ML) and automation to pro-actively address risk and employ machine-speed incident response for a majority of traditional Tier 1 events.

SEPIO SYSTEMS · DARKTRACE · Carbon Black. · SWIMLANE · CENTERITY · cyber OBSERVER · splunk> · POLARITY · CONTRAST SECURITY

1 - SOC Analyst leverages a unified UX to monitor instrumentation & cyber hygiene posture, as tools become more automated, ML-driven & self-directing. They collaborate with broader business teams, and focus more on strategy and business risk mitigation.

2 - Analyst has insight into ALL assets on the network, and would be alerted to a rogue device. However, quicker than the analyst can determine whether this is a problem, the SIEM is informed.

3 - While a device has been compromised, things happen so quickly that the analyst likely won't need to respond to an alert before automated security measures have mitigated the risk...

4 - Analyst is alerted to activities that are outside of "normal," and in this case, could see a network scanning alert as picked up by a UEBA & ML tool. At the same time, the SIEM is already integrating alert data.

5 - Before the analyst has time to process the alerts they are seeing, the SIEM has begun correlating alert data from the UEBA and rogue device tools. This is much faster than the analyst could do on their own.

6 - Quickly after the initial incidents occur (appearing as lesser, isolated alerts in yesterday's SOC), the system leverages the SOAR to parce together the disparate data points to establish an entire attack model.

7 - Again, in a matter of minutes, and likely without any SOC analyst intervention, the attack is identified, response actions initiated, and damage prevented.

8 - The SOC analyst will mostly see the event in an automated system action, where they can review actions taken if needed. If more analysis is needed, a tool like Polarity helps gather & track multiple disparate data points.

Protection | **Detection** | **Response** | **Recovery**

SOC/Future SOC

Fusion Center

NOC
DevSecOps
Risk
Facility Ops
Other Business

P. Parker, SOC Analyst

Business Risk Dashboard

Threat-Based Risk Management

Instrumentation Posture & Cyber Hygiene Monitor/Manage

Continuous Collaboration

CONTRAST SECURITY

Health | Events | Response
Unified SOC Visibility

cyber OBSERVER

CENTERITY

SIEM

Security Tools

Matter of Minutes...

Rogue Device Detected

SEPIO SYSTEMS

rogue device

SIEM splunk>

Align Asset Configurations and Privileges with Business Needs

Compromised Asset

Align Suspicious Activities with Business Risk and Other Operations

Suspicious Activity Issue

DARKTRACE

models of anomalous behavior

SIEM splunk>

Collaborative Response Activities Prioritized by Business Implications

Analyze & Respond

Informs and Enables Alignment of Current and Future Responses

Automated Response

Parces & Informs

SOAR SWIMLANE

Entire Attack Model
- Rogue device timestamp
- IP
- MAC address
- Port
- Host
- etc.

Prevents or Mitigates Damage done by Malicious Actors

Some Response Options:
- Disconnect/VLAN jail through NAC
- Shut down port/USB through Sepio
- Shut down VMware on server
- Leverage an EDR (Carbon Black) to remediate device
- Other, business specific...

Carbon Black.

Auto-response

Collaborative Continuous Improvement Actions

Mid-Event or After Action Review

Automated data analysis & retrieval for SOC review

POLARITY

SIEM | EPP | ...
EDR | NGFW

Attack Framework

S. Burch Adversary

S. Burch Adversary

Network

rootkit

B. Banner Innocent Victim

Network Scan

scanning

1 - Malicious actor performs recon activities, and due to lax physical security, is able to gain brief access to a network asset.

2 - Malicious actor is able to plug in a small network (rogue) device with a USB rootkit.

3 - Rogue device is able to deliver rootkit malware to a Windows 10 machine, and initiate network scanning.

4 - Network scanning activities are initiated, and flagged as anomalous behavior due to the spike in activity, activity type, and device initiating the scans.

5 - Quickly after the scanning begins, the SIEM is informed.

6 - Malicious activity is identified, with corroborating evidence, likely long before SOC analyst would put the pieces together.

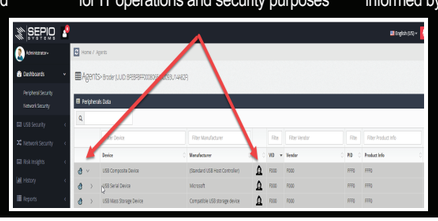
7 - Before too much damage is done, the rogue device is disabled or quarantined. The adversary is not able to maintain their presence.

Recon | **Weaponize** | **Deliver** | **Exploit** | **Control** | **Execute** | **Maintain**

Abbreviated Capabilities Storyboard

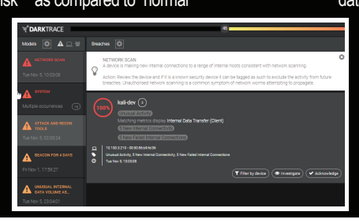
Full enterprise transparency for instumentation and cyber hygiene

Full enterprise transparency for HW/SW for IT operations and security purposes



Full transparency of assets,users & privileges, informed by business needs & calculated risk

Full awareness of enterprise status & events as compared to "normal"



Real-time, integrated views of pre-collected data points related to suspicious activity

Access to create, view, & edit playbooks plus "beyond playbook" automated system responses

Reliance on automation for a majority of issues